Cisco Secure Access Help

Cisco Secure Access
Updated September 15, 2026

Topics included

Part I: Getting Started and Onboarding....42

1 Introduction to Secure Access....44

Welcome to Cisco Secure Access....45
Secure Access Single Sign-On Authentication....45
Sign into Secure Access with Security Cloud Sign On....46
Configure Single Sign-On Authentication....47
Troubleshoot Single Sign On Authentication....48
Find Your Organization ID....49
Determine Your Current Package....49
Limitations and range limits....50
Destinations for Client-Based Zero Trust Traffic....51
Domain Names....52
File Inspection and File Analysis....52
Internet Protocol Versions....52
IP Address Restrictions....53
Other Components....54
Reports....56
Resource Connectors and Resource Connector Groups....56
Service Connections....56
Users and Groups....56
Endpoint Data Center Selection....57
Roaming Web Protection (Secure Web Gateway)....57
Zero Trust Access (ZTA) for Private Applications....58
Trusted Internet Access (TIA) via the ZTA Client....59
Remote Access VPN (VPNaaS)....59
Regional and US Federal Government Deployments....60
Information to Gather Before Contacting Cisco Support....60

2 Secure Access Dashboards....62

Secure Access Overview Dashboard....63
Get Started Workflow....63
Experience Insights....63
Network Tunnel Group Usage....64
Connectivity....64
Data Transfer....65
Security....65
Users and Groups....67

Private Resources....69
Service Analytics Dashboard....70
Security Insights Dashboard....72
Security Overview Tab....74
Data Security Tab....76
AI Governance Tab....77
Applications Tab....79
Users Tab....80
Threats Tab....81
Set Background Theme....83
Secure Access Status Portal....84
Interpreting Cloud Security Platform Service Status....85
Scheduled Maintenance....87
Service Status History....88
Manage Outage Notifications....89

3 Cisco Assistant for Secure Access....90
Get Started with the Cisco Assistant....91
Use the Cisco Assistant....91
Cisco Assistant Navigation....93
Add Rules with the Cisco Assistant....95
Enter a Natural Language Prompt to Generate Policy Rules....96
Cisco Assistant Rule Examples....99
Contextual Conversations....101
Find Documented Answers with the Cisco Assistant....101
Best Practices for Prompts....102
Contextual Conversations....102
Troubleshoot Access Issues with Private Resources....103
Optimize Access Policies....105
Messages Generated by the Cisco Assistant....108
Create Cisco Support Cases....109

4 Regions....112
Secure Access Regions....113

5 Network Requirements....120
Network requirements for Secure Access....121
DNS requirements....121
Secure Access DNS Resolvers....121
Secure Access Encrypted DNS Queries....123
Secure Access DNS, Web, and Block Pages....124
Secure Access DNS and Web – Client Configuration Services....124
Secure Access DNS and Web – Client Sync Services....125

Secure Access DNS and Web – Client Certificate Revocation Services....125
Secure Client requirements....126
Cisco Secure Client and Captive Portal Detection....126
Cisco Secure Client and Device Hostnames....126
Transport layer security protocol requirements....126
TLS 1.2 Support in Windows....127
TLS 1.2 Support in macOS....127
Secure web gateway service requirements....127
Egress IP Addresses for the Secure Web Gateway....127
Ingress IP Addresses for the Secure Web Gateway....127
Realtime DLP secure ICAP requirements....143
SaaS tenant requirements....144
Microsoft 365....144
SAML identity provider requirements....144
Secure Access SAML Gateway Services....144
Secure Access SAML Identity Provider Domains....145
Secure Access SAML Gateway Client Certificate Revocation Services....146
Virtual private network requirements....146
Secure Access VPN Services....146
Secure Access VPN Client Certificate Revocation Services....147
Zero trust access requirements....147
Secure Access Zero Trust Client-Based Enrollment Services....147
Secure Access Zero Trust Client-Based Proxy Services....147
Secure Access Zero Trust Client-Based Proxy – Client Certificate Revocation Services....148
Secure Access Zero Trust Proxy Services – Unmanaged Devices....148
Secure Access Zero Trust Services and Connector Groups....148

6 Secure Access Onboarding....150

Get Started....151
Secure Access Onboarding Workflow....151
Step 1 – Configure network connections....152
Step 2 – Configure access to resources....153
Step 3 – Configure end user connectivity....154
Step 4 – Configure endpoints and network sources....155
Hybrid Private Access Workflow....156
Procedure....157
Quickstarts....159
Quickstart – Cisco Secure Client with Zero Trust Access....160
Quickstart – Cisco Secure Client with Virtual Private Network....161
Quickstart – Cisco Secure Client with Internet Security....162
Quickstart – Browser with SAML Authentication....162
Quickstart – Bring Your Own Device with Zero Trust....163
Additional Onboarding Resources....164

7 Basic Network Setup....166
Fully Qualified Domain Names for Network Connections....167
About Fully Qualified Domain Names (FQDNs)....167
Global FQDN....167
Regional FQDNs....167
VPN Headend FQDN....168
Manage Registered Networks....168
Add Network Resources....168
Point Your DNS to Cisco Secure Access....175
Clear Your DNS Cache....178
Clear Your DNS Cache on Computers and Servers....179
Clear Your DNS Cache on Browsers....181
Manage Internal Networks....182
Add Internal Network Resources....183
Update an Internal Network Resource....185
Delete an Internal Network Resource....186
Manage Sites....186

Part II: Core Platform Administration....188

8 Accounts....190
Accounts Overview....191
Add a New Account....191
Edit Account Settings....192
Delete an Account....193
Hide sources with de-identification....194
Enable De-identification....195
Disable De-identification....196

9 Network Infrastructure....198
Manage Network Devices....199
How to Add a Network Device in Secure Access....199
Procedure for Managing Network Devices....199
Secure Access NAT as a Service....202
Web Traffic and NATaaS....202
Non-Web Traffic and NATaaS....203
Best Practices for NATaaS....203
Reserved IP Addresses....203
Reserved IP Supplemental Terms....206
Network Connections....207
Comparison of Network Connection Methods....208
Network Tunnels in Secure Access....209

Resource Connectors in Secure Access....209
Network Tunnel Groups....209
Add a Network Tunnel Group....210
Delete a Network Tunnel Group....218
Edit a Network Tunnel Group....218
View Network Tunnel Group Details....219
Manage Summary Subnets....221
Override Route Summarization for a Network Tunnel Group....222
View Global Routes....223
Establish an IPsec Tunnel....225
Supported IPsec Parameters....228
Routing Options and Guidelines for Network Tunnel Groups....230
NAT Mapping for Network Tunnel Groups....231
Static Routing....232
Dynamic Routing with BGP....233
Dynamic Routing with Multi-Region Backhaul....236
Global Routing....240
BGP Next-Hop Configuration....242
User VPN Pool Sizing and BGP Advertisement....242
Asymmetric Routes....244
Equal-Cost-Multi-Path (ECMP) Support....246
Route Summarization....250
BGP route filtering per network tunnel group....251

10 Network Tunnels by Device....258
Best Practices for Configuring Network Tunnels by Device....259
Configure Tunnels with Cisco Catalyst SD-WAN....259
Configure Automatic Tunnels with Catalyst SD-WAN....267
Enable DNS resolution....267
Configure API credentials in SD-WAN Manager....269
Create the Cisco Secure Access policy to be configured in the SD-WAN branches....270
Deploy the Cisco SSE policy to be configured in SD-WAN branches....274
Configure Tunnels with Cisco ISR....280
Configure Tunnels with Cisco Adaptive Security Appliance....284
Configure Tunnels with AWS Virtual Private Clouds and Elastic Compute instances....290
Deploy a New AWS Transit Gateway....292
Configure Two VPN Site-to-Site Connections to the New Transit Gateway....292
Configure Tunnels with VeloCloud SD-WAN....295
Configure Tunnels with Cisco Secure Firewall....296
Configure NAT Policy....305
Configure Access Policy....309
Configure Secure Firewall VTI, PBR, and Per Tunnel Identity....309
Troubleshooting....317
Configure Tunnels with Meraki MX....319

Prerequisites for Tunnels with Meraki MX....320
Caveats and Considerations....320
Supported Use Cases and Requirements....321
Step 1: Add a Network Tunnel Group in Secure Access....321
Step 2: Configure a Tunnel in Meraki MX....322
Verification and Troubleshooting....326
Optional Configurations....327
Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels....327
Configure Tunnels with NEC IX2000 Series Router....329
Site-to-Site VPN tunnels with Microsoft Azure....331
Configure Azure S2S Tunnels with Static Routing....333
Configure Azure S2S Tunnels with Dynamic Routing with BGP....349
Configure a Site-to-Site VPN tunnel with Amazon Web Services....365

11 DNS and DDNS Servers....376
Manage DNS and DDNS Servers....377
Manage DNS Servers....377
Add a DNS Server....377
View DNS Servers....379
Edit a DNS Server....380
Delete a DNS Server....381
Map DNS Servers to Regions....382
Manage DDNS Servers....385
Add a DDNS Server Group....386
View DDNS Servers....387
Edit a DDNS Server....388
Map DDNS Servers to Regions....389

12 Resource Connectors and Connector Groups....394
Manage Resource Connectors and Connector Groups....395
Requirements and Prerequisites for Resource Connectors and Connector Groups....396
Allow Resource Connector Traffic to Secure Access....398
Add Resource Connector Groups....402
Add Connectors to a Connector Group....405
Obtain the Connector Image....407
Provisioning Keys for Resource Connectors....410
Deploy a Connector in VMware....411
Deploy a Connector in AWS....417
Deploy a Connector in Azure....420
Deploy a Connector in Docker....426
Determine the Number of Connectors Needed in a Connector Group....432
Assign Private Resources to a Connector Group....433
View a Connector Group's Connectors and Assigned Resources....435
Edit a Resource Connector Group....435

Disable, Revoke, or Delete Resource Connectors and Groups....437
Maintain and Monitor Resource Connectors and Connector Groups....440
Monitor Connector Group Status....441
View Connector Groups in Secure Access....442
View Connectors in Secure Access....443
Monitor Connector Status....444
View a Connector's Status....448
Enable a Connector in Secure Access....450
Increase Connector Group Capacity....452
Check Connector CPU Load....452
Schedule Upgrade Windows or Delay for a Connector Group....452
Add Upgrade Windows for a Connector Group....453
Add Delay of Upgrades for a Connector Group....455
Troubleshoot Resource Connectors and Connector Groups....456
Throughput Capacity is Less Than Expected....457
Users Cannot Connect to Private Resources....457
Connector Software Auto-Upgrades....458
Connector Operating System (OS) Version has Security Vulnerabilities....458
Connector is Expired....458
Stop a Connector....459
Unable to Revoke or Delete a Connector....459
Unable to Sync....460
Connector-Related Status Graphs are not Current....460
(Container Only) Connector Troubleshooting Tools....460
(VM Only) Connector Diagnostics (CLI)....461
Diagnostic Codes....464

13 Roaming Devices....468
Manage Roaming Devices....469
View Internet Security Settings for Roaming Devices....469
Procedure....469
Edit Internet Security Settings for Roaming Devices....472
Procedure....473
Delete a Roaming Device....476

14 Private Resources....478
Manage Private Resources....479
Add a Private Resource....481
Discover Private Resources....492
Map a Discovered Resource to Existing Private Resources....494
Test Private Resource Reachability....497
Add a Private Resource Group....499
Private Resource Configuration Examples....500

15 Connections to Private Destinations....502
Manage Connections to Private Destinations....503
Using Private Resources for SaaS Internet Destinations....503
Comparison of Zero Trust Access and VPN....503
Timeout Intervals for Zero Trust Access Sessions....504
Comparison of Client-Based and Browser-Based Zero Trust Access Connections....505
Requirements for Zero Trust Access....506
Configure Client-Based Zero Trust Access for Private Destinations....507
Configure Browser-Based Zero Trust Access to Private Resources....508
Network Authentication for Zero Trust Access....508
Connection Scenarios for Private Destinations....509
Manage Branch Connections....509
Endpoint Connection Methods....510
Branch Networks in Private Access Rules....510
Add an IPS Profile on Private Access Rules....512
Log Connections From Branch Networks to Private Resources....512
Allow SSH and RDP Access to Private Resources....512
Browser-Based Zero Trust Access....513
Client-Based Zero Trust Access....515
Application Portal for Zero Trust Access Browser-Based User Access....516
Prerequisites....516
Configure an Application Portal for Zero Trust Access Browser-Based User Access....516
Filter Policies Based on Applications....519
(Optional) Modify Settings....519

16 Network and Service Objects....520
Get Started with Network and Service Objects....521
Quickstart: Network and Service Objects....522
Access Rules with Network and Service Objects....523
Combine Destinations with Boolean Logic....524
Manage Network Objects and Groups....526
Get Started with Network Objects....526
Get Started with Network Object Groups....535
View Network Objects and Groups....543
Manage Service Objects and Groups....546
Get Started with Service Objects....546
Get Started with Service Object Groups....554
View Service Objects and Groups....562

17 Manage API Keys....566
Manage API Keys....567
About Secure Access API Keys....567

Add an API Key....567
Refresh an API Key....569
Update an API Key....570
Delete an API Key....571
About Key Admin API Keys....571
Add a Key Admin API Key....572
Refresh a Key Admin API Key....574
Update a Key Admin API Key....574
Delete a Key Admin API Key....575

Part III: Identity and Access....578

18 Users, Groups, and Endpoint Devices....580
Manage Users, Groups, and Endpoint Devices....581
Manage End-User Connectivity....582
View Users Provisioned in Secure Access....582
View Group and Organizational Unit Details....590
View Details for Endpoint Devices....591
Export User Data to CSV....593
Unenroll Devices for Client-Based Zero Trust Access....594
Reenroll the User Device on the Secure Client....595
Disconnect Remote Access VPN Sessions....595

19 User Directories and Device Management....598
Manage User Directories and Device Management....599
Configure User Directory Integrations....599
View Directories....600
Manage Cloud Identity Providers....601
Add a Cloud Identity Provider....601
View an Integrated Cloud Provider....603
Edit an Identity Provider Integration....604
Delete an Identity Provider Integration....606
Manage API Keys for Provisioning Identities....607
Guidelines....607
Add the API Key for Managing Identities....607
Refresh the API Key for Managing Identities....609
Delete API Keys....610
View Details About Provisioned API Keys....610
View Details for Identities Provisioned with the API....611
View Endpoint Devices....612
Manage Active Directory Integration....612
Download the Active Directory Components....613
Edit the Active Directory Connector Auto-Upgrades....613

Edit Authentication Properties for the AD Integration....613
Enable DLP Email Notifications for Reporting Managers....613
View Active Directory Components....613
Manage Sites for AD Components....614
Delete Active Directory Integration....614
Manage Google Workspace Account....614
Manage Imported Users and Groups....615
Import Users and Groups from CSV File....615
Upload a New CSV File with Users and Groups....618
Delete an Imported CSV File....618

20 Advanced User Configuration Settings....620
Manage Advanced Configuration Settings....621
Set Up Authentication Preferences for Identity Providers....621
Set Up IP Surrogates for SSO User Authentication....621
Set Up API Authentication....622
Manage IP Surrogates for User Authentication....622
How HTTPS Inspection Works....622
Enable IP Surrogates for User Authentication....622
Add Internal Networks for Bypass....623
Delete Internal Networks for Bypass....624
Manage Behaviour Analytics Configuration....625
UEBA Scope....628
Configure Analytics for DLP Violation Spike....628
Configure Analytics for File Operations with AI....635
Configure Analytics for File Operations Manually....638
Configure Analytics for High-Risk Country File Activities....641
Configure Analytics for Impossible Travel....643
Configure Analytics for Anomalous MCP Activities....645
Configure Analytics for Unseen Location Activities....647
Configure Analytics for Traffic Spike and Destination Monitoring....648
Configure Analytics for Failed Private Resource Access Attempts....651
Known Issues....654

21 Identity Providers....656
Configure Identity Providers....657
Provision Users and Groups from Duo....657
Limits and Best Practices....657
Supported Features....658
Add the Duo IdP directory to Secure Access....658
View Provisioned Users and Groups in Secure Access....660
Refresh SCIM Token....660
Attribute Mapping (Mandatory)....660
Provision Users and Groups from Okta....661

Configure the Cisco User Management Connector App in Okta....662
(Optional) Add an objectGUID Attribute and Create the User Profile Mapping....666
Customize the authName Attribute....669
Map the Custom authName Attribute to a User Profile....671
Assign Users or Groups in the App....673
Push Users or Groups from the App to Secure Access....674
View Logs in the App....676
Provision Users and Groups from Microsoft Entra ID....677
Configure Provisioning in Microsoft Entra ID....678
Configure Guest Users....680

22 Provision Users, Groups, and Endpoint Devices from Active Directory....682
Provision Users, Groups, and Endpoint Devices from Active Directory....683
Prerequisites for AD Connectors....683
Connect Multiple Active Directory Domains....684
Active Directory Components....685
Manage AD Connectors....694
Configure Authentication for AD Connectors and VAs....695
Configure Updates on AD Connectors....699
Connect Active Directory to Secure Access....701
(Optional) Specify AD Groups in Selective Sync File....705
Deploy LDIF Files for AD Connector....707
Change the Connector Account Password....711
AD Connector Communication Flow and Troubleshooting....712
Edit AD Authentication Properties....715
Best Practices: Configuring the AD Authentication Properties....716
Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications....717
AD Integration with Virtual Appliances....717
Network Diagram for VA Deployments....718
How to Set Up AD Components with VAs....718
Prerequisites for AD Connectors and VAs....719
Prepare Your AD Environment....720
Connect Active Directory to VAs....728
Configure Active Directory User Exceptions in Secure Access....735
Multiple AD Domains with Secure Access Sites....739

23 User Authentication Profiles....742
Manage User Authentication Profiles....743
Requirements for Configuring SSO Authentication Profiles....743
About the Default Provisioning Profile....743
Add SSO Authentication Profiles....744
View SSO Authentication Profiles....745
About Single Sign-On for Users....746
Sign-On for Provisioned Users....746

Sign-On for Non-Provisioned Users....747
Edit an SSO Authentication Profile....748
(OIDC Only) Get Metadata for OIDC Configuration URL....748
Edit SAML User Authentication Profile....748
Edit OIDC User Authentication Profile....750
Delete SSO Authentication Profile....752
Delete SAML User Authentication Profile....753
Delete OIDC User Authentication Profile....754

24 Integrations with Open ID Connect Identity Providers....756
Configure Integrations with OIDC Identity Providers....757
About Using OpenID Connect with Secure Access....757
Use Cases - SSO Authentication....758
Configure Duo for OpenID Connect....758
Configure Duo SSO authentication through OIDC in Secure Access....759
View Provisioned Users and Groups in Secure Access....760
Configure Okta for OpenID Connect....761
Verify the UPN and preferred_username Mapping....761
Step 1 - Choose an Authentication Method....761
Step 2 - Add an Identity Provider....762
Step 3 - Configure the Identity Provider's OIDC Metadata....763
Step 4 - Add the OIDC Metadata in Secure Access....766
Configure Microsoft Entra ID for OpenID Connect....767
Step 1 - Choose an Authentication Method....768
Step 2 - Add an Identity Provider....769
Step 3 - Configure the Identity Provider's OIDC Metadata....770
Step 4 - Add the OIDC Metadata in Secure Access....772

25 Integrations with SAML Identity Providers....774
Configure Integrations with SAML Identity Providers....775
Use Cases - SSO Authentication....775
Prerequisites for SAML Authentication....776
Configure Microsoft Entra ID for SAML....778
Step 1 - Add SSO Authentication Profile in Secure Access....779
Step 2 - Add SAML Identity Provider in Secure Access....780
Step 3 - Add the Identity Provider's SAML Metadata to Secure Access....782
Configure Okta for SAML....789
Step 1 - Add SSO Authentication Profile in Secure Access....790
Step 2 - Add Okta SAML Identity Provider in Secure Access....791
Step 3 - Download the Secure Access Service Provider Files....793
Step 4 - Configure Okta with the Secure Access SAML Metadata....794
Step 5 - Get Metadata from Okta App Integration....796
Step 6 - Add Okta Metadata in Secure Access....797
Configure AD FS for SAML....798

Step 1 – Add SSO Authentication Profile in Secure Access....799
Step 2 – Add AD FS Identity Provider in Secure Access....800
Step 3 – Add the Identity Provider's SAML Metadata to Secure Access....802
Configure Duo Security for SAML....812
Step 1 – Add SSO Authentication Profile in Secure Access....812
Step 2 – Add Duo Identity Provider in Secure Access....814
Step 3 – Add the Identity Provider's SAML Metadata to Secure Access....815
Configure Ping Identity for SAML....819
Step 1 – Add SSO Authentication Profile in Secure Access....819
Step 2 – Add Ping Identity Provider in Secure Access....821
Step 3 – Add the Identity Provider's SAML Metadata to Secure Access....822
Configure OpenAM for SAML....825
Step 1 – Add SSO Authentication Profile in Secure Access....825
Step 2 – Add OpenAM Identity Provider in Secure Access....827
Step 3 – Add the Identity Provider's SAML Metadata to Secure Access....828
SAML Certificate Renewal Options....830
Test SAML Identity Provider Integration....832

26 Access Policies....834
Manage the Access Policy....835
About the Access Policy....836
Rule Data....837
Default Access Rules in Your Policy....842
Manage Global Settings for Access Rules....844
Display User Input Field on Warn Pages....845
Microsoft 365 Compatibility....845
Decryption....846
Configure Decryption for Specific Sources....847
Client Resolved Domain Destination List....848
Disable Decryption for Specific Sources....848
Decryption Logging....849
Certificate Pinning....849
Rule Defaults: Default Settings for Access Rules....850
Zero Trust Access: Endpoint Posture Profiles....850
Zero Trust Access: User Authentication Interval....850
Configure Access Rule Editing Sessions....851
Intrusion Prevention (IPS)....852
Security Profile....853
Isolation Profile....853
Tenant Control Profile....853
Edit Rule Defaults and Global Settings....853
Using Wildcard Masks on Access Rules....854
Wildcard Masks in Composite Sources or Destinations....854
Guidelines....855

Examples of Wildcard Masks....855
View Related Activity for an Access Policy Rule....855
View Related Events for an Access Policy Rule....856

27 Internet Access Rules....858
Internet Access Rules....859
Default Settings for Internet Access Rules....859
Global Settings for Internet Access Rules....860
Components for Internet Access Rules....860
Control Egress IP Address for Select SaaS Internet Destinations....873
Ensure Rule Matching for Encrypted Internet Traffic....873
Block Internet Access to Geographic Locations....874
Add an Internet Access Rule....874
Access Criteria....875
Security Control Options....916
Geolocation Sources and Internet Access Rules....917
Sources....919
Add Geolocation Sources on Internet Access Rules....919
View Events Report....920
Filter the Report by Firewall Requests....923
Filter the Report by Web Requests....926
Edit an Internet Access Rule....929
About Isolated Destinations....931
Secure Access Package Support for RBI and Isolation Rules....932
Verifying Isolation....933
Limitations of Isolation....934
Isolate Downgrade....934
Troubleshoot Internet Access Rules....936

28 Internet and SaaS Resources....940
Manage Internet and SaaS Resources....941
Manage Destination Lists....941
Add a Destination List....942
Upload Destinations From a File....943
Edit a Destination List....945
Search the Destination List....946
Delete a Destination List....947
Download Destinations to a CSV File....947
Control Access to Custom URLs....948
Control Access to Domains....952
About Client Resolved Domain Destination List....952
Troubleshoot Destination Lists....956
Manage Application Lists....958
Add an Application List....958

Application Categories....961
Edit an Application List....963
Delete an Application List....964
Manage Content Category Lists....965
Available Content Categories....966
Add a Content Category List....971
Delete a Content Category List....972
Request a Category for an Uncategorized Destination....973
Dispute a Content Category....973
View Content Categories in Reports....973
Manage Tenant Control Profiles....980
Control Cloud Access to Microsoft 365....980
Control Cloud Access to Google Workspace....983
Control Cloud Access to Slack....985
Control Cloud Access to Dropbox....987
Control Cloud Access to YouTube....988
Blocking Behavior for YouTube Tenant Control....989
Control Access to ChatGPT....990
Control Cloud Access to GitHub....991
Edit or Delete a Tenant Control Profile....992
Use Tenant Controls in Access Rules....993
Review Tenant Controls Through Reports....994

29 Private Access Rules....998
Get Started With Private Access Rules....999
Default Settings for Private Access Rules....999
Global Settings for Private Access Rules....1000
Components for Private Access Rules....1001
About Endpoint Requirements in Access Rules....1008
Add a Private Access Rule....1008
Geolocation Sources and Private Access Rules....1008
Set Up the Private Access Rule....1019
Configure Security Control Options....1029
Geolocation Sources and Private Access Rules....1029
About Geolocation Sources....1030
Add Geolocation Sources on Private Access Rules....1030
View Events Report....1031
Filter the Report by Firewall Requests....1034
Filter the Report by Web Requests....1037
Edit a Private Access Rule....1040
About ZTA Private Access Enforcement....1040
Most Specific Match Enforcement Mode....1041
Multi-App Match Enforcement Mode....1042
Multi-App with Resolved IP Match Enforcement Mode....1044

Allowing Traffic from Users and Devices on the Network....1046
Blocking Access to Private Destinations....1047
Troubleshoot Private Access Rules....1047

30 IPS Profiles....1050
Manage IPS Profiles....1051
How IPS Works....1051
Decryption is Required for Effective Intrusion Prevention....1052
Exceptions for Traffic That Should Not be Decrypted....1052
IPS is Used in Both Types of Access Rules....1052
Add a Custom IPS Signature List....1052

31 Security Profiles....1058
Manage Security Profiles....1059
Security Profiles for Internet Access....1059
Functionality Included in a Security Profile for Internet Access....1059
Decryption....1060
SSO Authentication....1060
Security and Acceptable Use Controls....1061
End-User Notifications....1061
Get Started: Security Profiles for Internet Access....1062
Add a Security Profile for Internet Access....1062
Enable SafeSearch....1072
Confirm That SafeSearch is Working....1072
Security Profiles for Private Access....1075
Add a Security Profile for Private Access....1076

32 App Risk Profiles....1078
Manage App Risk Profiles....1079
App Risk Profile Attributes....1079
Add an App Risk Profile....1079

33 Threat Categories....1088
Manage Threat Categories....1089
Threat Category Descriptions....1089
Add a Threat Category List....1090
Dispute a Threat Categorization....1091

34 Traffic Decryption....1092
Manage Traffic Decryption....1093
Internet Access Features That Require Decryption....1093
Internet Traffic That Should Not Be Decrypted....1094

Decryption in Private Access Rules....1094
Important Information About Do Not Decrypt Lists....1095
Add a Do Not Decrypt List for Security Profiles and Internet Access....1096

35 Schedules for Access Rules....1100
Manage Schedules....1101
Add a Schedule....1101
View and Manage Schedules....1103

36 Virtual Private Networks and Proxy Settings....1110
Manage Virtual Private Networks....1111
Manage Regions and IP Pools....1111
Manage RADIUS Servers and Groups....1122
Manage VPN Profiles....1127
Import ASA Device Configuration Files for Remote Access VPN....1144
Manage Machine Tunnels....1161
Add a Machine Tunnel and Configure General Settings....1162
Authenticate Device Identity with Active Directory....1169
Migrate AD User for Machine Tunnel to Identity Endpoint....1170
Manage Application-Based Remote Access VPN (Per App VPN)....1172
Manage Custom Attributes....1173
Manage Secure Client Scripts....1185
Guidelines and Limitations....1186
Enable Secure Client Scripts....1186
Upload Secure Client Scripts....1187
Manage VPN Connection Posture Profiles....1189
Add a VPN Connection Posture Profile....1189
Manage Proxy Chaining....1194
Forwarded-For (XFF) Configuration....1195

37 Zero Trust Access....1198
Manage Client-Based Zero Trust Access in Secure Access....1199
What is ZTA and How Does it Compare to VPN?....1199
Zero Trust Access Use Cases....1200
Block Experience with ZTA....1201
Cached Block Verdict Types for ZTA....1202
Regional Static IP for Client-based ZTA for Edgev2....1202
Zero Trust Access with Captive Portal Detection....1206
Zero Trust Access Logs....1207
Zero Trust Access Requirements and Limitations....1207
Post Zero Trust Access Enrollment Action Items....1214
Pre-login and Post-login Authentication to your Cisco Secure Client....1214
Traffic Steering for Zero Trust Access Client-Based Connections....1214

Best Practices....1215
Limits: Zero Trust Traffic Steering Rules....1217
Manage the DNS Steering Rule in a Zero Trust Access Profile....1217
Add a Zero Trust Access Profile....1219
Edit a Zero Trust Traffic Rule....1224
Delete a Zero Trust Traffic Rule....1224
Enable Client-Based Zero Trust Access to Destinations....1225
Using Wildcards to Configure Traffic Steering for Private Destinations....1226
Addresses That Never Use Zero Trust Access....1227
Zero Trust Access to Internet Destinations....1228
Trusted Networks for Zero Trust Access Connections....1229
Manage Threat Defense Devices for Universal Zero Trust Network Access....1232
Manage User Trust Profile Zero Trust Access....1243
Enable User Trust Profile....1243
Bypass Untrusted User....1245
Manage Zero Trust Access Posture Profiles....1249
Add a Client-Based Zero Trust Access Posture Profile....1250
Add a Browser-based Zero Trust Access Posture Profile....1253
View a Browser-based Zero Trust Access Posture Profile....1258

38 Endpoint Security....1262
Manage Endpoint Security....1263
Endpoint Posture Assessment....1263
Endpoint Attributes....1263
View a Endpoint Posture....1267

Part IV: Security Protection and Enforcement....1270

39 Virtual Appliances....1272
Get Started with Virtual Appliances....1273
Supported Deployments....1273
How Secure Access Virtual Appliances Work....1273
Virtual Appliances and Granular Identity Information....1273
Active Directory Integration....1274
Configure Granular Rules....1274
Prerequisites for Virtual Appliances....1274
Virtual Appliance Deployment Guidelines....1277
Virtual Appliance Sizing Guide....1279
Manage VAs in Secure Access....1281
Configure Authentication for Virtual Appliances....1282
Manage DNS Forwarders....1286
Manage Site for Virtual Appliance....1290
Configure Updates for Virtual Appliances....1293

Configure Failover to Third-Party Resolvers....1296
Deploy Virtual Appliances....1299
Deploy VAs in Hyper-V for Windows 2012 or Higher....1300
Procedure for Deploying VAs in Hyper-V for Windows 2012 or Higher....1300
Deploy VAs in VMware....1311
Procedure for Deploying VAs in VMware....1311
Deploy VAs in Microsoft Azure....1315
Procedure for Deploying VAs in Microsoft Azure....1315
Deploy VAs in Amazon Web Services....1321
Procedure for Deploying VAs in Amazon Web Services....1322
Deploy VAs in Google Cloud Platform....1326
Procedure....1326
Deploy VAs in KVM....1332
Procedure for Deploying VAs in KVM....1333
Deploy VAs in Nutanix....1341
Deploy VAs in Alibaba Cloud....1343
Procedure....1344
Create a Custom Image....1349
Deploy the Secure Access VAs from the Imported Custom Image....1354
First-time Login to Secure Access VA....1358
Configure Virtual Appliances....1362
Enter Configuration Mode on a VA Deployed on VMware, Hyper-V, or KVM....1362
Enter Configuration Mode on a VA Deployed in Azure, AWS, or Google Cloud Platform....1364
Configure the VA Through Configuration Mode....1364
Configure a Second VA....1366
Configure Settings on VAs....1366
Local DNS Forwarding....1378
Manage Domains in the VA....1378
Configure Local DNS Servers on the VA....1380
Test Virtual Appliance Deployments....1381
Resolve Public and Local DNS Queries....1381
Test with Endpoints....1382
Transition Production Traffic....1383
SNMP Monitoring for Virtual Appliances....1384
Enable SNMP Monitoring....1384
Standard OIDs Supported by the Virtual Appliance....1386
Extended OIDs Supported by the Virtual Appliance....1387
Troubleshoot Virtual Appliances....1387
Use Configuration Mode to Troubleshoot....1388
Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed on Azure....1388
Troubleshoot DNS Resolution in Configuration Mode....1388
Troubleshoot DNS Resolution Failures Behind a Firewall....1389

40 File Inspection and Analysis....1390

Manage File Inspection and File Analysis....1391
Overview of Configuring File Inspection and Analysis....1391
File Inspection Details....1391
Cisco Secure Malware Analytics (formerly Threat Grid) Details....1392
Enable File Inspection....1393
Prerequisites for Enable File Inspection....1394
Procedure for Enable File Inspection....1394
Enable File Analysis by Cisco Secure Malware Analytics....1395
Prerequisites for Enable File Analysis by Cisco Secure Malware Analytics....1395
Procedure for Enable File Analysis by Cisco Secure Malware Analytics....1396
Test File Inspection for Internet Access....1397
Block Page Diagnostic Information....1398
Monitor File Inspection and Analysis Activity....1398
Monitor and Review Secure Malware Analytics....1398
Troubleshoot File Inspection and Analysis....1399

41 File Type Controls....1400
Manage File Type Controls....1401
File Types to Block....1401
Enable File Type Controls....1401
Enable File Type Blocking for Internet Access....1402
Enable File Type Blocking for Private Access....1403
Review File Type Controls Through Reports....1404

42 Notification Pages....1410
Manage Notification Pages....1411
View Notification Pages Displayed to End Users....1412
About Warn Pages for Internet Access Traffic....1413
Warn Page: Enter Key Word and Continue to Destination....1414
Preview Notification Pages....1416
System-Provided Notification Pages for Firewall and Secure Web Gateway....1418
Create Custom Block and Warn Pages....1421
Allow Users to Contact an Administrator....1425
Block Page IP Addresses....1427

43 Data Loss Prevention....1430
Manage the Data Loss Prevention Policy....1431
Best Practices for the Data Loss Protection Policy....1432
Supported File and Form Types....1433
Understand Exclusions in a Real Time Rule....1439
Supported Applications....1439
Add a Real Time Rule to the Data Loss Prevention Policy....1442
Create a DLP Real Time Rule Step 1 – Establish General Settings....1444

Create a DLP Real Time Rule Step 2 – Select Data Classifications....1445
Create a DLP Real Time Rule Step 3 – Select Files Controls....1446
Create a DLP Real Time Rule Step 4 – Select Identities....1453
Create a DLP Real Time Rule Step 5 – Select Destinations for Inclusion....1454
Create a DLP Real Time Rule Step 6 – Select Destinations for Exclusion....1462
Create a DLP Real Time Rule Step 7 – Select the Rule Action....1466
Create a DLP Real Time Rule Step 8 – Disable/Enable Payload Transmission for DLP Violations (ICAP Only)....1468
Create a DLP Real Time Rule Step 9 – Enable and Configure Pop-Up Notifications for Violations....1469
Create a DLP Real Time Rule Step 10 – Enable and Configure Email Notifications for Violations....1472
Add a SaaS API Rule to the Data Loss Prevention Policy....1478
Create a DLP SaaS API Rule Step 1 – Establish General Settings....1479
Create a DLP SaaS API Rule Step 2 – Select Data Classifications....1479
Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant....1481
Create a DLP SaaS API Rule Step 4 – Select Files Controls....1482
Create a DLP SaaS API Rule Step 5 – Select Users....1490
Create a DLP SaaS API Rule Step 6 – Select Resource Labels....1494
Create a DLP SaaS API Rule Step 7 – Select Resources....1495
Create a DLP SaaS API Rule Step 8 – Configure Exposure Settings....1497
Create a DLP SaaS API Rule Step 9 – Select Action....1500
Create a DLP SaaS API Rule Step 10 – Enable and Configure Email Notifications....1509
Add an AI Guardrails Rule to the Data Loss Prevention Policy....1514
Create a DLP AI Guardrails Rule Step 1 – Establish General Settings....1515
Create a DLP AI Guardrails Rule Step 2 – Select Data Classifications....1516
Create a DLP AI Guardrails Rule Step 3 – Select Files Controls....1517
Create a DLP AI Guardrails Rule Step 4 – Select Identities....1522
Create a DLP AI Guardrails Rule Step 5 – Select Destinations....1523
Create a DLP AI Guardrails Rule Step 6 – Select the Rule Action....1524
Create a DLP AI Guardrails Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations....1525
Create a DLP AI Guardrails Rule Step 8 – Enable and Configure Email Notifications for Violations....1527
Integrate Email Threat Defense with Secure Access DLP....1532
Add an Email Rule to the Data Loss Prevention Policy....1533
Create a DLP Email Rule Step 1 – Establish General Settings....1534
Create a DLP Email Rule Step 2 – Select Data Classifications....1535
Create a DLP Email Rule Step 3 – Select Files Controls....1536
Create a DLP Email Rule Step 4 – Select the Senders....1540
Create a DLP Email Rule Step 5 – Select the Recipients....1543
Create a DLP Email Rule Step 6 – Select the Rule Action....1546
Create a DLP Email Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations....1547
Create a DLP Email Rule Step 8 – Enable and Configure Email Notifications for Violations....1549
Discovery Scan....1553
Initiate a Discovery Scan....1554
Cancel a Discovery Scan....1556
Edit a Data Loss Prevention Rule....1558

Delete a Data Loss Prevention Rule....1558
Enable or Disable a Data Loss Prevention Rule....1559
Disable a Rule....1560
Enable a Rule....1560
Manage Global Settings....1561

44 Secure Browser Extension....1564
Secure Browser Extension 1565
Manage the Secure Browser Extension....1565
Install the Cisco Secure Browser Extension....1565
Onboarding and Activation....1568
Configure Browser Policy....1570
Content Agnostic Browser Control Profile....1573
Content-Aware Real Time DLP rule....1573
Browser Action Protection Enforcements....1574
View Reports....1575

45 Data Classifications....1576
Manage Data Classifications....1577
Create a Data Classification....1578
Procedure for Creating a Data Classification....1579
Copy and Customize a Built-In Data Classification....1586
HIPAA Data Classification....1586
Procedure for Copy and Customize a Built-In Data Classification....1588
Delete or Edit a Classification....1597
Delete a Classification....1597
Edit a Classification....1598
Exact Data Match Identifiers....1599
Prerequisites for Exact Data Match Identifiers....1599
Create an Exact Data Match Identifier....1600
Index Data for an EDM....1605
Exact Data Match Field Types....1610
Indexed Document Match Identifiers....1611
Limitations....1612
Create an Indexed Document Match Identifier....1613
Monitor the Indexed Data Set and Re-Index as Needed....1617
Troubleshooting....1618
Built-In Data Classifications....1618

46 Built-in Data Identifiers....1636
Built-in Data Identifiers....1637
Tolerances....1637
Copy and Customize a Data Identifier....1638

Create a Custom Identifier....1641
Custom Regular Expression Patterns....1645
Individual Data Identifiers....1646

47 AI Guardrails Data Classifications....1648
AI Guardrails Data Classifications....1649

48 Secure ICAP....1650
Manage Secure ICAP....1651
Secure ICAP Integration....1651
Modify an ICAP Server Connection....1653
Disconnect from an ICAP Server....1654

49 Requirements for Salesforce Tenants....1656
Requirements for Salesforce Tenants for Cloud Malware and SaaS API DLP....1657
Salesforce sObjects Supported for SaaS API DLP....1657
Install or Update `Node.js`....1659
Install the Salesforce CLI....1660
Deploy the Salesforce Quarantine Package to your Salesforce Tenant....1660
Log In to Your Salesforce Org....1662
Set Permissions in Salesforce....1663

50 SaaS API Data Loss Prevention....1668
Manage SaaS API Data Loss Prevention....1669
Enable SaaS API Data Loss Prevention for AWS Tenants....1670
Enable CloudTrail Event Logging for S3 Buckets and Objects....1670
Obtain Your AWS Account ID....1671
Authorize an AWS Tenant....1672
Create an AWS Stack....1675
Revoke Authorization....1678
Enable SaaS API Data Loss Prevention for Azure Tenants....1678
Authorize an Azure Tenant....1679
Run an Azure PowerShell Script to Obtain Account Information....1681
Revoke Authorization....1681
Enable SaaS API Data Loss Prevention for Box Tenants....1682
Authorize a Tenant....1682
Revoke Authorization....1685
Enable SaaS API Data Loss Prevention for Confluence Tenants....1686
Enable SaaS API Data Loss Prevention for Dropbox Tenants....1689
Authorize a Tenant....1689
Revoke Authorization....1692
Enable SaaS API Data Loss Prevention for GitHub Tenants....1693
Authorize a Tenant....1694

Install the GitHub connector....1696
Verify Cisco Secure Access for GitHub app integration....1700
Revoke Authorization....1701
Enable SaaS API Data Loss Prevention for Google Drive Tenants....1701
Validation....1702
Authorize a Tenant....1702
Revoke Authorization....1704
Enable SaaS API Data Loss Prevention for Jira Tenants....1705
Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants....1707
Prerequisites for Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants....1708
Authorize a Microsoft 365 Tenant....1709
Revoke Authorization....1711
Enable SaaS API Data Loss Prevention for Salesforce Tenants....1712
Enable SaaS API Data Loss Prevention for Salesforce Commerce Tenants....1717
Enable SaaS API Data Loss Prevention for ServiceNow Tenants....1721
Find the Instance Name for your ServiceNow admin Account....1721
Assign the oauth_user role to the ServiceNow admin Account....1722
Add an OAuth Client to Your ServiceNow Deployment....1723
Authorize a Tenant....1723
Revoke Authorization....1725
View the Cisco Quarantine Table in Service Now....1726
Enable SaaS API Data Loss Prevention for Slack Tenants....1727
Authorize a Tenant....1727
Revoke Authorization....1730
Enable SaaS API Data Loss Prevention for Webex Teams....1731
Authorize a Tenant....1731
Revoke Authorization....1733

51 Cloud Malware Protection....1736
Manage Cloud Malware Protection....1737
Enable Cloud Malware Protection....1739
Revoke Authorization for a Platform....1741
Enable Cloud Malware Protection for AWS Tenants....1744
Enable CloudTrail Event Logging for S3 Buckets and Objects....1745
Obtain Your AWS Account ID....1745
Authorize an AWS Tenant....1746
Create an AWS Stack....1749
Revoke Authorization....1751
Enable Cloud Malware Protection for Azure Tenants....1752
Authorize an Azure Tenant....1752
Run an Azure PowerShell Script to Obtain Account Information....1755
Revoke Authorization....1756
Enable Cloud Malware Protection for Box Tenants....1756
Verify Box Application Settings....1757

Authorize a Tenant....1757
Edit a Tenant....1763
Revoke Authorization....1767
Enable Cloud Malware Protection for Confluence Tenants....1768
Enable Cloud Malware Protection for Dropbox Tenants....1772
Authorize a Tenant....1772
Edit a Tenant....1777
Revoke Authorization....1783
Enable Cloud Malware Protection for GitHub Tenants....1783
Authorize a Tenant....1784
Revoke Authorization....1788
Enable Cloud Malware Protection for Jira Tenants....1789
Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants....1792
Prerequisites for Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants....1792
Authorize a Tenant....1793
Edit a Tenant....1800
Revoke Authorization....1806
Enable Cloud Malware Protection for Salesforce Tenants....1806
Edit a Salesforce Cloud Malware Tenant....1812
Enable Cloud Malware Protection for ServiceNow Tenants....1815
Find the Instance Name for your ServiceNow admin Account....1816
Assign the oauth_user role to the ServiceNow admin Account....1817
Add an OAuth Client to Your ServiceNow Deployment....1818
Authorize a Tenant....1818
Edit a Tenant....1824
Revoke Authorization....1828
View the Cisco Quarantine Table in Service Now....1829
Enable Cloud Malware Protection for Slack Tenants....1830
Authorize a Tenant....1830
Edit a Tenant....1834
Revoke Authorization....1836
Enable Cloud Malware Protection for Webex Teams....1836
Authorize a Tenant....1836
Revoke Authorization....1839
Cloud Access Security Broker Protection for Google Drive and Microsoft 365....1840
Enable Cloud Access Security Broker Features for Google Drive....1840
Authorize a Tenant....1841
Edit a Tenant....1848
Revoke Authorization....1854

52 Remote Browser Isolation....1856
Get Started with Remote Browser Isolation....1857
Manage Remote Browser Isolation Profiles....1857
System Default Profile....1857

Create a Remote Browser Isolation Profile....1858
Edit or Delete a Remote Browser Isolation Profile....1860
Remote Browser Isolation Advanced Isolation Controls Reference....1860
Watermarking....1860
Copy, Paste and Keyboard Control....1861
Document Isolation....1861
File Transfers....1862

53 Internet Security....1864
Manage Internet Security....1865
Set Up Internet Security on User Devices....1865
Manage Internet Security Bypass....1867
Configure Cisco Secure Client Settings....1873

54 PAC Files....1880
Manage PAC Files....1881
Requirements for Downloading PAC Files to User Devices....1881
About Using the Secure Client with PAC Files....1881
Managing PAC File Deployments....1881
Deploy the Secure Access PAC File for Windows....1882
Deploy the Secure Access PAC File for macOS....1885
Customize the Secure Access PAC File....1888
Upload Custom PAC Files to Secure Access....1891
Manage Uploaded Custom PAC Files....1894

55 Certificates....1896
Manage Certificates....1897
Certificate Installation Methods....1897
Certificates for Internet Decryption....1897
Certificates for Decrypting Internet Traffic....1898
Manage Certificates for Private Resource Decryption....1899
Install a Certificate Authority Certificate on a Private Resource....1899
Upload Private Resource Certificates....1899
View Notifications About Expired Private Resource Certificates....1900
View, Delete, or Replace a Private Resource Certificate....1901
Install the Cisco Secure Access Root Certificate....1902
Download the Cisco Secure Access Root Certificate....1903
Automatically Install the Cisco Secure Access Root Certificate (For an Active Directory Network)...1903
Install the Cisco Secure Access Root Certificate in Firefox Using Group Policy....1905
Install the Cisco Secure Access Root Certificate on Chromebooks Using the Google Admin Console....1905
Manually Install the Cisco Secure Access Root Certificate (Single Computer)....1905
Add Custom CA Signed Root Certificate....1908

Certificate Requirements....1908
Install Root Certificate in Browsers....1909
Adding a Custom CA Signed Root Certificate....1909
Renew the Custom CA Signed Root Certificate....1911
View the Cisco Trusted Root Store....1912
Extract the Certificates....1913
View an Individual Certificate File....1914
Certificates for SAML Authentication....1914
Manage SAML Certificates for Service Providers....1914
Manage SAML VPN Service Provider Certificate Rotation....1917
Manage SAML Certificates for Identity Providers....1919
VPN Certificates for User and Device Authentication....1921
Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment....1921
View Notifications About Expired CA Certificates for Client Authentication....1922
Upload Certificate Authority (CA) Certificates for client authentication....1922
View Uploaded CA Certificates....1923
Manage Certificate Revocation Settings....1924
View CA Certificate Details....1925
Change the Purpose of an Uploaded CA Certificate....1927
Delete a Client Authentication CA Certificate....1927

56 Secure Access Investigate....1930

Manage Secure Access Investigate....1931
Getting Started with Investigate....1931
About Passive DNS....1936
About Investigate View Types....1936
About the Investigate Domain Summary....1936
Domain Summary Details....1937
Investigate Domain Risk Score....1937
Keyword Score....1938
Lexical Score....1938
TLD Score....1938
Geo Popularity....1939
About Investigate Passive DNS Timeline....1939
Dispute Content Categorization....1940
About DNS Resolution in Investigate....1941
About Associated Samples in Investigate....1942
About the Subdomains Tab in Investigate....1944
About Related Domains in Investigate....1944
About the Geographic Distribution View in Investigate....1945
About the Sample View in Investigate....1946
About the IP Address View in Investigate....1948
About WHOIS Record Information....1951
About the WHOIS Nameserver View....1953

FAQs....1955
About the ASN View....1956
Current Information....1956
Current Routes....1957
Research AS From IP Address View....1957

Part V: Mobile Device Management....1960

57 Client-based Zero Trust Access from Mobile Devices....1962
Get Started and Manage Client-based Zero Trust Access from Mobile Devices....1963
Set up the Zero Trust Access App for iOS Devices....1963
Guidelines and Limitations....1963
Configure iOS Settings....1964
Install the App....1964
Have End Users Enroll in Zero Trust Access....1965
Notes for administrators....1965
Set up the Zero Trust Access App for Android Devices....1965
Configure Cisco Secure Access....1966
Install the App....1966
Notes for administrators....1966
Set up the Zero Trust Access App for Android on Samsung Devices....1966
Configure Android Settings in Secure Access....1967
Install the App....1967
(Optional) Set up the Android device for Zero Trust Access using MDM....1968
Enroll the Device in Zero Trust Access....1970
Notes for administrators....1971
Monitor and Troubleshoot the Zero Trust Access App from Mobile Devices....1971
Troubleshoot iOS Devices....1972
Troubleshoot Samsung Devices Running Android OS....1972
Troubleshoot access issues....1972

58 Cisco Secure Client on Windows, macOS, and Linux Devices....1974
Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices....1975
Windows, macOS, and Linux Device Prerequisites....1975
Download and Install Cisco Secure Client....1976
ThousandEyes Endpoint Agent Module....1979
Download the OrgInfo.json File....1980
Manual Installation of Cisco Secure Client (Windows and macOS)....1981
Mass Deployment Overview....1982
Customization Options....1983
Mass Deployment (Windows)....1984
Customize Windows Installation of Cisco Secure Client....1987
(Optional) OrgInfo.json Parameter Configurations....1988

Mass Deployment (macOS)....1989
Customize macOS Installation of Cisco Secure Client....1993
Step 1 – Make the .dmg Package Writeable....1993
Step 2 – Generate the Module Installation Configuration File....1993
Step 3 – Copy OrgInfo.json to Cisco Secure Client Installation Directory....1994
Step 4 – (Optional) Hide the VPN Module....1994
Step 5 – Customize the Cisco Secure Client Installation Modules....1994
Sample Customization....1995
Step 6 – Set Up the Correct Extension Permission Settings....1999
Step 7 – Install Secure Client with Selected Modules....2000
Optional OrgInfo.json Parameter Configurations....2000
VPN Headend Deployment....2001
Secure Firewall Management Center and Secure Firewall Threat Defense....2002
Procedure to enable Secure Client Secure Access Module in Management Center and Threat Defense....2002
(OPTIONAL) VPN Local Authentication (Management Center 7.0 or later required)....2005
Meraki Systems Manager (SM) Deployment....2006
Migration from Secure Access Roaming Client....2007
Install the Root Certificate for All Browsers....2007
Cloud Management....2007
Deploying Cisco Secure Client....2008
Uploading the Orginfo.json profile....2009
Create a Deployment....2011
Post Deployment....2014
Additional References....2016
Manage Device Deployment....2017
Prerequisites for Device Deployment Management....2017
Add and Activate Deployment Key....2018
Manage Deployment Key Compromise....2020
Delete a Deployment Key....2021
Reverting to Using Legacy Deployment Implementation....2022
Backward Compatibility....2022

59 Zero Trust Access using Cisco Secure Client....2024
Manage Zero Trust Access using Cisco Secure Client....2025
Enroll Devices in Zero Trust Access Using Certificates....2026
Enroll Devices in Zero Trust Access Using SSO Authentication Overview....2029
Troubleshoot Client-Based Zero Trust Access....2031
Unenroll a Device from Zero Trust Access....2033

60 Endpoint Data Loss Prevention using Cisco Secure Client....2040
Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac....2041
Prerequisites for Endpoint Data Loss Prevention....2042
Enroll Devices in Endpoint Data Loss Prevention Using Certificates....2043

Troubleshoot Endpoint Data Loss Prevention for Windows....2050
Troubleshoot Endpoint Data Loss Prevention for Mac....2053
Extract and Stream Logs for Cisco Secure Client - Endpoint DLP on macOS....2055
Logging with the Console Application....2057
Troubleshoot Endpoint Data Loss Prevention for Linux....2058
Deploying Cisco Secure Client – Endpoint DLP on macOS using a generic MDM....2059
Grant Required Privacy Permissions Using MDM....2059
Uninstall Cisco Secure Client - Endpoint DLP on macOS....2060
Uninstall Cisco Secure Client Endpoint DLP on Linux....2061

61 Virtual Private Networks on Cisco Secure Client....2062
Manage Virtual Private Networks on Cisco Secure Client....2063
Prerequisites....2063
Download the Virtual Private Network XML Profile....2063
CA Certificates for VPN Connections....2064

62 Internet Security on Cisco Secure Client....2066
Manage Internet Security on Cisco Secure Client....2067
Umbrella Roaming Security Module Requirements....2067
Domain Management....2070
Interpret Internet Security Diagnostics....2071
Procedure....2072
DNS Protection Status....2073
View DNS Protection Status....2073
SWG Protection Status....2075
View SWG Protection Status....2076

63 Endpoint Diagnostic Tool....2078
Cisco Endpoint Diagnostic Tool....2079

64 Managed iOS....2088
Cisco Security Connector: Secure Access Setup Guide....2089
Requirements....2089
Getting Started....2091
Quick Start....2091
Manage Device Deployment....2097
Meraki Registration....2101
Anonymization....2101
Register with Meraki....2101
Verify Secure Access with Meraki....2107
Meraki Documentation....2116
Register an iOS Device Through Apple Configurator 2....2117
Procedure for Registering an iOS Device Through Apple Configuration 2....2117

Verify Secure Access on Your Device....2119
IBM MaaS360 Registration....2120
Procedure for Registering IBM MaaS360 MDM Solution....2121
Verify Secure Access on Your iOS Device....2123
Intune Registration....2124
Procedure for Registering Intune MDM Solution....2124
Verify Secure Access on Your iOS Device....2126
Jamf Registration....2127
Procedure for Registering Jamf MDM Solution....2127
Anonymization....2130
Verify Secure Access on Your iOS Device....2130
MobileIron Registration....2131
Procedure for Registering MobileIron MDM Solution....2132
Verify Secure Access on Your iOS device....2134
MobileIron Configuration....2135
MobiConnect Registration....2136
Procedure for Registering MobiConnect MDM Solution....2137
Verify Secure Access on Your iOS Device....2140
Workspace ONE Registration....2140
Procedure....2141
Verify Secure Access on Your iOS Device....2143
Register an iOS Device Through a Generic MDM System....2144
Register the iOS Device Through a Generic MDM System....2145
Verify That Your Device is Protected by Secure Access....2147
Apply an Access Policy to Your Mobile Device....2148
Add User Identity for Cisco Security Connector....2150
Test Integration of User Identity With Cisco Security Connector....2152
Anonymize Devices....2152
Export Device Data to CSV....2153
Procedure....2154
DNS Protection Status in Exported Reports....2155
SWG Protection Status in Exported Reports....2156
Push the Cisco Root Certificate to Managed Devices....2156
Configure Cellular and Wifi Domains....2157
Configuring DNS Suffix Allow List....2158
Troubleshooting....2159
Generate Diagnostics and Email the Secure Access Reports....2159
Generate Diagnostics and Share the Secure Access Reports....2160

65 Managed Android....2162
Secure Access Module for Cisco Secure Client (Android OS)....2163
Device Security....2163
Prerequisites....2163
Deploy the Android Client....2165

Android Configuration Download....2165
Manage Device Deployment....2168
Cisco Meraki MDM....2172
MobileIron MDM....2177
VMware Workspace ONE....2180
Microsoft Intune MDM....2192
Samsung Knox MDM....2198
Push the Cisco Root Certificate to Devices....2203
Manage Identities....2204
Cisco Meraki Systems Manager....2205
Microsoft Intune....2206
Samsung Knox....2208
VMWare WorkspaceOne....2209
Access User Identities on the Secure Access Dashboard....2210
Export Device Data to CSV....2212
Procedure....2212
DNS Protection Status in Exported Reports....2213
SWG Protection Status in Exported Reports....2214
Troubleshooting....2215
Known Issues....2215
First Launch of App....2215
Is this a VPN to Secure Access?....2216
An Internal Site Isn't Loading....2217
Configuration Issues....2217
Check for VPN Connection and Policy....2218
Check Block Page....2219
Get the Android ID....2219
Fail Close/Open Scenario....2220
Check Device Registration....2221
Missing CA Certificate....2221
Org ID on Policy Page is 0....2222
App Installation is Blocked....2222
Offboarding Users....2222
Frequently Asked Questions about Managed Android....2222

66 Unmanaged Mobile Devices....2226
Unmanaged Mobile Device Protection....2227
Administrator Actions....2227
End-user Actions....2229

Part VI: Monitor and Report....2236

67 Experience Insights....2238

About Experience Insights....2239
Onboard Experience Insights....2240
Cisco AI Assistant for Experience Insights....2245
How to Use the Cisco AI Assistant in Experience Insights....2245
Prompt examples....2246
Contextual Conversations....2246
ThousandEyes Account Management in Experience Insights....2247
Edit Default Test Target....2249
Register ThousandEyes Agents....2251
Experience Insights Overview....2253
Endpoints....2257
Wi-Fi Descriptions....2258
Experience Score....2259
View SaaS Application Performance....2262
View User Dashboard....2264
View the User Dashboard....2269
Configure Identity Providers for Experience Insights....2269
About Endpoint Agent Tests....2270
Manage endpoint tests in Secure Access....2271
Manage endpoint agents and tests in ThousandEyes....2272
Limitations....2272
Estimate Peak Traffic to Custom Targets for Default Endpoint Tests....2273
Create HTTP Server Tests....2274
Create Network Tests....2277
View HTTP server test results....2279
View Network Test Results....2281

68 Logging....2284

Manage Logging....2285
Enable Logging on a Rule in Access Policy....2286
Enable Logging to Your Own S3 Bucket....2287
Enable Logging of DLP Violation Evidence to Your Own S3 Bucket....2290
Enable Logging to a Cisco-Managed S3 Bucket....2296
Change the Location of Event Data Logs....2301
Log export failures to Amazon S3....2303
Stop Logging....2304
Delete Logs....2304
Log Formats and Versioning....2305
Log File Name Formats....2305
Reports and CSV Formats....2311
Admin Audit Log Formats....2315
Cloud Firewall Log Formats....2317
Data Loss Prevention (DLP) Log Formats....2321
DNS Log Formats....2324

File Events Log Formats....2326
IPS Log Formats....2329
Network Connectivity Log Formats....2332
Remote Access VPN Log Formats....2334
Web Log Formats....2339
Zero Trust Access Log Formats....2344
Zero Trust Access Flow Log Formats....2349
Zero Trust Access Enrollment Log Formats....2353

69 Monitor with Alert Rules....2356
Monitor Secure Access with Alert Rules....2357
Manage Alert Rules....2357
Add and Edit Alert Rules for API Anomalies....2359
Add and Edit Alert Rules for Changes on Access Rules....2363
Add and Edit Alert Rules for Behavior Analytics....2367
Add and Edit Alert Rules for Tunnel Connectivity....2372
Add and Edit User Access Alerts....2376
Add and Edit Alert Rules for Resource Connectors....2378
Manage Alert Rules for Destination Lists....2382
Monitor Alerts from Secure Access....2389
Splunk Integration: Configure Alert Rules for Access Policy Changes....2390
ServiceNow Integration: Configure Alert Rules for Access Policy Changes....2390

70 Monitor with Reports....2392
Monitor Secure Access with Reports....2393
Available Reports....2393
Export Report Data to CSV....2393
Bookmark and Share Reports....2395
Report Scheduling....2396
Schedule a Report....2397
Update a Scheduled Report....2400
Report Search Window and Retention....2401
Report Search Window....2402
Report Retention....2402
Assess and Monitor Configurations in Secure Access....2403

71 Activity Reports....2408
Activity Search Report....2409
View and Customize the Activity Search Report....2409
View Firewall Events in Activity Search Report....2421
View Web Events in Activity Search Report....2424
View Zero Trust Events in Activity Search Report....2427
View AI Semantic Inspection Events in Activity Search Report....2431

View Activity Search Report Actions....2432
Schedule an Activity Search Report....2437
Use Search and Advanced Search....2438
Security Activity Report....2442
View Activity and Details by Filters....2442
View Activity and Details by Event Type or Security Category....2445
View an Event's Details....2448
Search for Security Activity....2450
Activity Volume Report....2452
View Requests by Volume of Activity....2453
View Activity Volume by Threat Categories....2454
View Activity Volume by Policy Traffic....2455
View Trends....2455

72 Admin Audit Log Report....2456
Admin Audit Log Report....2457
Generate Admin Audit Log Report....2457
Export Admin Audit Log Report to an S3 Bucket....2458

73 AI Related Reports....2460
AI Supply Chain Report....2461
AI Semantic Inspection Report....2462
View AI Semantic Inspection Report....2464

74 App Related Reports....2468
App Discovery Report....2469
View the App Discovery Report....2469
View the Highest Risk Apps....2472
Review Apps in the Apps Grid....2473
View App Details....2479
Change App Details....2483
Control Apps....2487
Control Advanced Apps....2489
View Traffic Data Through SWG Service....2491
Third-Party Apps Report....2495
View the Third-Party Apps Report....2495
Search the Third-Party Apps Report....2498
Export the Third-Party Apps Report....2499
View App Details....2500

75 Cloud Malware Report....2504
Cloud Malware Report....2505
View the Cloud Malware Report....2505

Use the Cloud Malware Report....2507

76 Data Loss Prevention Report....2516

Data Loss Prevention Report....2517

View Events....2517

Discovery....2538

77 Data Security Posture Management Report....2542

Overview....2543

Data Catalogue....2544

Insights....2547

Analytics....2549

78 Events Report....2552

Events Report....2553

Key Features of Events Report....2554

View Events Report....2554

Event Type Specific Details....2557

View Browser-based ZTA Flow Events....2560

Schedule an Events Report....2561

Saving a Search in the Events Report....2561

Customize and Manage Saved Searches....2563

Filter Events Using Basic Search Options....2563

Filter Events Using Advanced Search....2564

Known Limitations....2565

79 Network Connectivity Monitoring....2568

Network Connectivity Monitoring....2569

Network Tunnel Logs....2569

Resource Connector Logs....2571

80 Network Tunnel Group Usage Report....2576

Network Tunnel Group Usage....2577

View Top Network Tunnel Groups by Traffic....2579

81 Remote Access Log Report....2584

About the Remote Access Log Report....2585

View the Remote Access Log Report....2586

View Zero Trust Access Events in the Remote Access Log....2590

Schedule a Remote Access Log Report....2592

82 Top Categories Report....2594
Top Categories Report....2595
View the Top Categories Report....2595
Top Categories Quick View....2597
View Category in Other Reports....2597
Category Details....2598

83 Top Destinations Report....2604
Top Destinations Report....2605
View the Top Destinations Report....2605
View Further Details....2608
Destination Details....2608

84 Total Requests Report....2614
Total Requests Report....2615
View Trends in the Total Requests Report....2615

Part VII: Integrations....2620

85 Secure Access Integrations....2622
Manage Third-Party Integrations....2623
Additional Secure Access Integration Guides....2623
Chrome Enterprise Browser....2623
Configure the Chrome Enterprise Browser Third-Party Integration....2624
Microsoft Intune Third-Party Integration....2626
Configure the Microsoft Intune Third-Party Integration....2626
Jamf Pro Third-Party Integration....2627
Configure the Jamf Pro Third-Party Integration....2627
Push Security Events Third-Party Integration....2628
Add Third-Party Integrations for Push Security Events....2629
View Third-Party Integrations for Push Security Events....2631
Edit a Third-Party Integration for Push Security Events....2633
Delete a Third-Party Integration for Push Security Events....2635
Splunk Integration: Configure Push Security Events....2635
ServiceNow Integration: Configure Push Security Events....2636
Microsoft Edge for Business Third-Party Integration....2637
Add Third-Party Integration for Microsoft Edge for Business....2637
View Third-Party Integration for Microsoft Edge for Business....2639
Edit a Third-Party Integration for Microsoft Edge for Business....2641
Island Enterprise Browser Third Party Integration....2643
Add a Third-Party Integration for Island Enterprise Browser....2643

Edit a Third-Party Integration for Island Enterprise Browser....2643
Delete a Third-Party Integration for Island Enterprise Browser....2644
Threat Intelligence Feeds....2644
Add Third-Party Integrations for Threat Intelligence Feeds....2646
View Integrated Threat Intelligence Feeds....2647
Edit or Delete a Threat Intelligence Feed....2649
Manage Webhooks for Third-Party Integrations....2650
Add a Webhook for a Third-Party Integration....2651
View Details for Webhooks....2652
Edit a Webhook for a Third-Party Integration....2653
Delete a Webhook for a Third-Party Integration....2655
Integrate ISE (Identity Services Engine) with Secure Access....2655
Solution Overview....2656
Security Group Tags....2656
Components and Prerequisites....2657
Solution Workflow....2658
Connect Cisco ISE and Cisco pxGrid Cloud....2658
Enable Cisco Security Cloud Exchange....2659
Integrate Cisco ISE with Secure Access....2661
Verify and Monitor Context Sharing....2666
Integrate Catalyst SD-WAN with Secure Access....2669
Solution Overview....2669
Components and Prerequisites....2670
Solution Workflow....2671
Configure Context Sharing Between Catalyst SD-WAN and Secure Access....2671
Verify and Monitor Context Sharing....2674
Integrate Cisco Identity Intelligence with Secure Access....2677
Configure a New Duo and Cisco Identity Intelligence Tenant with Secure Access....2678
Configure an Existing Duo and Cisco Identity Intelligence Tenant with Secure Access....2680
After Integrating Cisco Identity Intelligence....2683
Integrate Cisco SASE with Meraki SD-WAN....2685

86 Cisco Security for Chromebook Client....2690
About Cisco Security for Chromebooks....2691
Key benefits....2691
Prerequisites for Cisco Security for Chromebooks Client....2691
Limitations for Cisco Security for Chromebooks....2692
Integrate the Google Workspace Identity Service....2693
Limitations....2694
Integrate the Google Workspace Identity Service....2694
Deploy the Cisco Security for Chromebooks Client....2697
About DNS-Layer Protection....2697
About SWG-Layer Protection....2697
High-Level Steps for Deploying Cisco Security for Chromebook Client....2697

Bypass Internal Domains from DNS-over-HTTPS (DoH)....2704
Enable Reporting for the Private IP Address of a Chromebook Device....2706
Verify Cisco Security for Chromebooks Client Deployment....2708
Export Device Data to CSV....2710
Manage Device Deployment....2713
Troubleshoot Cisco Security for Chromebooks Client Deployment....2717
View Protection Status of Chromebook Devices....2718
Procedure....2718
Add Policies to a Chromebook Device....2719
Procedure....2719
Cisco Security for Chromebooks Client FAQ....2720
Google Workspace Identity Service FAQ....2721

Part I

Getting Started and Onboarding

Topics:

- Introduction to Secure Access
- Secure Access Dashboards
- Cisco Assistant for Secure Access
- Regions
- Network Requirements
- Secure Access Onboarding
- Basic Network Setup

Getting started with Secure Access.

1 Introduction to Secure Access

Topics:

- Welcome to Cisco Secure Access
- Secure Access Single Sign-On Authentication
- Find Your Organization ID
- Determine Your Current Package
- Limitations and range limits
- Endpoint Data Center Selection

Provides an overview of Secure Access, including Welcome to Cisco Secure Access, Sign into Secure Access with Security Cloud Sign On, and Find Your Organization ID. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Provides an overview of Secure Access.

Welcome to Cisco Secure Access

Describes Welcome to Cisco Secure Access. Secure Access is Cisco's cloud-based platform that provides you with multiple levels of defense against internet-based threats.

Secure Access is Cisco's cloud-based platform that provides you with multiple levels of defense against internet-based threats. Connect securely to the internet, SaaS apps, and your private digital resources, whether you connect from your organization's network or roaming off a network.

Apply and enforce comprehensive security controls on collections of resources, users, and devices. The Secure Access policy is a container for your security configuration rules. Organize your policy rules to protect your users and permit access to resources. The policy manages the connections and resources for users and devices in your organization, and the network components that forward traffic to resources.

Secure Access collates various reports and logs. The Secure Access Overview dashboard and Security Activity report show snapshots of user and device traffic and connection events over distinct time periods. You can audit digital behaviors and observe top network and security activities in your organization.

After procuring your Secure Access license, you will receive an email with a claim code, activate the Secure Access subscription through Cisco Security Cloud Control. Follow the procedure provided in the Security Cloud Control guide.

Sign into Secure Access

After you receive an invitation to log into Secure Access, set up the accounts for the users in your organization and configure network connections. For more information, see Sign into Secure Access.

Find Your Organization

Locate the organization ID for your account. For more information, see Find Your Organization ID.

Determine Your Current Package

View information about your package. For more information, see Determine Your Current Package.

Contact Support

You can reach support for Secure Access by contacting Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Secure Access Single Sign-On Authentication

Provides an overview for Secure Access Sign On workflow in Cisco Secure Access.

Cisco Secure Access supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access console. An administrator signs in to Secure Access from Cisco Security Cloud Sign On (SCSO). Cisco Duo Security or the IdP that you integrated with Security Cloud Sign On provides single sign-on (SSO) authentication of Secure Access administrators through SCSO. For more information, see Cisco Security Cloud Sign On Identity Provider Integration Guide.

To sign in to Secure Access, an administrator must have a Secure Access account and configure single sign-on authentication in SCSO. A Secure Access administrator signs in to SCSO authenticates to the IdP, and then automatically signs in to Secure Access.

Any changes made in your organization's SAML identity provider (IdP) are synced with Secure Access. If you update an account or change a password in the IdP, the changes are immediately reflected in your login. Only the username (email address) is stored in Secure Access. You must sign in to Secure Access with the same email address that you configured in your SCSO account. For more information, see Getting Started Guide for New Customers of Security Cloud Control.

> **Note**
>
> You can only use SCSO to authenticate your login to Secure Access. The IdP that you set up in SCSO does not authorize an administrator's permissions to read, create, or update resources on Secure Access. A Secure Access role defines the permissions on the Secure Access account. For more information about user roles, see Manage Accounts.

Add Your Organization's Identity Provider in Security Cloud Sign On

You can add an SAML identity provider (IdP) in SCSO for Secure Access. Once you add an IdP and provision user accounts in Security Cloud Sign On, administrators in your organization are not required to complete the **Sign Up Now** steps. For more information, see Cisco Security Cloud Sign On Identity Provider Integration Guide.

Add Administrators to Secure Access

A Cisco Secure Access administrator can add additional administrators to their Secure Access organization (Org) and assign a role to the new administrator's account. To establish an account, provide the email address of the new administrator and choose the Secure Access role for the account. For more information, see Manage Accounts.

When an administrator provisions a Secure Access account, an email is sent from Secure Access to the new administrator with the instructions to use SSO authentication to sign in to their Secure Access Org.

The new administrator has a Secure Access account and must create an SSO account through the Security Cloud Sign On (SCSO) portal. The email address in the Secure Access account must match the email address entered to create the SCSO account. The SCSO portal manages SSO authentication through an integrated IdP.

Sign into Secure Access with Security Cloud Sign On

Provides instructions for completing the Sign into Secure Access with Security Cloud Sign On workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access supports Security Assertion Markup Language (SAML) for authenticating administrators to the Secure Access console. Administrators sign in to Secure Access using their Cisco Security Cloud Sign On (SCSO). Cisco Duo Security provides single sign-on (SSO) authentication of Secure Access administrators through SCSO.

Sign in to Secure Access through the Cisco Security Cloud Sign On (SCSO) portal. If you do not have an SCSO account, follow the steps to Configure Single Sign-On Authentication.

Before you begin

- A valid Secure Access account. For more information, see Manage Accounts.

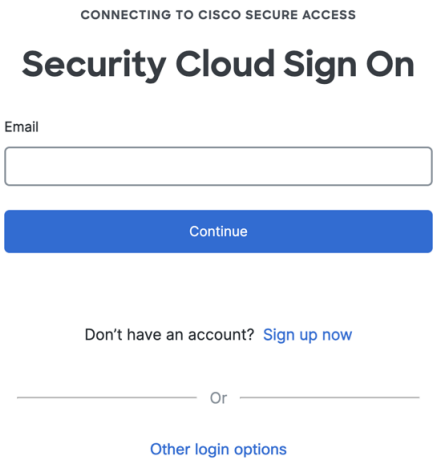
Procedure

1. Navigate to your Secure Access organization at https://dashboard.sse.cisco.com/org/<*org_number*>.

   Secure Access uses single sign-on authentication through **Security Cloud Sign On**.

2. In **Security Cloud Sign On**, enter the email address where you received the invitation to join a Secure Access organization.

   Your Secure Access account and the SCSO account must use the same email address.



3. If you have a Security Cloud Sign On account, click **Continue** to sign in to Secure Access.

Configure Single Sign-On Authentication

Provides instructions for completing the Configure Single Sign-On Authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure SSO authentication for Secure Access through Cisco Security Cloud Sign On (SCSO).

Cisco Secure Access supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access console. An administrator signs in to Secure Access using Cisco Security Cloud Sign On (SCSO). Cisco Duo Security provides single sign-on (SSO) authentication of Secure Access administrators through SCSO.

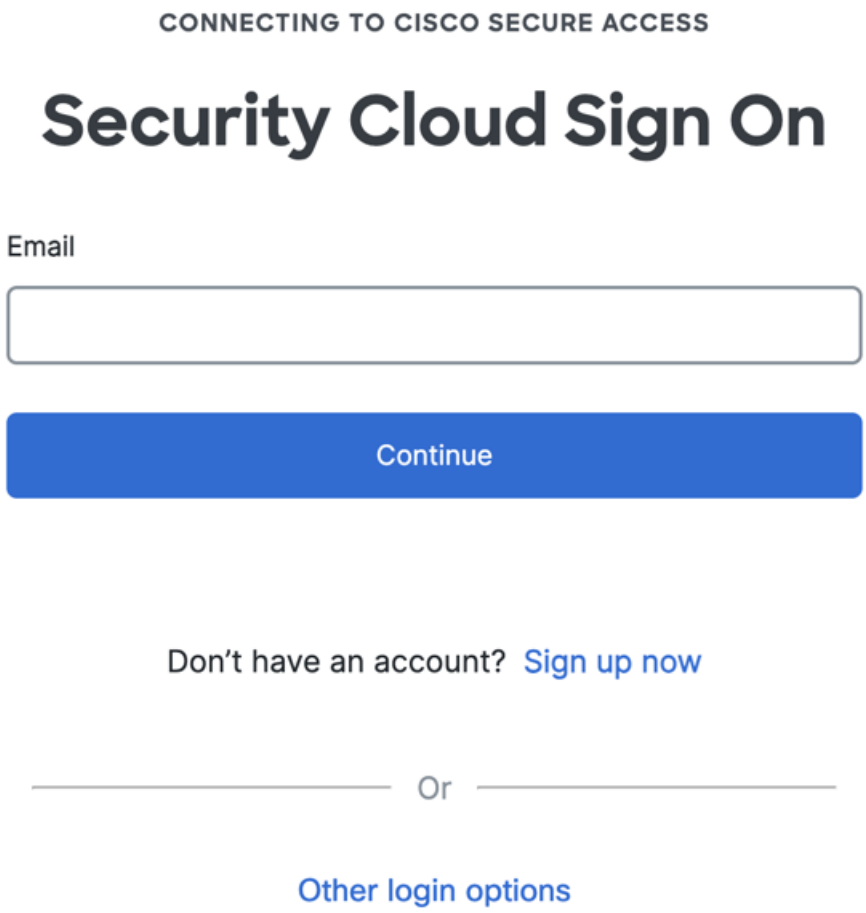
Before you begin

- A valid Secure Access account. For more information, see Manage Accounts.

Procedure

1. Navigate to your Secure Access organization at https://dashboard.sse.cisco.com/org/<org_number>.

   Secure Access uses single sign-on authentication through **Security Cloud Sign On**.



2. In **Security Cloud Sign On**, enter the email address where you received the invitation to join a Secure Access organization.

   Your Secure Access account and the SCSO account must use the same email address.

3. Click **Sign up now** and create an SCSO account.

   Secure Access sends you an invitation to create an SCSO account.

4. Once you receive an email from Secure Access inviting you to create an SCSO account, click the link in the email and follow the instructions to set up your SCSO account with your IdP.

   For more information, see Getting Started Guide for New Customers of Security Cloud Control.

5. Follow the steps to sign in to your Secure Access organization.

   For more information, see Sign In to Secure Access with Security Cloud Sign On.

Troubleshoot Single Sign On Authentication

Provides a link for contacting support.

If you are unable to sign in to Secure Access through Cisco Security Cloud Sign On, contact Support.

Find Your Organization ID

Provides instructions for completing the Find Your Organization ID workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Every Secure Access customer organization (Org) is a separate instance of Secure Access. Organizations are identified by their account name and a unique numeric organization ID (Org ID).

The Org ID is used to identify your organization when deploying network tunnels and when enrolling users and groups in the organization.

Before you begin

- A minimum user role of Read Only. For more information, see Manage Accounts.

Procedure

1. Sign in to Secure Access.
2. Check the URL in the browser's address bar: `https://dashboard.sse.com/org/<orgId>/#/<page>` where `orgId` is your unique Secure Access organization ID.
3. Navigate to the name of your user account, and expand your username to view the organizations where the username is a member.

   Confirm that you are signed in to the correct Secure Access organization. Your organization name is listed under your account name.
4. Click **Switch Organizations** to change to another Secure Access organization.
5. Locate **System Status**–the overall health status of Secure Access.

Determine Your Current Package

Provides instructions for completing the Determine Your Current Package workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Within your Cisco Secure Access subscription, the Secure Access *package* determines the features available to you as well as your level of support. You can see your current package listed on the Cisco Secure Access Subscription page.

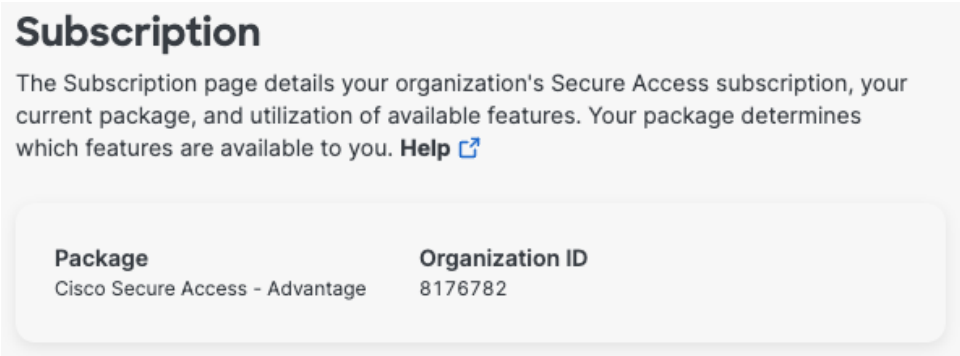
For more information about your current package, contact your sales representative.

Before you begin

- A minimum user role of Read Only. For more information, see Manage Accounts.

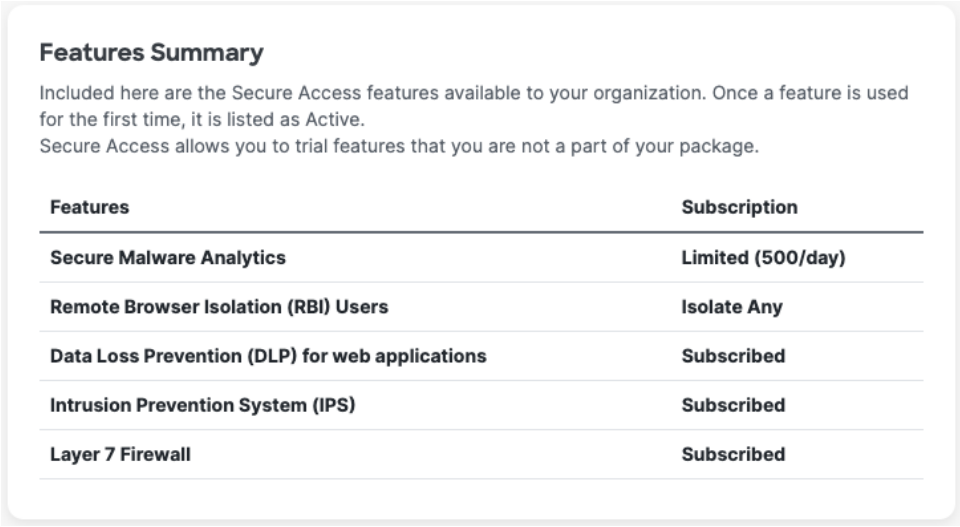
Procedure

1. Navigate to **Admin** > **Subscription** and review the information about your current package.



- **Package**–The name of your package.
- **Organization ID**–The ID assigned to your instance of Secure Access.

2. View the list of features and the status of the feature subscriptions for your package.



- **Feature**–The name of the feature.
- **Subscription**–The description of the status of the subscription. Indicates whether your organization subscribes to the feature in the package or if there are limitations on the feature.

Limitations and range limits

Limitations and range limits related to the maximum number of certain components and the amount of time that your data is retained by Secure Access.

Cisco Secure Access sets limitations by component and defines the amount of time that your data is available on our system. These general limitations affect how you configure, deploy, and interact with Secure Access.

Access Policy

For information about the Access policy, see Manage the Access Policy.

- You can add a maximum of 10,000 access rules in the Access policy.
- You can add a maximum of 250 sources on each access rule in the Access policy.

The total number of sources accepted in an access rule includes both pre-configured sources (resources) and sources that you enter directly on an access rule (composite sources).

You can add at most 10 composite sources in an access rule.

- You can add a maximum of 5000 destinations on each access rule in the Access policy.

  The total number of destinations accepted on an access rule includes both pre-configured destinations (resources) and destinations that you enter directly on an access rule (composite destinations).

  You can add at most 10 composite destinations in an access rule.

Zero Trust Access

The components of Zero Trust Access (ZTA) support the following limits:

- You can create a maximum of 100 ZTA profiles per organization.
- You can add a maximum of 100,000 steering destinations per ZTA profile, and 1 million steering destinations per organization.

For an in-depth list of limitations specific to Zero trust access, see Zero Trust Access Requirements and Limitations on page 1207.

Cisco Secure Client

- Secure Access checks the Cisco Secure Client Zero Trust Access (ZTA) posture profile every 5 minutes.
- Secure Access applies private application configuration changes to the Cisco Secure Client every 10 minutes. However, on iOS this is every 4 hours.
- Secure Client version 5.1.13 and later supports both IPv4 and IPv6.

Data Retention

- DNS logs–Summary data (such as queries per identity or domain) is available for one calendar year.
- DNS, Web proxy, firewall logs–Data retained for 90 days.

Destinations for Client-Based Zero Trust Traffic

Describes Destinations for Client-Based Zero Trust Traffic in Cisco Secure Access. Secure Access limits the number of Zero Trust traffic steering rules added in an organization for end-user connectivity.

Secure Access limits the number of Zero Trust traffic steering rules added in an organization for end-user connectivity. In Secure Access, the Zero Trust traffic steering rules appear on **Connect** > **End User Connectivity** > **Zero Trust**. For more information, see Traffic Steering for Zero Trust Access Client-Based Connections.

These limits include:

- Destinations that are automatically added to the Zero Trust traffic steering page. When an organization enables client-based zero trust connections, Secure Access adds a traffic steering rule for each "Internally reachable address" configured for Private Resources.
- Wildcard exceptions to the private resource addresses, which you configure on the Zero Trust traffic steering page.
- Any other destinations configured directly on the Zero Trust traffic steering page, which is not recommended.

To reduce the number of rules, consider using wildcards. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.

Domain Names

Describes Domain Names in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can configure various components in Secure Access with domain names, for example:

- Destination Lists
- Private Resources
- End-User Connectivity

> **Note**
>
> A domain name can have a maximum of 253 characters. A subsection or label in the domain name must have at least two and no more than 63 characters. Domain names may contain alphanumeric characters and the hyphen.

File Inspection and File Analysis

Describes File Inspection and File Analysis in Cisco Secure Access. See Manage File Inspection and File Analysis for details about supported files and limitations for file inspection and analysis performed by Cisco Advanced Malware Protection (AMP), Secure Access antivirus scanner, and Cisco Secure Malware Analytics.

See Manage File Inspection and File Analysis for details about supported files and limitations for file inspection and analysis performed by Cisco Advanced Malware Protection (AMP), Secure Access antivirus scanner, and Cisco Secure Malware Analytics.

Internet Protocol Versions

Describes Internet Protocol Versions in Cisco Secure Access and explains Single Stack versus Dual Stack and Internet Protocol support by Function. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports various IP versions to accommodate different network environments. The dashboard and wizards guide you in selecting the appropriate protocol based on your requirements.

Protocol Configuration Type

- **Pure IPv6 stack:** A configuration where the entire communication path, including tunnels and end to end traffic, is strictly IPv6.
- **Dual stack:** A configuration where tunnel endpoints communicate over IPv6, while the encapsulated internal traffic flows as IPv4.

Upstream connectivity and protocol handling : For upstream connectivity to web servers and internet-hosted resources, Secure Access connects using either IPv4 or IPv6 depending on the client configuration and destination resource. In any single transaction, only one IP version is used.

Important

Secure Access does not support automatic IPv6 fallback to IPv4. If an upstream session or resource connection fails over IPv6, the system does not fall back or translate the request to IPv4. Clients attempting to reach IPv4-only resources over a pure IPv6 connection or unresolvable IPv6 path will fail to connect. Ensure your network routing and client configurations support the intended protocol end-to- end.

The following table outlines internet protocol and configuration support across Secure Access functions:

Table 1: Internet Protocol support by Function

Function in Secure Access	Client-to-Cloud Connection (Ingress)	Cloud-to-Destination Forwarding (Egress)
Remote Access VPN	IPv4, pure IPv6, or Dual stack	IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)
IPsec tunnel (Network Tunnel Group)	IPv4, pure IPv6, or Dual stack	IPv4 and IPv6 traffic forwarding (No IPv6 to IPv4 fallback)
Remote Security Module	IPv4 or pure IPv6	IPv4 or pure IPv6
Secure Client Zero Trust Access (ZTA) - Private Access	Dual stack	Dual stack (Resource only) **Note** You can only configure IPv6 as a private resource, not a private destination.
Secure Client Zero Trust Access (ZTA) - Internet Access	IPv4 or pure IPv6	Not supported
DNS	IPv4, pure IPv6, or Dual stack	IPv4 or pure IPv6

IP Address Restrictions

Provides reference information about IP Address Restrictions in Cisco Secure Access, including Restricted Networks/Addresses. It summarizes the values, options, and related details presented in the topic.

The following networks/addresses are not valid for use as:

- Client IP pools
- System IP pools
- DNS and DDNS servers
- RADIUS servers
- Private resources

Using these addresses in the specified contexts can cause conflicts, routing issues, or operational failures.

Table 2: Restricted Networks/Addresses:

Network/Address	Description
0.0.0.0/8	Addresses in this block identify source hosts on 'this' network
127.0.0.0/8	Loopback
127.0.53.53	Name collision occurrence
169.254.0.0/16	Link local
192.0.0.0/24	IETF protocol assignments

Network/Address	Description
192.0.2.0/24	TEST-NET-1 (Documentation and examples)
198.18.0.0/15	Network interconnect device benchmark testing
198.51.100.0/24	TEST-NET-2 (Documentation and examples)
203.0.113.0/24	TEST-NET-3 (Documentation and examples)
224.0.0.0/4	Multicast
240.0.0.0/4	Reserved for future use
255.255.255.255/32	Limited broadcast

Note

You can use 198.18.0.0/15 network with the Secure Access internal networking fabric, in client IP pools, and for private resources. Keep it blocked for all other use cases.

For more information, refer to the following documentation topics:

- Manage Regions and IP Pools
- Add an IP Pool
- Manage DNS and DDNS Servers
- Add a RADIUS Group
- Manage Private Resources

Other Components

Describes Other Components in Cisco Secure Access. A destination list is not active until you set an access rule that includes the destination list.

Feature	Limit	Description
Block Page Bypass	You cannot use the Block Page Bypass feature with a redirected block page.	If configured, Secure Access uses the default appearance of the block page.
Bypass Domains	No more than 2000 bypass domains may be added to Secure Access.	The number of bypass domains can be increased upon request.
Customer CA Signed Root Certificate	Six certificates per organization.	

Feature	Limit	Description
Destination Lists	• A destination list is not active until you set an access rule that includes the destination list. • A destination list's comment string can contain at most 256 characters. • A destination list does not support regular expressions in URL paths. • No more than 250K destinations may be added to the Secure Access across all the destination lists.	Destination lists may contain fully qualified domain names (FQDN), URLs, or IP addresses.
File Download	The maximum file size that can be downloaded is 5 GB, which applies only for access rules with the **Isolate** action.	If the access rule does not specify the **Isolate** action, Secure Access will permit downloads of files greater than 5 GB. Secure Access scans the downloaded files.
File Scanning (Antivirus, Threat Grid, and AMP)	• A file must be less than 50 MB. • Compressed file scanning supports no more than 16 levels of recursion. • AMP: The system computes only the archive hash, not hashes for files inside archives.	
File Transfer	The maximum file size that the Secure Web Gateway (SWG) can upload is 20 GB.	
Internal Networks	No more than 5000 internal networks may be added to Secure Access.	
Network Tunnel Groups	• Static Traffic Selector Prefixes must not exceed 100 • BGP prefixes must not exceed 10,000	• The combination of local and remote traffic selector prefixes (those configured dashboard in the dashboard plus transmitted via IKE) must not exceed 100. Customers should utilize BGP for more complex or dynamic networks. • Network Tunnel Groups with BGP can support up to 10,000 prefixes.
Reserved IP	20 reserved IP addresses per organization per DC or Secure Access region.	Reserved IP supports 20 IPs per organization per region (sufficient for 160 Gbps of throughput).
WebSockets and HTTP PATCH	For WebSockets or HTTP PATCH requests, the Secure Access Secure Web Gateway does not perform file inspection.	

Reports

Describes Reports in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

For details on data retention periods for each report type, see Report retention.

Feature	Limit
• Scheduled Report (email attachment)	Accepts up to 10,000 rows of data.
• Exported Report (CSV export)	Exports no more than 100,000 rows of data.

Resource Connectors and Resource Connector Groups

Describes Resource Connectors and Resource Connector Groups in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Feature	Limit
Maximum number of connector groups per organization	50
Maximum number of connectors per connector group	50

Service Connections

Describes Service Connections in Cisco Secure Access. The number of total, concurrent browser-based Secure Shell (SSH) and Remote Desktop Protocol (RDP) sessions supported is limited to the total number of Secure Access Advantage, Secure Private Access (SPA) licenses purchased, regardless of the number of configured applications.

The number of total, concurrent browser-based Secure Shell (SSH) and Remote Desktop Protocol (RDP) sessions supported is limited to the total number of Secure Access Advantage, Secure Private Access (SPA) licenses purchased, regardless of the number of configured applications.

Users and Groups

Describes Users and Groups in Cisco Secure Access. For general information about adding users, groups, and endpoint devices, see Manage Users, Groups, and Endpoints Devices.

For general information about adding users, groups, and endpoint devices, see Manage Users, Groups, and Endpoints Devices.

Cloud Identity Providers

Secure Access supports provisioning up to 1000 groups from a supported cloud identity provider (IdP). For information about provisioning users and groups, see Manage Cloud Identity Providers.

> **Note**
>
> If you have more than 1000 groups in the organization, contact Support to get assistance with importing the groups in Secure Access. For more information, see Cisco Support.

Users and Private Applications

For access to private applications, configure the user and private applications to use the same data center.

Endpoint Data Center Selection

Explans how DNS, Geo-Load Balancing (GeoLB), Anycast, routing policies, and configuration choices influence the data center where your users connect.

As organizations deploy Cisco Secure Access, a common question arises: *“How does the endpoint decide which data center to connect to?”*

Cisco Secure Access does not have a single "nearest data center" rule that governs all traffic. Cisco Secure Access utilizes distinct architectural paths depending on the service being consumed - Secure Client roaming web protection (SWG), Zero Trust Access (ZTA) for private applications, Trusted Internet Access (TIA), or Remote Access VPN (VPNaaS).

This section bridges the gap between high-level summaries and deep-dive architectural behavior, explaining how DNS, Geo-Load Balancing (GeoLB), Anycast, routing policies, and configuration choices influence where your users connect.

Roaming Web Protection (Secure Web Gateway)

Describes Roaming Web Protection (Secure Web Gateway) in Cisco Secure Access. When the Secure Client provides roaming web protection using the Secure Web Gateway (SWG) module, it connects the user to Cisco's cloud web-security service.

When the Secure Client provides roaming web protection using the Secure Web Gateway (SWG) module, it connects the user to Cisco's cloud web-security service.

Discovery and Initial Placement

The client relies on DNS-based service discovery. It queries either a standard Cisco proxy hostname (e.g., swg-url-proxy-https-sse.sigproxy.qq...) or a newer version with the customers’ org ID embedded (e.g., swg-url-proxy-https-\#\#\#\#\#.sseproxy.qq...), and the DNS resolver returns the IP address of the closest optimal data center. Anycast routing ensures the endpoint reaches a nearby DNS resolver, optimizing the initial connection speed.

Geo-Load Balancing (GeoLB) and Country Rules

Proximity is the baseline, but GeoLB can override the "closest" data center. GeoLB is the intelligent global load balancer that incorporates customer preferences, reserved IP configurations, country alignment, and more.

You can use GeoLB to apply the following:

- **Maintenance & Failover:** Seamlessly shifting traffic away from data centers undergoing maintenance.
- **Regional Balancing:** Distributing load across multiple facilities.
-

Reserved IP and Ingress Control

If your organization purchased Reserved IP to ensure dedicated egress IP addresses for SaaS allowlisting, the data center selection logic changes significantly.

- **Ingress Control:** Cisco must ensure the user connects to a data center where your organization actually holds a reserved IP.
- If the physically closest data center does not have your reserved IP provisioned, the network will automatically bypass it and route the user to the nearest data center that *does* host your reserved IP.

> **Note**
>
> Reserved IP ingress control is primarily supported for standard HTTP/HTTPS roaming SWG traffic.

Zero Trust Access (ZTA) for Private Applications

Describes Zero Trust Access (ZTA) for Private Applications in Cisco Secure Access. Client-based ZTA intercepts traffic destined for configured private resources and brokers the connection through the Secure Access cloud without requiring a traditional VPN tunnel.

Client-based ZTA intercepts traffic destined for configured private resources and brokers the connection through the Secure Access cloud without requiring a traditional VPN tunnel.

> **Note**
>
> Because ZTA always ingresses to the nearest PoP, a user traveling in Canada will ingress into a Canadian data center. If your application requires a US source IP, you do *not* force the user's ingress to the US. Instead, you deploy the Resource Connector in a US-based environment (e.g., AWS US-East). The traffic will automatically backhaul across the Cisco backbone and egress out of the US-based Resource Connector, satisfying the geo-blocking requirement.

Ingress and Traffic Pathing

The ZTA client has slightly different data center selection logic than the SWG module. The design minimizes the first-mile and last-mile time spent on the internet, and maximizes connection time spent on the Cisco backbone.

- **Ingress:** The ZTA client utilizes DNS proximity routing to connect to the **nearest available ZTA Point of Presence (PoP)**.
- **Backbone Transport:** Once connected, the traffic traverses the Cisco Secure Access backbone.
- **Egress:** The traffic routes to the Cisco PoP closest to where your **Resource Connector** or IPsec tunnel is deployed.
- **Delivery:** The Resource Connector delivers the traffic to the private application.

Universal / Hybrid ZTNA and Trusted Networks

If your environment utilizes Universal /Hybrid ZTNA with Cisco Secure Firewalls, the ZTA client performs Trusted Network Detection (TND). If the client determines it is on a trusted internal corporate network, Secure Access redirects the connection to a local on-premises Secure Firewall enforcement point, entirely bypassing the cloud PoP to prevent unnecessary hairpinning.

Failover

ZTA session failover is evaluated per private resource attempt. If an active PoP goes offline, the client uses DNS to seamlessly resolve and connect to the next closest available data center. This happens transparently to the user without dropping the overall Secure Access application session.

Trusted Internet Access (TIA) via the ZTA Client

Describes Trusted Internet Access (TIA) via the ZTA Client in Cisco Secure Access. Trusted Internet Access leverages the modern ZTA client architecture to secure outbound internet destinations, applying device posture checks, firewall rules, IDS/IPS, and SWG enforcement.

Trusted Internet Access leverages the modern ZTA client architecture to secure outbound internet destinations, applying device posture checks, firewall rules, IDS/IPS, and SWG enforcement.

- **Placement:** The TIA client connects to the nearest available cloud enforcement PoP **that your organization has explicitly enabled**. Only data centers that the customer has requested to be enabled (via TAC/Support) are considered for connection. If a specific PoP is not enabled for your tenant, users will never connect to it, regardless of proximity.
- **Best Practice for Availability:** Customers should always have at least **two** DCs or Regions enabled to ensure proper high availability and failover routing.
- **Distinction from SWG roaming module:** TIA utilizes a newer version of the global DNS balancer. It has similar latency-based selection of the nearest enabled data center for the client requests.
- **Failover:** TIA relies on the inherent multi-region resiliency of the ZTA architecture. If a local region is degraded, traffic is seamlessly handled by neighboring enabled regions.

Remote Access VPN (VPNaaS)

Describes Remote Access VPN (VPNaaS) in Cisco Secure Access. Secure Access provides Remote Access VPN using a unique organizational FQDN (e.g., *your-org-id*.vpn.sse.cisco.com).

Secure Access provides Remote Access VPN using a unique organizational FQDN (e.g., *your-org-id*.vpn.sse.cisco.com).

Default Data Center Selection

By default, when a user initiates a VPN connection to your organizational FQDN, Cisco's DNS routing dynamically directs them to the closest available PoP or Region. The user is locked to that data center for the duration of the session.

Administrator Controls and Regional Profiles

While auto-selection based on proximity is the default, administrators have significantly more control over VPN placement than they do with ZTA ingress:

- **Region-Specific Profiles:** Administrators can push region-specific VPN profiles and FQDNs to Secure Clients. This allows end-users to manually select their connection region via a drop-down (e.g., forcing a connection to a European hub while traveling in the US).
- **IP Pools:** Administrators must configure IP pools (up to 50 per region). Users can only connect to regions where an admin has actively deployed VPNaaS and allocated IP pools.

High Availability and Failover

VPN failover is aggregated for all private resources in a session.

- Within a region, VPNaaS is distributed across multiple Availability Zones (AZs) or Virtual Edge Data Centers (VEDCs). If one fails, users are automatically handled by the other AZ.

- If an entire region fails, users can automatically fail over to a secondary region–**provided the administrator has configured IP pools in that secondary region**.

Regional and US Federal Government Deployments

Describes regional and US federal government deployments in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Depending on regulatory and compliance requirements, Secure Access offers specialized environments with strict rules on data center selection and client roaming:

- **Secure Access China (SSE China):** For organizations utilizing Secure Access China, Roaming Client traffic features automatic geographical detection. The client detects whether the user is inside or outside of China and seamlessly adjusts the set of data centers it connects to.

> **Note**
>
> A customer must have subscriptions to both global Secure Access and Secure Access China for this seamless internal/external roaming to function

- **Secure Access - Local data residency deployments:** In these deployments, data in the control, management, and data planes remain within a specific region rather than in a global cloud. The core security features are comparable to standard Secure Access. For data processing details, see the Cisco Secure Access with Local Data Residency Offer Disclosure on the Cisco Trust Portal.
- **Cisco Secure Access for Government:** This is a separate instance of Secure Access certified for FedRAMP Class D (High). Access to this product is restricted to eligible users under FedRAMP PMO and CISA regulations. Government users must connect within the government boundary at the government cloud access points.

Information to Gather Before Contacting Cisco Support

Describes the information you need to gather before you contact Cisco Support with issues related to user connections.

If you suspect users are terminating in the incorrect region or experiencing sub-optimal routing, gather the following before opening a case:

- **Connection Method:** Is the user connecting via SWG Roaming Module, ZTA Private Access, TIA, or RA VPN?
- **Network State:** Is the device on a trusted corporate network or a remote/public network?
- **DNS Resolution:** What IP address does the client resolve for the Secure Access proxy or VPN headend? (Are they using public DNS, ISP DNS, or Cisco Umbrella resolvers?)
- **Enabled PoPs (for TIA):** Have you verified with TAC which data centers are actively enabled for your organization's TIA routing?
- **Reserved IP:** Does your organization utilize Reserved IP, and is the provisioned region different from the user's physical location?
- **Application Architecture:** If complaining about "wrong location" for private apps, where is the Resource Connector deployed?
- **VPN Config:** For VPN, which profile is the user selecting, and are IP pools configured in the expected region?
- **Tenant Type:** Is the user registered to a specialized environment (such as Secure Access China, Cisco Secure Access for Government, or a local data residency) that enforces strict boundary rules?

2 Secure Access Dashboards

Topics:

- Secure Access Overview Dashboard
- Service Analytics Dashboard
- Security Insights Dashboard
- Secure Access Status Portal

Provides an overview of Secure Access Dashboards, including Secure Access Overview Dashboard, Service Analytics Dashboard, and Security Insights Dashboard. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Secure Access Overview Dashboard

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage.

The Secure Access Overview dashboard lists the latest information about your organization's traffic and the amount of data that was transferred over your connections and how the data correlates this with security events.

From the Overview dashboard, you can set up Secure Access through the **Get Started with Secure Access** workflow. If you have established network connectivity, the first workflow is completed and lists your network connections. For more information about Secure Access workflows and how to start, see Begin Secure Access Onboarding Workflow.

Once you configure your organization's network connectivity, confirm that traffic from user devices can reach Secure Access. For information about the Secure Access reports, see Get Started with Reports.

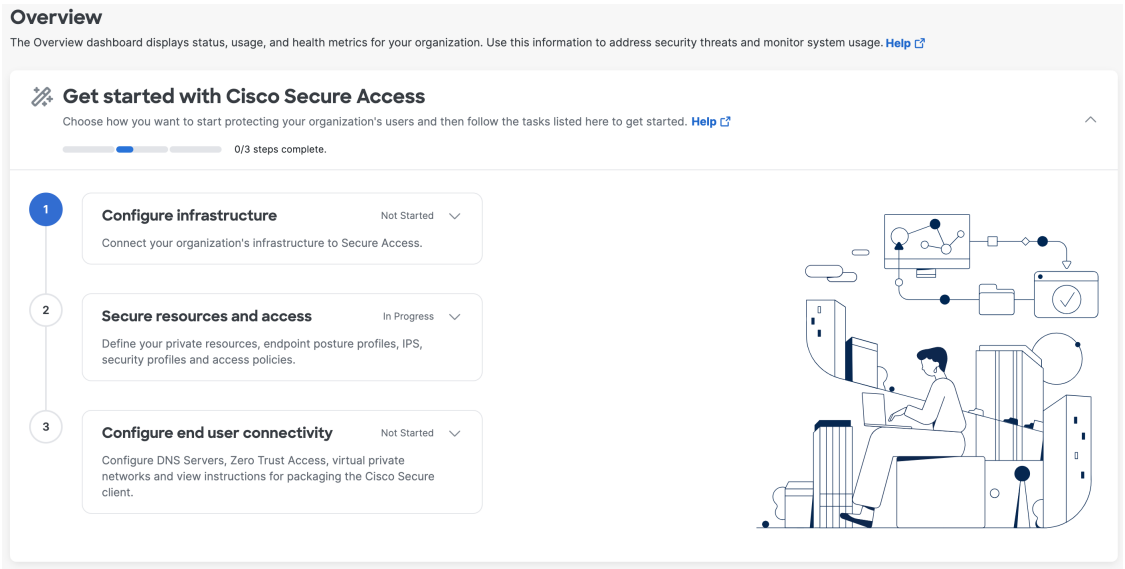
Prerequisites

- A minimum user role of Read Only. For more information, see Manage Accounts.

Get Started Workflow

Describes Get Started Workflow in Cisco Secure Access. The Getting Started with Secure Access Workflow describes the first configuration steps required to begin protecting your systems with Secure Access.

The **Getting Started with Secure Access Workflow** describes the first configuration steps required to begin protecting your systems with Secure Access.

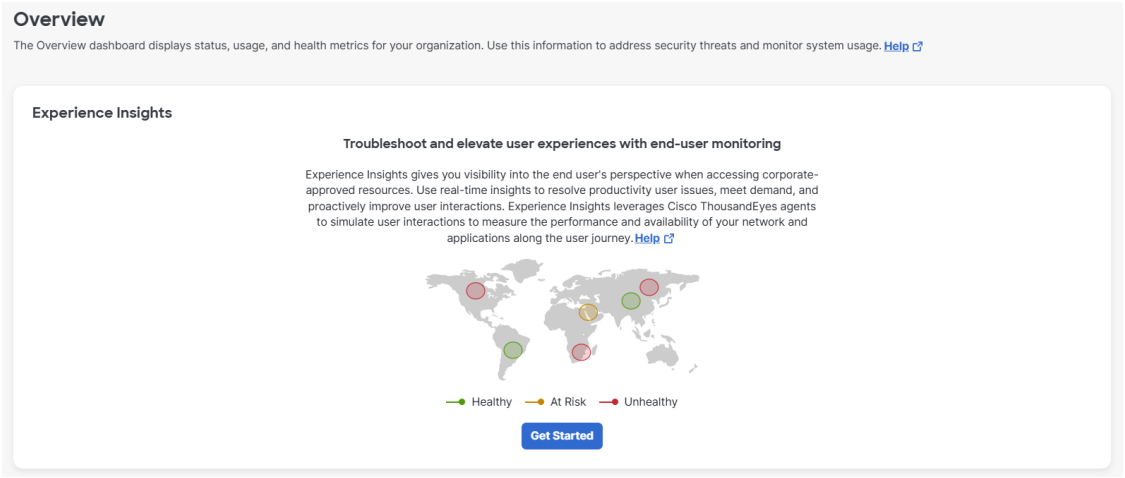


Experience Insights

Describes Experience Insights in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The **Experience Insights** section describes the Secure Access feature and its benefits. Click **Get Started** to begin the process of onboarding and configuring Experience Insights.

- After you onboard Experience Insights, the section will no longer display.



Network Tunnel Group Usage

Monitor your organization's network tunnel group traffic usage.

The Network tunnel group usage section displays the traffic usage for your organization's network tunnel groups. Use this section to analyze traffic patterns and monitor traffic usage across network tunnel groups for the selected billing period (current billing month, Previous billing month, Last six billing months, or a custom date range).

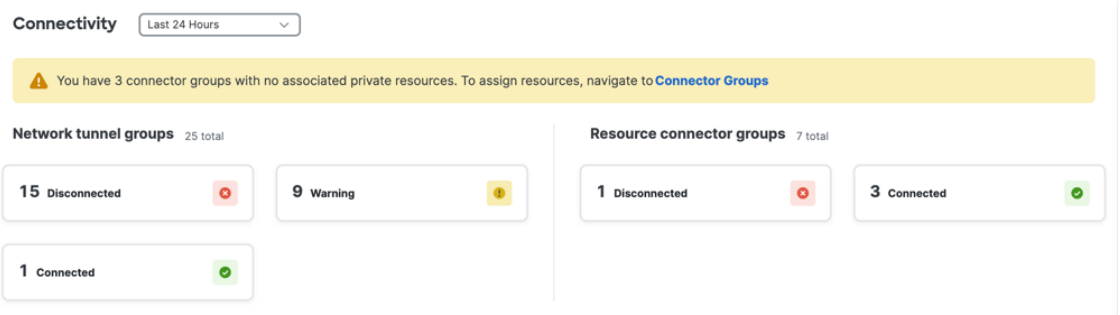
- **Region**: By default, the dashboard displays usage for All regions. You can use the region filter to isolate data for specific geographic areas.
- **Traffic summary**: Displays the total traffic transferred for the selected billing period.
- **Top network tunnel group by traffic**: Displays the Network tunnel group with the highest traffic usage. Clicking the tunnel group name opens a side panel where you can select a billing period (Current billing month, Previous billing month, Last 6 billing months, or a Custom date range) to view these detailed metrics:
  - **Traffic trends**: A visualization of inbound and outbound traffic over your selected period. You can hover over the chart to view specific traffic data for any given date.
  - **Traffic breakdown**: A summary of total inbound (In) and outbound (Out) data volume.
  - **Traffic used**: The aggregate volume of data transferred through the tunnel group.
  - **View**: Click **View** to open the Network tunnel group usage report. For more information, see Network tunnel group usage.
  - **Export report**: In the side panel, click **Export Report** to download the usage data for the selected billing period. For more information, see Export Report.

> **Note**
>
> The system automatically adjusts traffic units (for example, KB, MB, GB, TB) based on the volume of data to ensure the charts remain readable.

Connectivity

Describes Connectivity in Cisco Secure Access. The Connectivity section describes the status of your organization's configured Network Tunnel Groups and Resource Connector Groups.

The **Connectivity** section describes the status of your organization's configured Network Tunnel Groups and Resource Connector Groups.



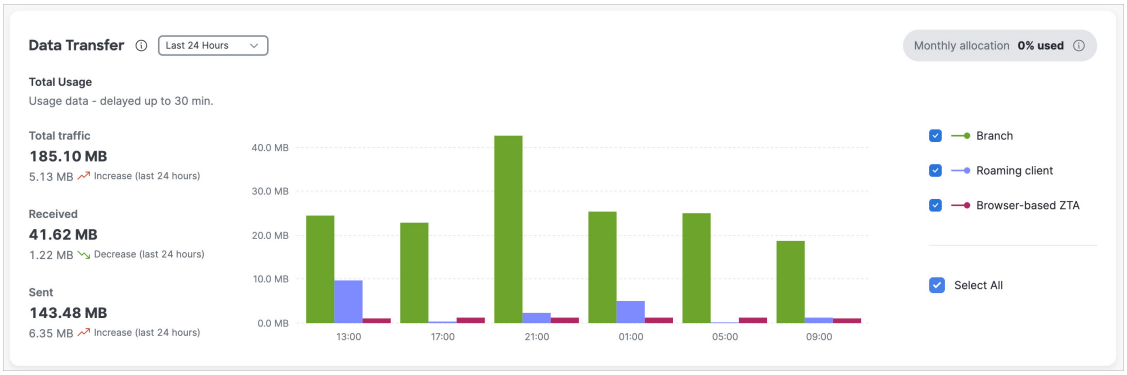
For more information, see View Network Tunnel Group Details and Manage Resource Connectors and Connector Groups.

Data Transfer

Describes Data Transfer in Cisco Secure Access. The Data Transfer section describes the total traffic, and the amount of data received and sent over the networks in your organization.

The **Data Transfer** section describes the total traffic, and the amount of data received and sent over the networks in your organization. Filter the usage data by the source to identify trends related to the type of connectivity:

- **Branch**
- **Roaming client**
- **RAVPN**
- **Client-based ZTA**
- **Browser-based ZTA**



Security

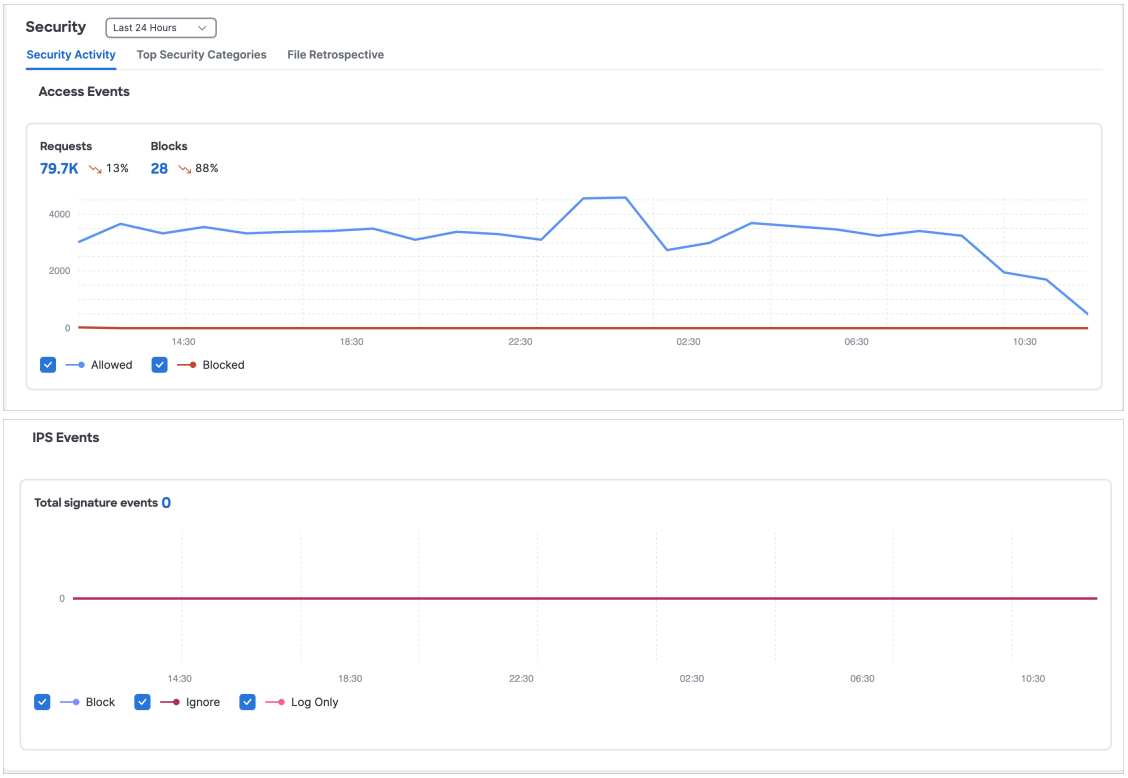
Describes Security in Cisco Secure Access. The Security section includes information about the security activity (requests and blocks) and top security categories visited by devices and users in your organization.

The **Security** section includes information about the security activity (requests and blocks) and top security categories visited by devices and users in your organization.

Security Activity

Describes Security Activity in Cisco Secure Access. The Security> Security Activity section displays the number of access events–requests and blocks.

The **Security**> **Security Activity** section displays the number of access events–requests and blocks. It also displays the number IPS events–signature events.



The **Security > Security Activity > IPS Events** section displays an expiry banner when a certificate for Private Resource Decryption has expired or will expire within 90 days.

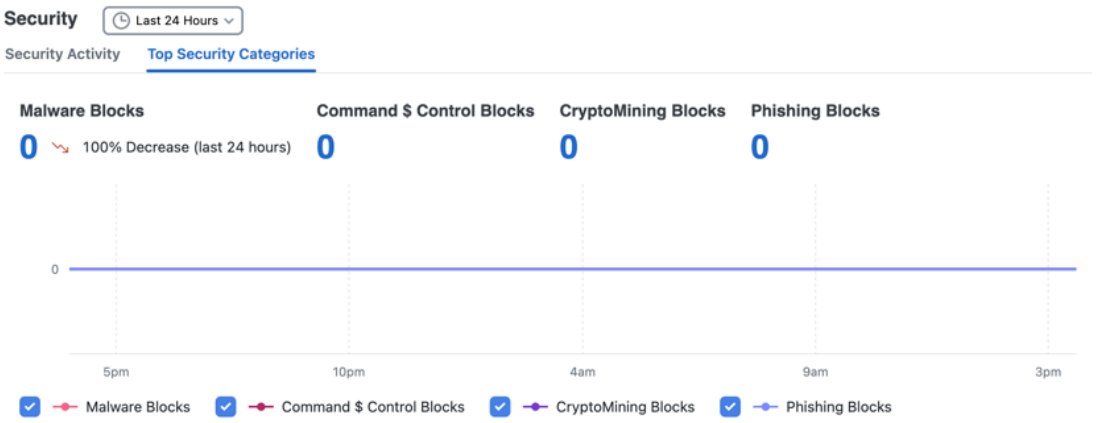


Users with the **Full Admin** or **Security Administrator** role can follow the **Certificates** link to update the certificate, or close the banner. If the certificate is not updated, a closed banner will reappear the next time the user opens the **Overview** page.

Top Security Categories

Describes Top Security Categories in Cisco Secure Access. The Top Security Categories displays the number of requests to the top security categories.

The Top Security Categories displays the number of requests to the top security categories.



File Retrospective

Describes File Retrospective in Cisco Secure Access. The File Retrospective section lists the SHA256 name, the threat score, the malware name, and the date the file was detected.

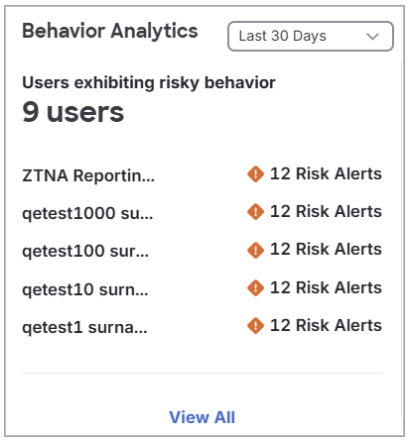
The File Retrospective section lists the SHA256 name, the threat score, the malware name, and the date the file was detected. The threat score is a percentage from 0-100 ranking the likelihood that the file is malicious. The score is generated from the data provided in the Secure Malware Analytics (Threat Grid) Report.

Users and Groups

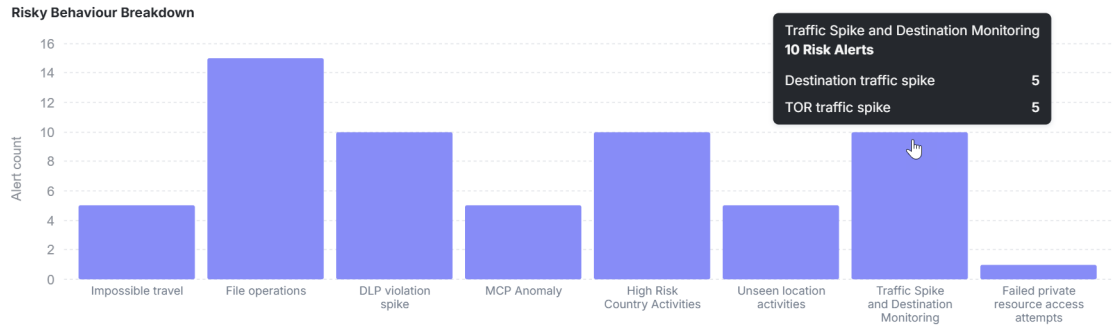
Describes Users and Groups in Cisco Secure Access. The Users and Groups section displays the following information: The count of users exhibiting risky behaviour.

The **Users and Groups** section displays the following information:

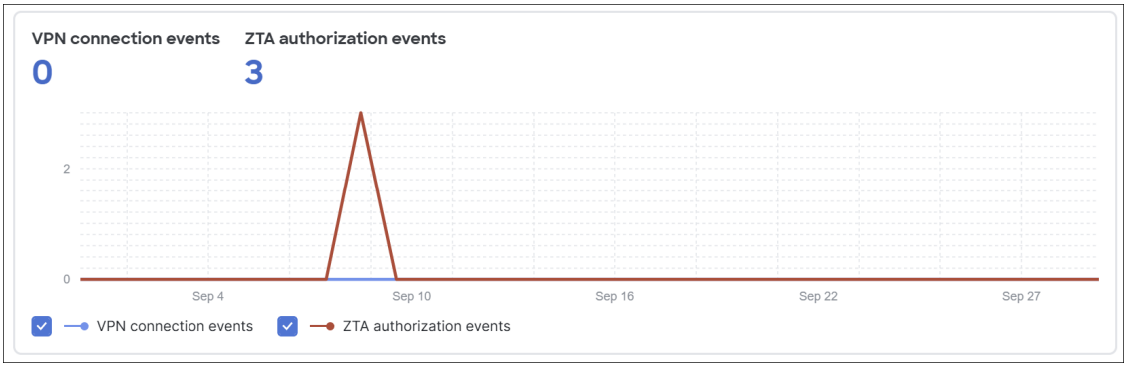
- The count of users exhibiting risky behaviour. Clicking the user count opens the **Users, Groups, and Endpoint Devices** page for more details.



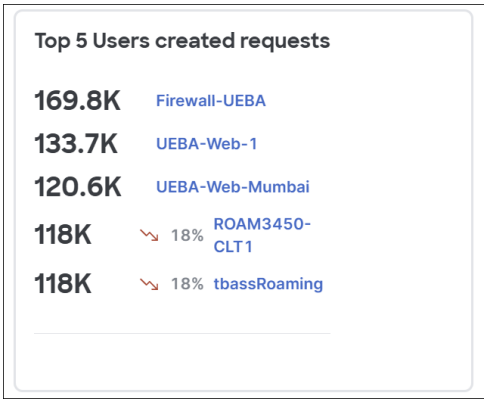
- List of top risky users with the count of risk alert categories detected for each user. Clicking **View All** opens the **Users, Groups, and Endpoint Devices** page for more details.
- The **Risky Behaviour Breakdown** chart displays the number of events detected for all the risk categories.



- The user trust levels chart displays the number of users with each trust level.
- The number of virtual private network (VPN) connections and Zero Trust Network Access authorization events over time.

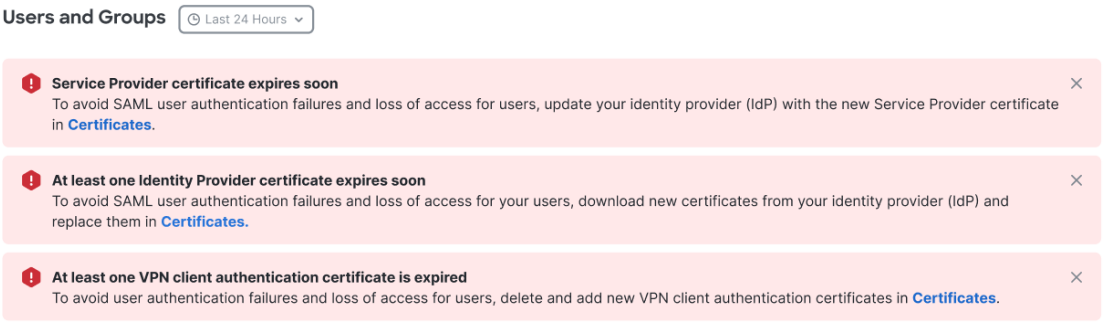


- The list of the top users in your organization who made the greatest number of requests in the selected time period.



Users and Groups displays expiry banners for certificates that impact user authentication and access when:

- A certificate has expired
- A certificate will expire within 90 days



Users and Groups certificate expiry banners apply to three certificate types:

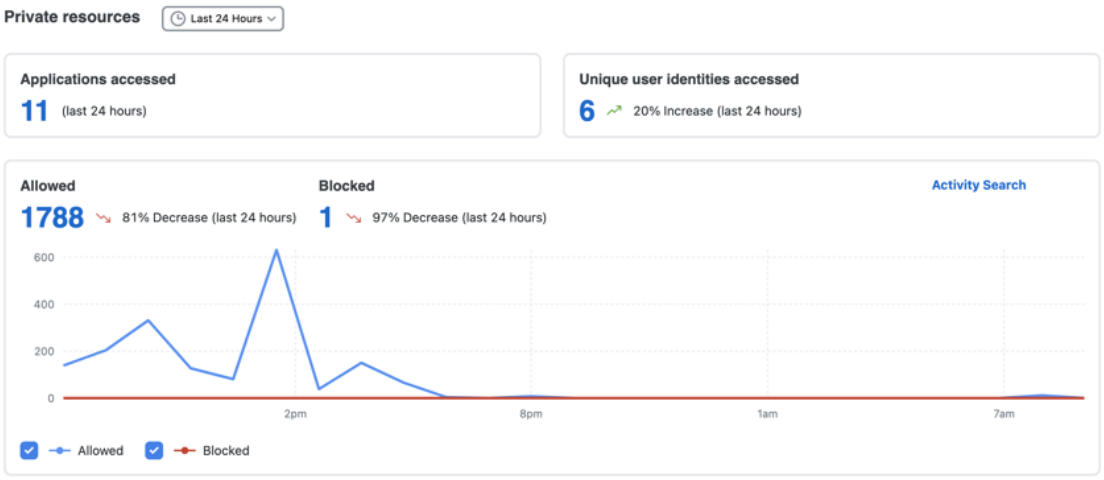
- Manage SAML Certificates for Service Providers
- Manage SAML Certificates for Identity Providers
- VPN Certificates for User and Device Authentication

Users with the **Full Admin** or **Security Administrator** role can follow the **Certificates** link to update the certificate, or close the banner. If the certificate is not updated, a closed banner will reappear the next time the user opens the **Overview** page.

Private Resources

Describes Private Resources in Cisco Secure Access. The Private Resources section displays the number of times applications are requested, the number of unique active users that request access, and the number of requests that are allowed or blocked over the selected time period.

The **Private Resources** section displays the number of times applications are requested, the number of unique active users that request access, and the number of requests that are allowed or blocked over the selected time period.



The **Private Resources** section also displays the number of times remote users connected to Secure Access and the method of the connection: virtual private network (VPN),client-based ZTNA, or clientless ZTNA. The section also includes the top resources that received traffic.



Service Analytics Dashboard

Service Analytics is a dashboard that provides real-time insights into the performance, health, and usage metrics of your organization's successful RAVPN and Zero Trust Access connections.

Service Analytics provides a real-time view of your organization's health, performance, and usage of RAVPN and Zero Trust Access capabilities. These pages show user distribution by region, Cisco Secure Client versions, operating system type, device compliance, Duo client versions, and browsers in use.

Service Analytics logs RAVPN, ZTA, Secure Client, and OS information only for successful connections; it does not record data for failed attempts. Data usage reflects only active users who generated connect or disconnect events during the selected time frame.

Navigate by going to **Home** > **Service Analytics**.

RAVPN (Remote Access VPN)

Active sessions: View a real-time graph of how many active users are online. Filter by time and view all regions or up to 12 selected regions.

> **Note**
>
> Secure Access samples the active connection count every 15 mins and hence the current hour's data point may take up to 15 mins past the hour to be shown on the graph.

- **Most recent active sessions**: Shows the time with the number of active sessions from the last 15 minutes within the selected time frame.
- **Peak active sessions**: Shows the time with the highest number of active sessions across the selected regions.

IP Pool Metrics: RAVPN IP pools are assigned to a specific geographical region where a Secure Access data center is located and users connecting to a region are assigned an IP address from that region's pool. This can help manage IP address allocation per region and support dynamic scaling and high availability. Admins can use this tile to understand their IP pool usage. If an IP pool is exhausted or almost exhausted, new connections may fail. Admins can increase capacity to avoid such connection failures for users.

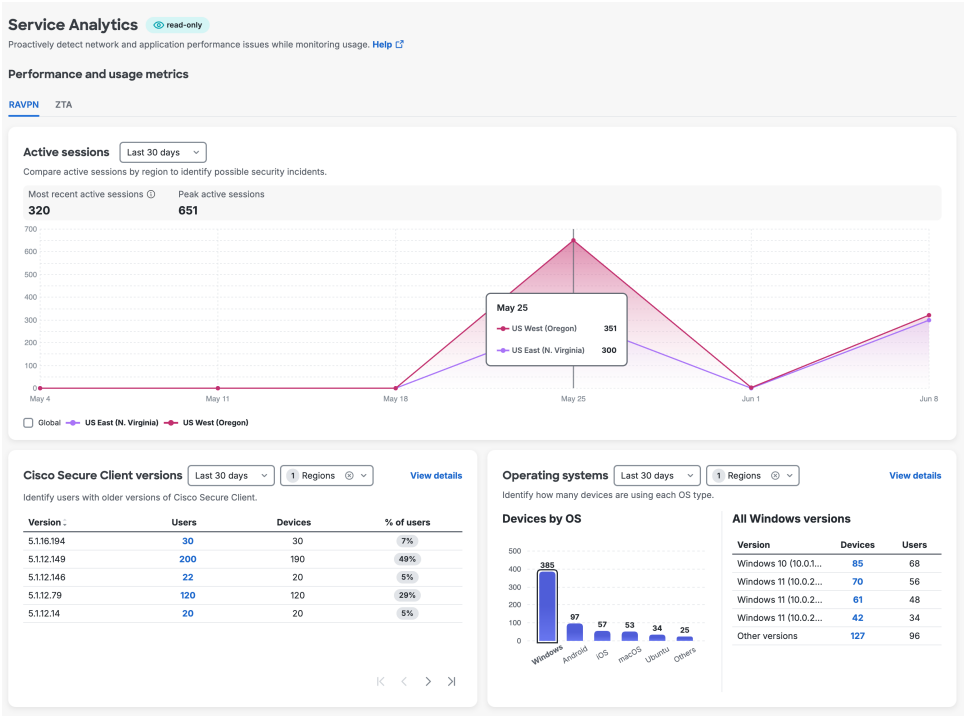
The RAVPN IP pools widget includes the following metrics, polled and generated every 15 minutes; review them using the guide of icons and meanings located at the top of the widget to identify regions or IP pools experiencing issues.

- **Status** – The status of the IP pools; this icon alerts you to the most severe pool status and is not a generalized summary of status' if a region has more than one IP pool configured.

- **Region** – the region configured for the IP pool partnered with a more granular location within the region where the Secure Access data center is located. Regions include data from both IPv4 and Ipv6.
- **IP Pool** – The status of the configured IP pool and how many IP pools are configured per region. Since a singular region can host more than one IP pool, each pool has the capacity to have a different status. Hover your cursor on the IP Pool name to see the consumption of any pool in details including IPv4 and IPv6.

Cisco Secure Client versions: Shows the number of users and devices by the Cisco Secure Client version. Click the users count to see additional user's information. Filter by time and view all regions or up to 12 selected regions.

Operating system: Shows up to five operating systems at a time; additional systems appear in the others category. Each operating system includes the version on the device. You can click the device bar graph to view the top four versions for that operating system and click **Others** to see the full list of operating systems and versions.



ZTA

Users by region: Shows the number of users in each region in the last 24 hours, 7 days, or 30 days. Click a user count to view additional details, including device name and email address. For more information on regions, see Secure Access Regions.

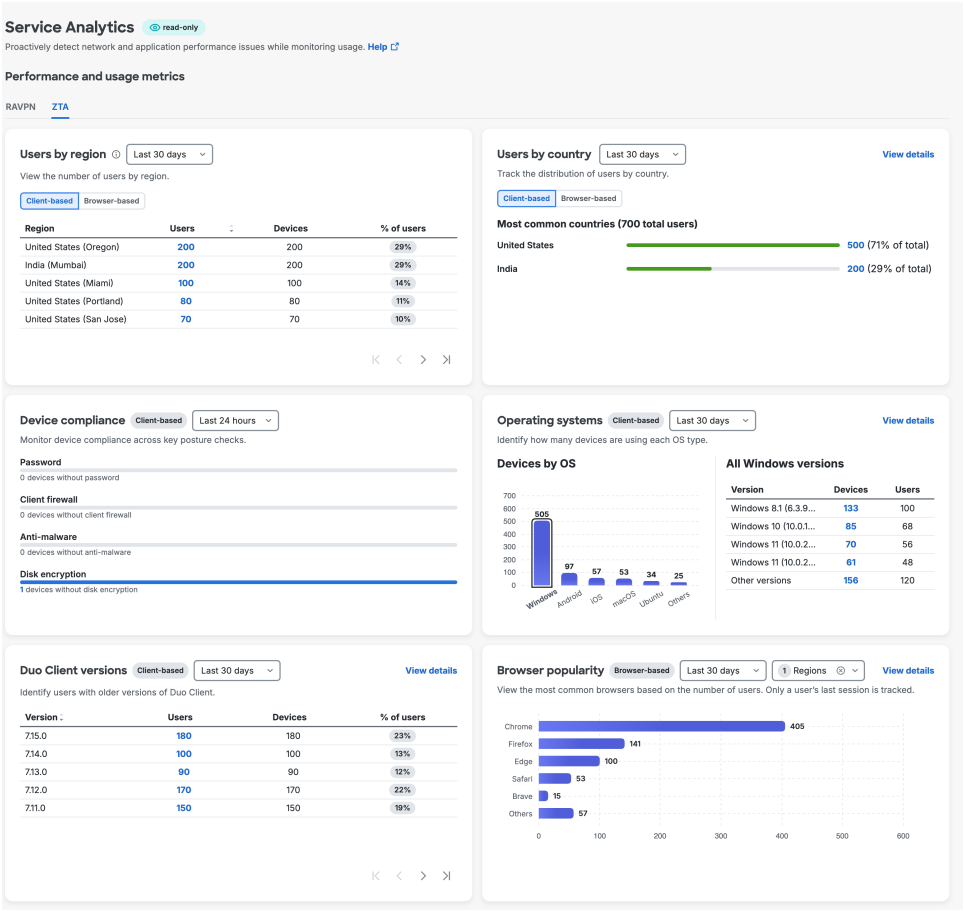
Users by country: Shows the number of users in each country based on their geolocation. Click a user count to view additional details, including device name and email address.

Device compliance: Monitor device security via posture checks. Identify endpoints missing critical protections–such as passwords, firewalls, anti-malware, or disk encryption–and view your overall device posture status.

Operating systems: Shows up to five operating systems at a time; additional systems appear in the Others category. Each operating system includes the version on the device. You can click the device bar graph to view the top four versions for that operating system and click **Others** to see the full list of operating systems and versions.

Duo Client versions: Shows which Duo Client version is installed on each end user's device. Click a user count to view additional details, including device name and email address.

Browser popularity: Displays the five most-used browsers at a time; additional browsers appear in the others category. You can click the device bar graph to view more details, including user name and user email address. Click **Others** to see the full list of browsers and versions. You can view data for all regions or filter by up to 12 regions at a time.



Security Insights Dashboard

Security Insights is a cross-domain operational dashboard in Cisco Secure Access that unifies security posture, data protection, AI governance, application risk, identity risk, and threat activity into a single investigation surface.

About Security Insights

Security Insights is a dashboard in Secure Access for security teams that need to understand risk across users, applications, data, and threats without starting from separate reports. The dashboard presents operational insights from Secure Access controls, Cisco Identity Intelligence, Data Loss Prevention, App Discovery, and threat reporting.

It brings together insights that have historically lived in separate reports and workspaces, including:

- Threat enforcement outcomes (allowed and blocked)
- Data Loss Prevention (DLP) violations across web, SaaS API, email, endpoint, and private app channels
- Generative AI application discovery and AI Guardrail violations
- Application risk, including third-party app authorizations
- User trust levels from Continuous Identity Intelligence (CII)
- User and Entity Behavior Analytics (UEBA) detections
- Connection type distribution (VPN versus ZTNA)

Requesting access

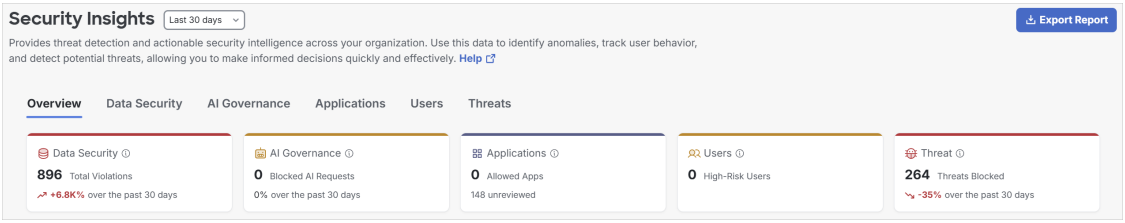
Security Insights is available on request. To enable Security Insights for your organization, contact Cisco Support. For contact information, refer to Welcome to Cisco Secure Access.

Opening Security Insights

After the feature is enabled for your organization, open Security Insights from the Secure Access left navigation menu.

Tabs in Security Insights

The dashboard is organized into six tabs. Each tab uses a consistent layout: a top row of summary cards that scope the tab's subject matter, followed by visualizations and tables that support investigation. Most panels link to existing reports and policy pages where you can perform deeper analysis or take action.



Tab	Focus
Security Overview	Cross-domain summary of traffic, threat outcomes, and security enforcement
Data Security	DLP violations by channel, classification, user, rule, and destination
AI Governance	GenAI app discovery, AI Guardrail violations, and sensitive data sent to AI
Applications	Allowed, not-allowed, unreviewed, and third-party risk apps
Users	User trust levels, top risky users, UEBA detections, and connection types
Threats	Blocked and allowed threats, rule efficacy, trends, and risky destinations
Set Background Theme	Set the user interface theme to light theme, dark theme, or to adopt the theme your browser uses.

How to use the dashboard

- **Start with Security Overview**. Use it as your landing page to confirm whether anything requires immediate attention.
- **Pivot by clicking.** Summary cards, Sankey nodes, table rows, and panel titles link to the corresponding tab, report, or policy page.
- **Use time-range controls.** Most panels honor the dashboard period switcher (24 hours, 7 days, 30 days, 60 days). Some panels have fixed intervals, which are noted in the panel description.

Related information

- Events Report
- Data Loss Prevention Report
- Manage the Data Loss Prevention Policy
- App Discovery Report
- Third-Party Apps Report

- Manage Users, Groups, and Endpoint Devices
- Manage Behaviour Analytics Configuration
- Integrate Cisco Identity Intelligence with Secure Access

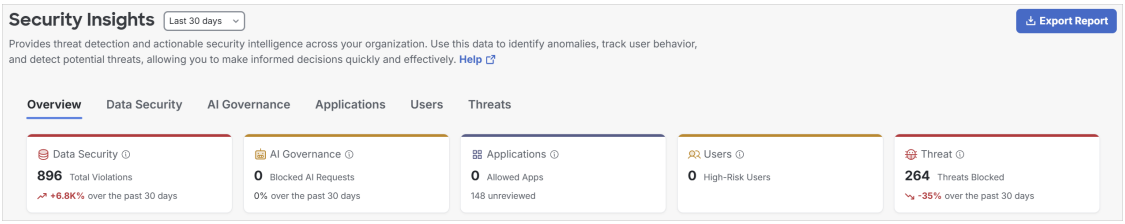
Security Overview Tab

Dashboard visibility into cross-domain summary of traffic sources, threat outcomes, and security enforcement for the selected time period.

The **Security Overview tab** of the Security Insights dashboard is the landing page for cross-domain security status. It summarizes what generated traffic, whether Secure Access allowed or blocked threats, and which enforcement controls acted on the traffic. Use the Security overview tab to understand overall security posture, traffic flow, threat outcomes, and enforcement activity across Secure Access.

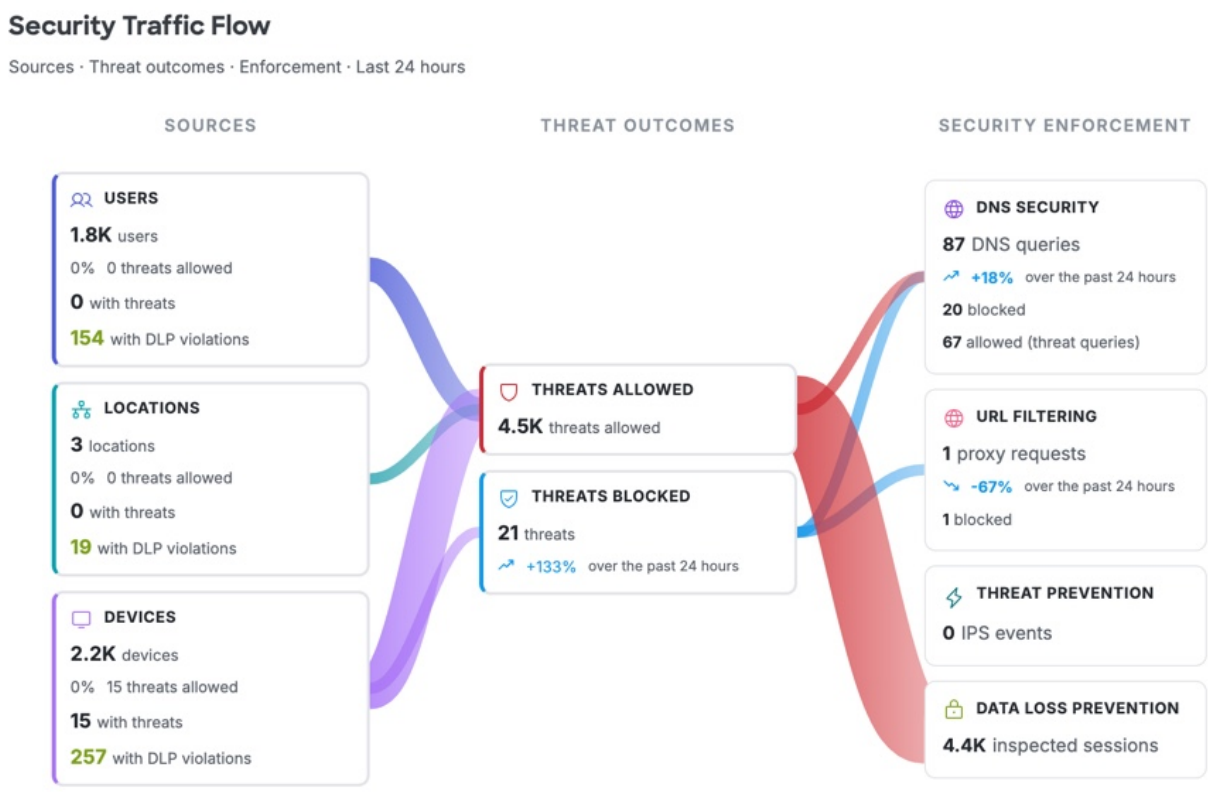
Summary cards

Shows a quick health snapshot for the other dashboard tabs and lets you move to the tab that matches the question you have.



Security traffic flow

A diagram that maps traffic from **Sources** → **Threat outcome** → **Security enforcement**. Shows which users, locations, sites, or devices generated traffic, whether threats were allowed or blocked, and which controls enforced the traffic. Use the period switcher (24 hours, 7 days, 30 days) at the top right. The default selection is **Last 24 hours**.



Column	Nodes	Where to learn more
Sources	Users, Locations, Devices	• Manage Users, Groups, and Endpoint Devices • Discover and Configure Catalyst SD-WAN Sites in SASE Management
Threat outcome	Threats allowed, Threats blocked	Events Report
Security enforcement	DNS security, URL filtering, Threat prevention, DLP / Inspection	• Events Report • Manage IPS Profiles • Manage the Data Loss Prevention Policy • Data Loss Prevention Report

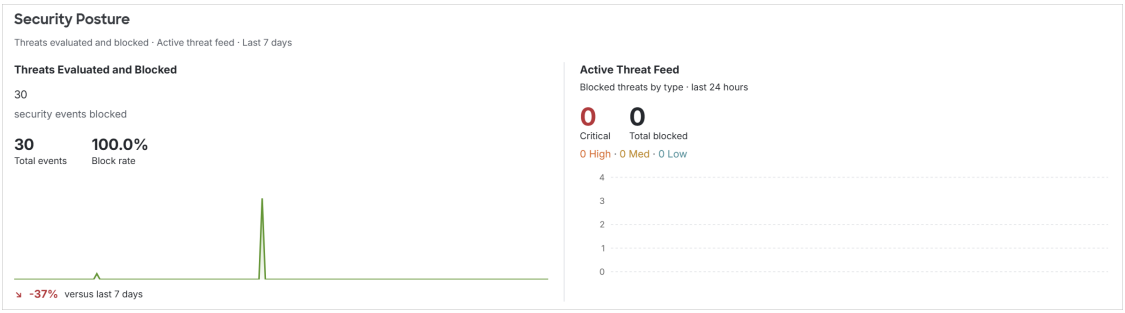
Hover over a card to highlight the related flows. Click a card to open a detail drawer.

Below the diagram:

- **Top Rules Allowing Threats** – Click a rule name to open the rule in the Access Policy.
- **30-day trend line** – Threats allowed versus blocked (fixed 30-day interval).

Security posture

- **Enforcement summary** – 30-day view of enforcement activity.
- **Active threat feed** – Blocked threats by severity and type over the last 24 hours, including malware, command-and-control, phishing, grayware, and cryptomining.



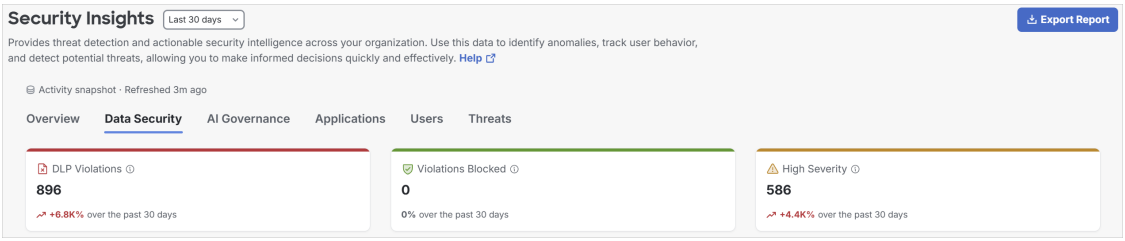
Data Security Tab

Dashboard visibility into Data Loss Prevention violations across channels and data classifications, with drill-down into users, rules, and destinations.

The **Data Security tab** of the Security Insights dashboard provides visibility into Data Loss Prevention (DLP) violations across channels and data classifications. Use this tab when you need to understand where sensitive data is moving, which rules are triggered, and who or what is responsible for violations. Use this tab with the Data Loss Prevention Report when you need the underlying events and filters.

Summary cards

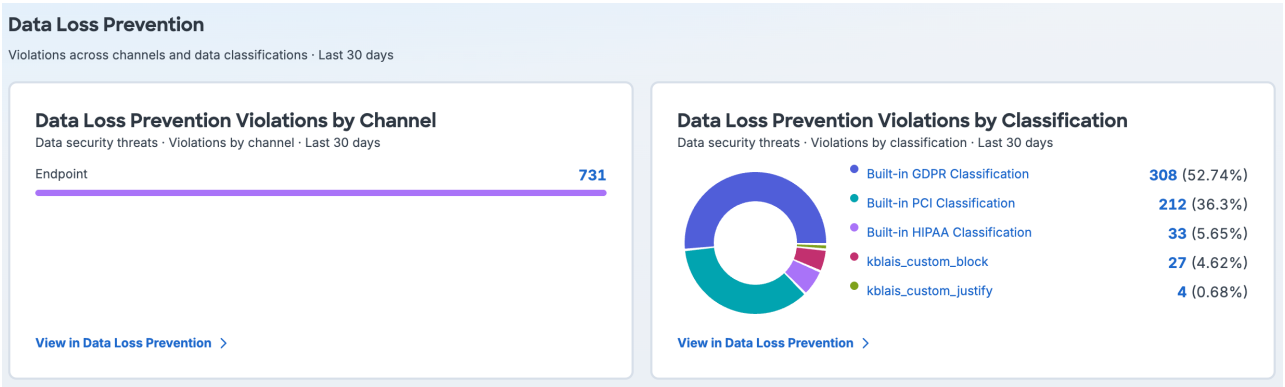
See total Data Loss Prevention violations, enforced violations, and high-severity violations for the current period.



Card	What it shows
DLP Violations	Total DLP policy matches across web, SaaS API, email, endpoint, and private apps (last 7 days), with delta versus previous 7 days
Violations Blocked	Violations blocked or quarantined before data left the organization
High Severity	Violations classified as Critical or High

Click any card to open the Data Loss Prevention Report.

DLP violations by channel and classification



- **Data Loss Prevention Violations by Channel** – Breakdown or trend view across Web, SaaS API, Email, Endpoint, Private Apps, and Other.
- **Data Loss Prevention Violations by Classification** – PII, Financial, HIPAA, Intellectual Property, and Other.

Top Data Loss Prevention Violations by User

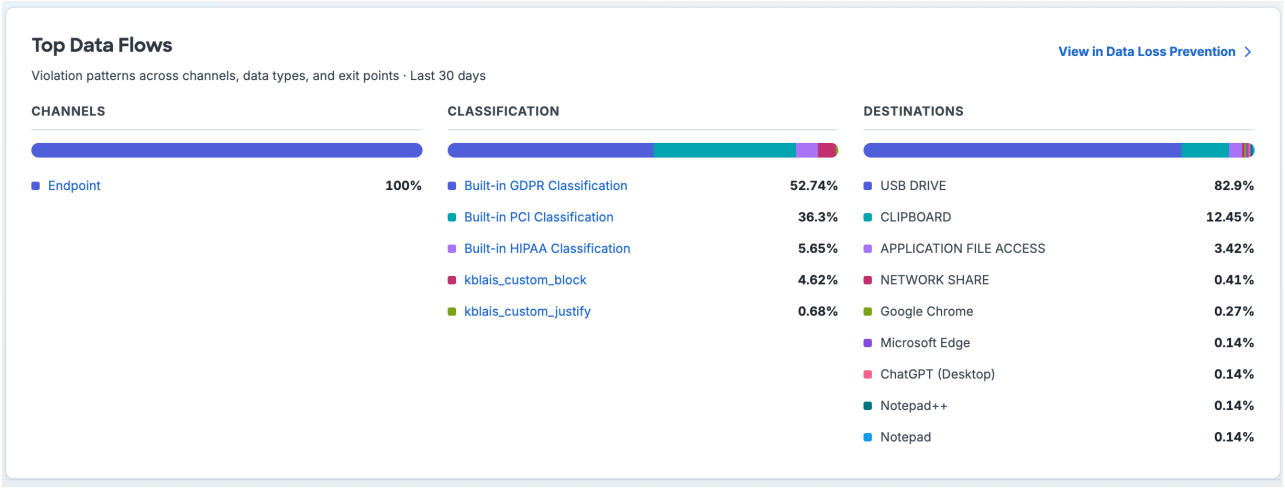
Users with the most policy violations over the last 30 days, including channel, violation count, and classification. Click **View all violators** to open the Data Loss Prevention Report.

Top DLP Rules Triggered and Apps Receiving Sensitive Data

- **Top Data Loss Prevention Rules Triggered** – By hit count over the last 30 days.
- **Applications Accessing Sensitive Data** – Destinations with DLP violations, with a breakdown or trend view.

Data Loss Prevention Violation Breakdown

Violation patterns across channels, data types, and exit points.



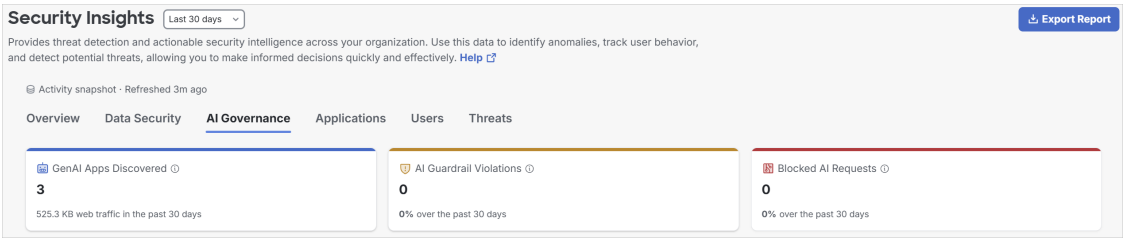
AI Governance Tab

Dashboard visibility into Generative AI application usage, AI Guardrail violations, and sensitive data sent to GenAI destinations.

The **AI Governance tab** of the Security Insights dashboard provides visibility into Generative AI application usage, AI Guardrail violations, and sensitive data sent to GenAI destinations. Use this tab when you want to review generative AI adoption and decide whether you need an app-centric investigation, a rule review, or a data protection review. Use the App Discovery Report for app-centric investigation and the Data Loss Prevention Report for content- and rule-centric investigation.

Summary cards

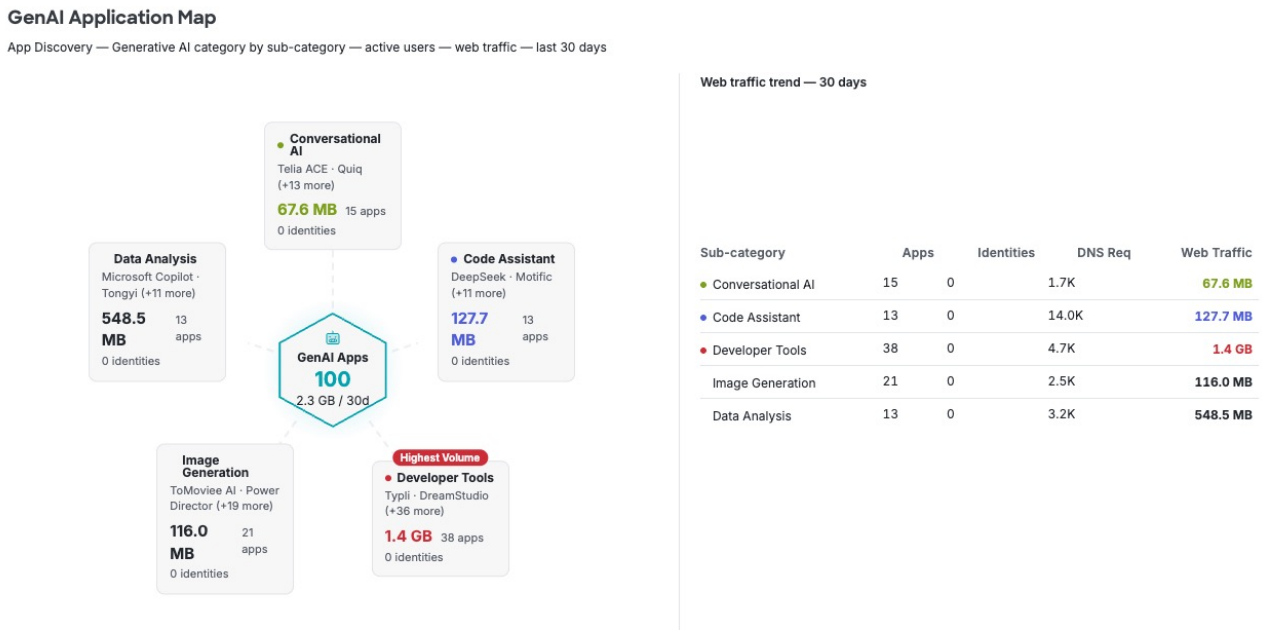
Shows the number of discovered GenAI applications, AI guardrail violations, and blocked AI requests.



Card	What it shows	Opens
GenAI Apps Discovered	GenAI apps found in App Discovery, across conversational AI, code assistants, image generation, developer tools, and data analysis	App Discovery Report
AI Guardrail Violations	DLP events scoped to AI Guardrail rules, including prompt injection, sensitive data in prompts, jailbreak attempts, and unauthorized model access	Data Loss Prevention Report
Blocked AI Requests	AI requests blocked by DLP, guardrail, and access policies	AI Activity view (not sure what this is?)

GenAI Application Map

A network diagram centered on GenAI apps, with nodes for the highest-volume and most-used sub-categories, plus developer tools, image generation, and data analysis. Each node shows apps, traffic volume, and identity counts. Includes a 30-day web traffic trend.



AI Guardrail Violations

Table of violations by type (Prompt Injection Attempt, Sensitive Data in Prompt, Jailbreak Attempt, Unauthorized Model Access, Ethical Violation), count, severity, and 30-day trend. Click a row to open the

Click **View in DLP Events** to open the Data Loss Prevention Report.

For more information, refer to Add an AI Guardrails Rule to the Data Loss Prevention Policy and Manage AI Guardrails Data Classifications.

DLP Violations for GenAI and Sensitive Data Sent to GenAI

- **DLP Violations for GenAI** – By data classification, last 30 days.
- **Sensitive Data Sent to GenAI** – By classification, detection type, and destination.

Click **View in DLP Events** to open the Data Loss Prevention Report.

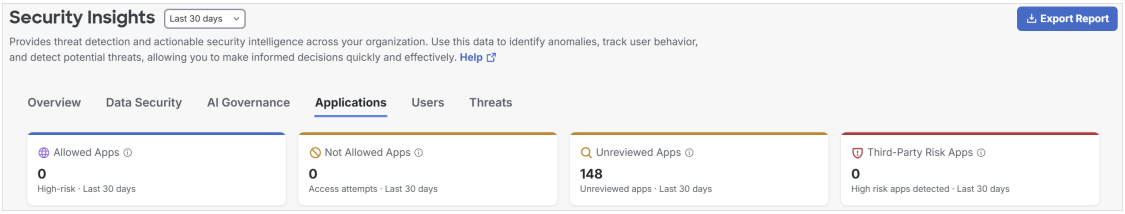
Applications Tab

Dashboard visibility into inventory and risk posture of applications in use, including third-party app authorizations.

The **Applications tab** of the Security Insights dashboard helps you understand application use and third-party application risk before you open detailed application reports. Use this tab when you want to review application adoption and decide where to allow, block, or investigate an application. Use this tab together with your Access Policy when you need to move from observed application use to policy changes.

Summary cards

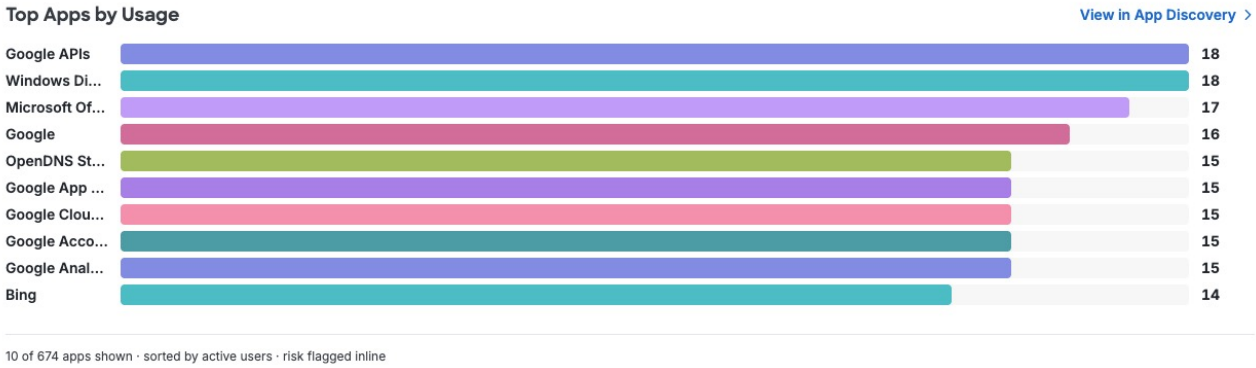
Shows how many applications are allowed, not allowed, unreviewed, or identified as third-party risk.



Card	What it shows
Allowed Apps	Apps permitted by policy. Click to open the App Discovery Report.
Not Allowed Apps	Apps blocked by policy. Click to open the Events Report.
Unreviewed Apps	Apps discovered but not yet categorized by policy. Click to open the App Discovery Report.
Third-Party Risk Apps	Third-party cloud apps authorized to access sanctioned tenant apps. Click to open the Third-Party Apps Report.

Top Apps by Usage

App usage alongside DNS request counts. Click **View in App Discovery** to open the App Discovery Report.



Not Allowed Apps and Top Risky Apps

- **Not Allowed Apps** – Apps that users are attempting to access despite policy restrictions. Click **View not allowed in Events** to open the Events Report.
- **Top Risky Apps** – Discovered apps with a risk score greater than 7.0. Click **View in App Discovery** to open the App Discovery Report

High Risk Third-Party Apps and Top Users with Risky Third-Party Apps

- **High Risk Third-Party Apps** – Sourced from the Third-Party Apps Report.
- **Top Users with Risky Third-Party Apps** – Users with the most high-risk app permissions. For more information, refer to View User Details

Click **View in Third-Party Apps** to open the Third-Party Apps Report.

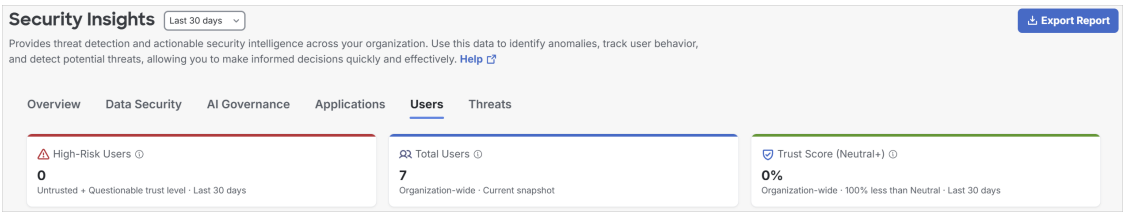
Users Tab

Dashboard visibility into user trust levels, top risky users, UEBA detections, and connection type distribution, scored by Cisco Identity Intelligence (CII).

The **Users tab** of the Security Insights dashboard provides visibility into user trust levels, top risky users, User and Entity Behavior Analytics (UEBA) detections, and connection type distribution, scored by Cisco Identity Intelligence (CII). Use this tab when you want an identity-first investigation path that starts with trust, recent detections, or how users connect. Trust level and behavior data are most useful when you pair this tab with Manage Behaviour Analytics Configuration.

Summary cards

Shows how many users are high risk, how many active users are scored, and what percentage of users are at Neutral or above trust.



Card	What it shows
High-Risk Users	Users at Untrusted or Questionable trust level
Total Users	Active users scored by CII
Trust Score (Neutral+)	Percentage of users at Neutral trust or above

For more information, refer to View Users Provisioned in Secure Access and Integrate Cisco Identity Intelligence with Secure Access

User trust levels, Top 5 risky users and Recent UEBA detections

Distribution of users across trust levels, and a list of the highest-risk users in the environment.

Detections from User and Entity Behavior Analytics, including:

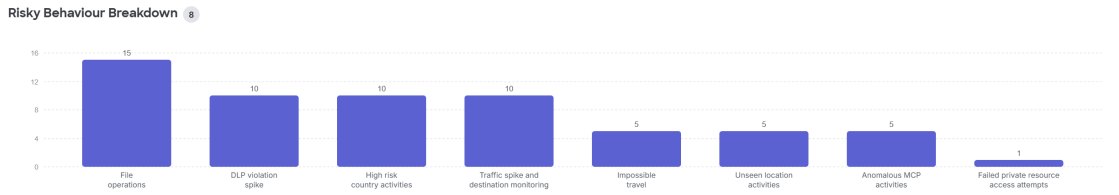
- Impossible Travel – Identify events from geographically distant locations within unrealistic timeframes.
- File Operations – Monitor file operation thresholds for downloads, uploads, and deletions within defined periods.
- DLP Violation Spike – Detect unusual increase in DLP policy violations within a specified time period.

- Failed Private Resource Access Attempts – Detect when an end user makes an unusually high number of failed attempts to access private resources through client-based ZTNA.
- High-Risk Country File Activities – Monitor file uploads sent to and file downloads from countries you designate as high-risk.
- Anomalous MCP Activity – Detect unusual Model Context Protocol (MCP) activity, including potential injection activity or a sudden increase in requests.
- Unseen Location Activity – Monitor user activity from a city or source IP address that was not observed for that user during the previous 60 days.
- Traffic Spike and Destination Monitoring – Detect unusual increase in requests to a specific destination or any TOR relay.

For more information, refer to View Users Provisioned in Secure Access and Integrate Cisco Identity Intelligence with Secure Access.

Risky behaviour breakdown

Distribution of UEBA-scored risky behaviors. For more information, refer to Add and Edit Alert Rules for Behavior Analytics.



Connection types: VPN versus ZTNA

Distribution of VPN versus ZTNA sessions over the last 30 days, with a toggle between breakdown and trend views. Click **View connection data** to open the Events Report.

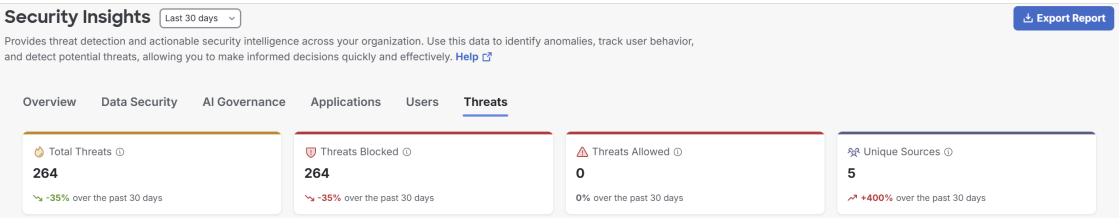
Threats Tab

Dashboard visibility into blocked and allowed threat activity, rule efficacy, threat trends, and the top risky destinations and blocked users.

The **Threats** tab of the Security Insights dashboard helps you identify where Secure Access blocks threats, where policy allows threats, and which rules, destinations, categories, or users require follow-up. Use this page when you need to separate detection coverage from policy gaps and decide whether to tune policy, investigate users, or review destinations. Use this page with the Events Report when you need to inspect the underlying detections.

Summary cards

Shows how many threats were blocked, how many were detected overall, how many were allowed, and how many distinct sources generated the activity.



Card	What it shows
Total Threats	Combined count of blocked and allowed threats

Card	What it shows
Threats Blocked	Threats blocked by DNS security, web security, firewall, and IPS policies
Threats Allowed	Threats detected but not blocked – indicates enforcement gaps
Unique Sources	Distinct source IPs or user identities generating threat traffic

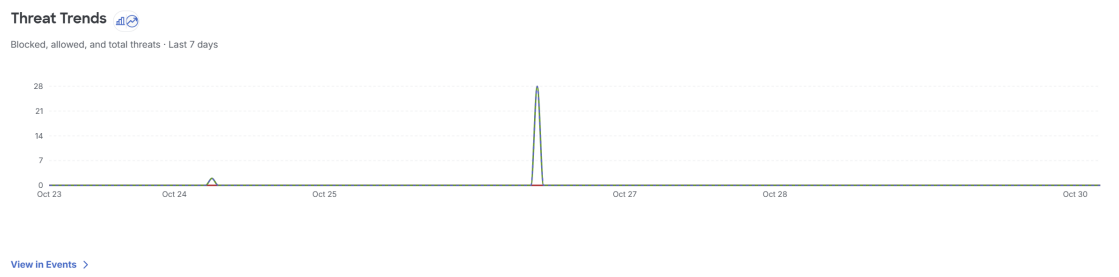
Click a card to open the Events Report.

Blocked and allowed threats and Top rules allowing threats

- **Blocked and Allowed Threats** – Shows which threat categories Secure Access blocked and which categories still reached users or destinations. By category: Command and Control, Malware, Grayware, Phishing, Cryptomining.
- **Top Rules Allowing Threats** – Shows which rules permit traffic that later matched threat detections. Policies permitting threat traffic; review recommended.

Threat trends

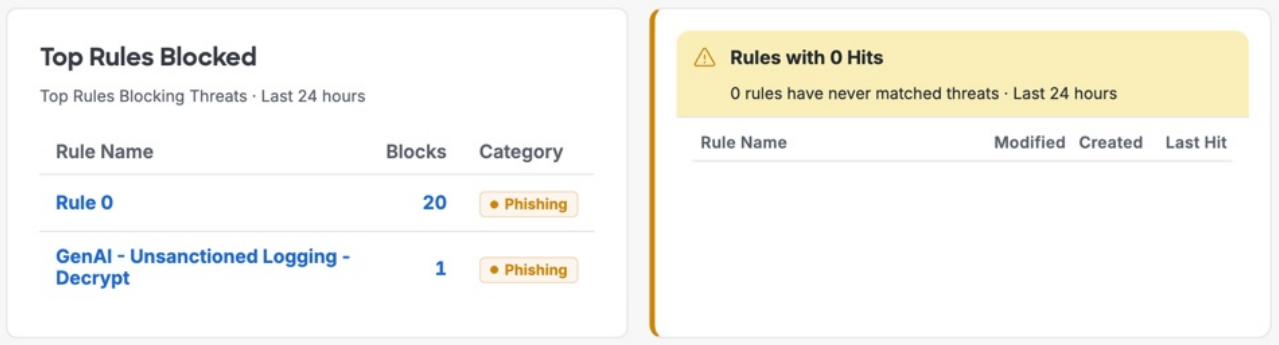
Shows whether blocked, allowed, and total threat volume is rising or falling over time.



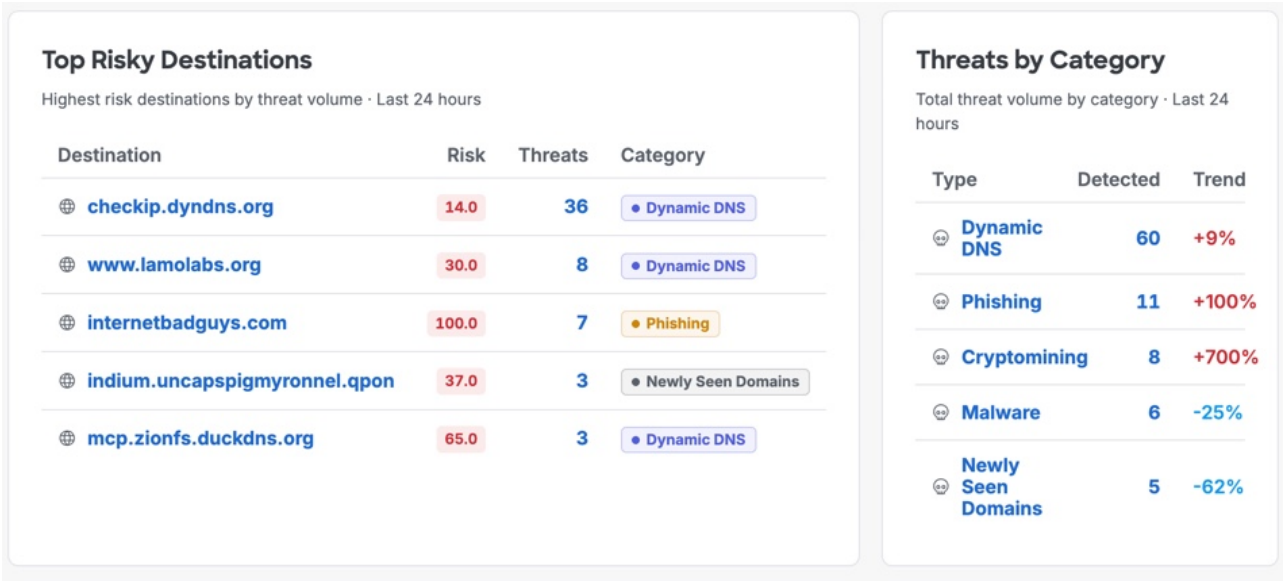
Toggle between stacked threat volume and a line chart of blocked, allowed, and total threats (30 days). Click **View in Events** to open the Events Log.

Detection efficacy

- **Top Rules Blocked** – Rules generating the most blocks.
- **Rules with 0 Hits** – Rules that have never matched threats in the past 24 hours. This time frame is always 24 hours.



- **Top Risky Destinations** – Highest-risk destinations by threat volume.
- **Threats by Category** – Detected volume by threat type over the last 30 days.



Top blocked users

Users generating the most blocked threat traffic over the last 30 days. Click through to Manage Users, Groups, and Endpoint Devices.

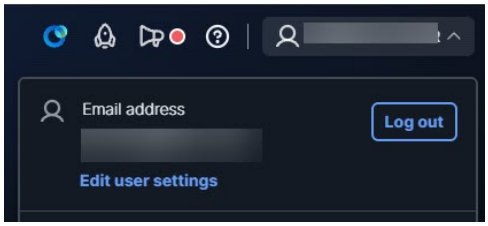
Set Background Theme

Describes how to set the user interface theme of Secure Access to a light theme, dark theme, or to adopt the theme your system uses.

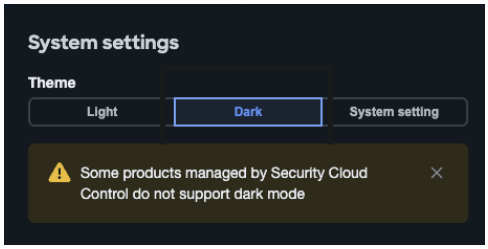
This procedure describes how to set the user interface theme of Secure Access to light theme, dark theme, or to adopt the theme your browser uses. Most integrated products and platform pages in Secure Access use the theme you set.

Procedure

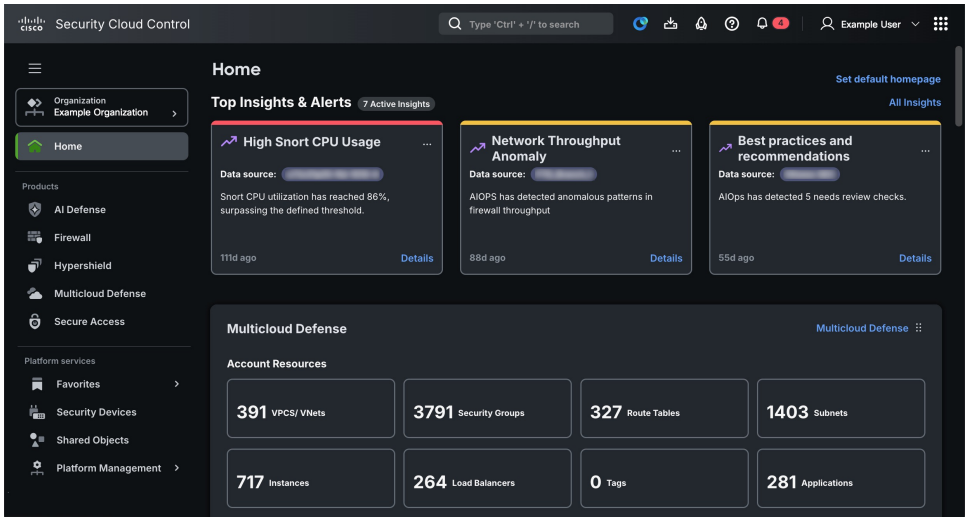
1. From the home page of Security Cloud Control or any integrated product page, click the user menu and select **Edit user settings**



2. In the **System settings** area, choose from:
   - Light theme
   - Dark theme
   - System theme - The system theme adopts the theme your browser uses.



Here is an example of Security Cloud Control using the dark theme:



Secure Access Status Portal

The Cisco Secure Access Status Portal enables you to quickly see the current status of Secure Access in your region, and to access relevant current, upcoming, and historical service information.

The Cisco Secure Access Status Portal makes incident and maintenance information easier to find, filter, and review. In the status portal, you can quickly access relevant current, upcoming, and historical service information, including a list of current and historical maintenance events with detailed time ranges, regions, and impact descriptions. The portal includes:

- Tabbed navigation
- Keyword search
- Impact and component filters
- Compact upcoming-maintenance cards
- Interactive calendars
- Expand/collapse controls

You can access the Status Portal at: https://status.sse.cisco.com.

It allows you to:

- Verify whether a service issue is platform-related or local (Interpreting Cloud Security Platform Service Status)
- Identify region-specific impacts (Interpreting Cloud Security Platform Service Status)

- Understand incident severity and scope (View Service Status History)
- Track planned maintenance activities (View Scheduled Maintenance)
- Subscribe to notifications for proactive awareness (Manage Outage Notifications)

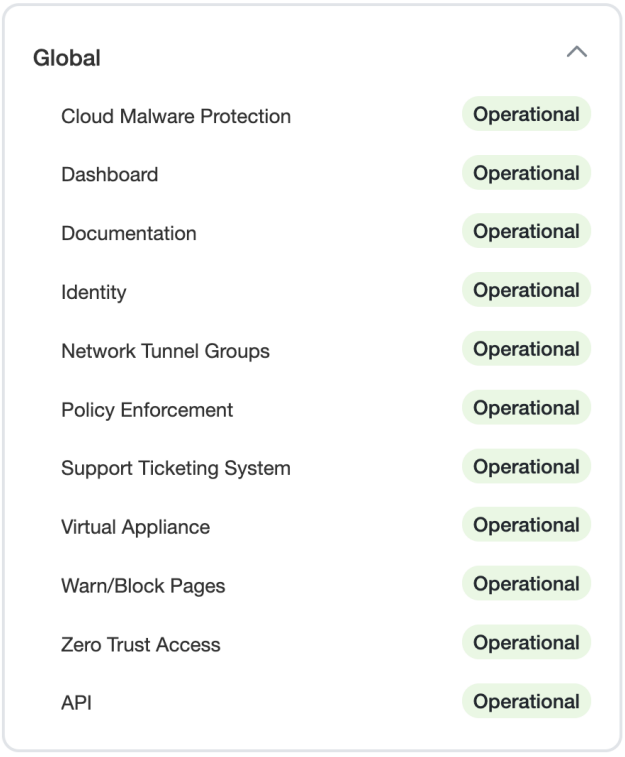
Interpreting Cloud Security Platform Service Status

Describes Interpreting Cloud Security Platform Service Status in Cisco Secure Access. The Cloud Security Platform section on the Cisco Secure Access Service Status page provides visibility into the operational status of Secure Access services from both a global and a region-specific perspective.

The **Cloud Security Platform** section on the Cisco Secure Access Service Status page provides visibility into the operational status of Secure Access services from both a global and a region-specific perspective. Administrators use this information to understand the scope of service-impacting events and to determine whether observed behavior affects all users or only users in specific locations.

Global Status

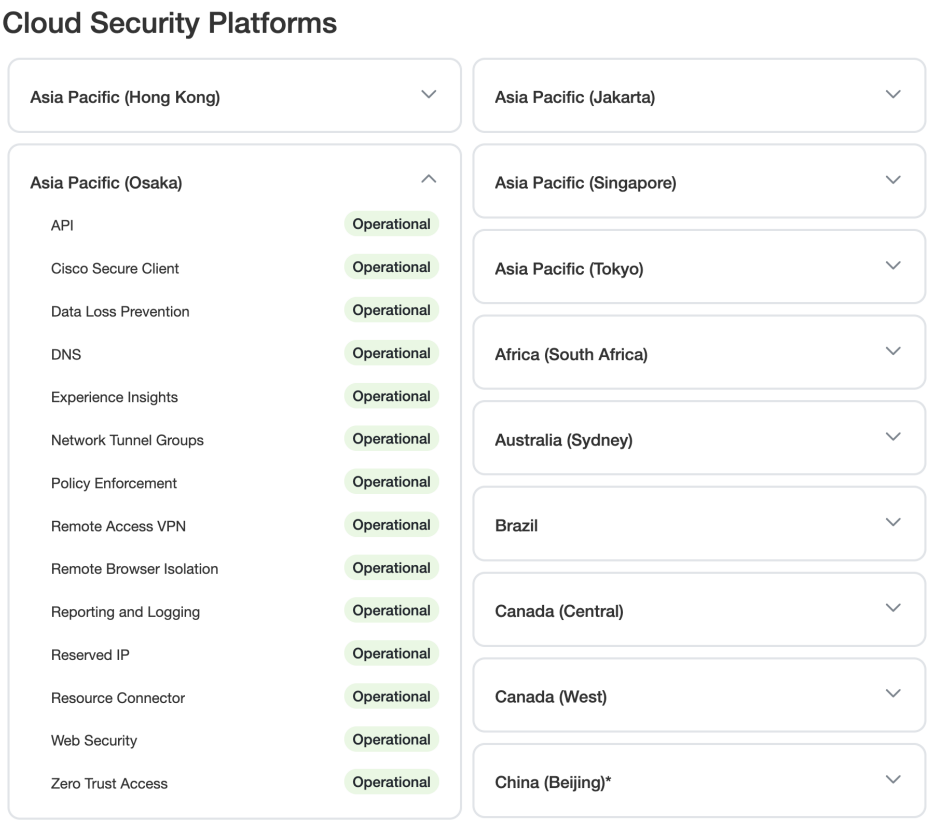
The **Global** view displays the status of Secure Access services aggregated across all regions. Expand **Global** to view the list of Secure Access services and their current operational state based on active incidents or maintenance events.



Administrators should use the **Global** view to determine whether a service condition is widespread and potentially affecting users across multiple regions.

Region-Specific Status

The region-specific view displays the status of Secure Access services for a specific geographic region. Expand a region to view the list of services and their current operational state for that region.



Administrators should use the region-specific view to identify localized service impact, especially when user issues are limited to a specific region or access location.

Service Status Definitions

The Cloud Security Service Status describes the state of a service component using one of the following statuses. These definitions apply to both Global and region-specific service status views.

- **Operational**–The service is available and functioning as expected.
- **Under Maintenance**–Scheduled or ongoing maintenance is being performed. During maintenance, traffic is automatically redirected to the closest available data center to ensure continued service availability. No user action is required.
- **Degradation**–The service remains online, but users may experience reduced performance or partial impact.
- **Outage**–A data center is unreachable. To maintain service continuity, traffic to Cloud Security services is automatically routed using Anycast.

Secure Access Service Descriptions

The Cloud Security Platform section lists Secure Access services whose operational status is displayed at both the Global and Region-specific levels. The following descriptions help administrators understand the functional scope of each service when interpreting service status information.

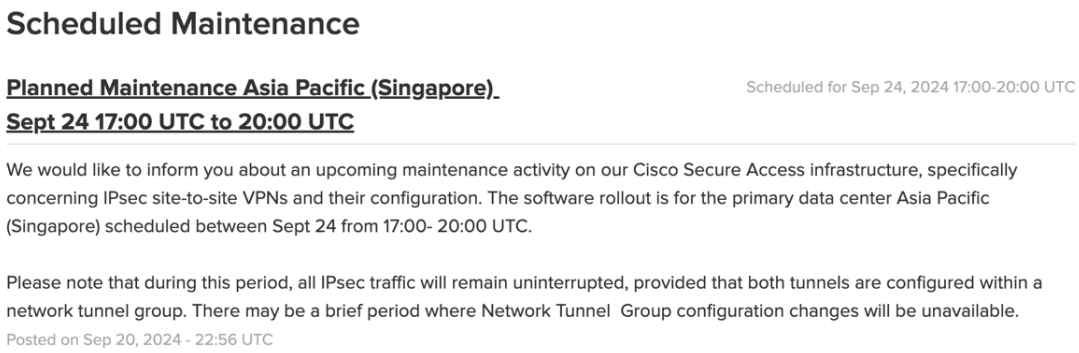
- **API**–Platform API services that support programmatic access, automation, integrations, and administrative operations within Cisco Secure Access.
- **Cisco Secure Client**–Services that support Secure Access client connectivity, including client-based access to internet, SaaS, and private applications.
- **Cloud Malware Protection**– Detects and removes malware from cloud-based file storage applications. It enriches security protection by scanning files automatically and flagging malicious content for remediation, supporting services such as Box, Dropbox, Webex, Microsoft 365, Google Drive, AWS S3, and Azure.

- **Dashboard**–Provides visibility in reports and applied policies down to the user level by leveraging Cisco Secure Client, Virtual Appliances, and third-party integrations.
- **Data Loss Prevention**–Services that inspect traffic to detect and prevent the exposure of sensitive data based on configured data protection policies.
- **DNS**–Secure DNS resolution and enforcement services used to apply security policies, control domain access, and route user traffic.
- **Documentation**–Provides access to user guides and API programming guides for Secure Access services.
- **Experience Insights**–Services that collect and analyze user experience and performance data to provide visibility into connectivity quality and service behavior.
- **Identity**–Integrates identity trust levels into Secure Access, enabling adaptive access policies based on live identity data and user trust profiles.
- **Network Tunnel Groups**–Services that manage network tunnel groups used for establishing and maintaining secure tunnels between customer networks and Cisco Secure Access.
- **Policy Enforcement**–Core enforcement services responsible for applying security and access policies across Secure Access traffic flows.
- **Remote Access VPN**–Services that provide secure remote connectivity for users accessing internet, SaaS, and private resources through Cisco Secure Access.
- **Remote Browser Isolation**–Services that isolate web browsing sessions in a remote environment to protect users from web-based threats.
- **Reporting and Logging**–Services that generate, store, and provide access to logs and reports related to Secure Access traffic, security events, and system activity.
- **Reserved IP**–Services that manage reserved public IP addresses used for consistent source IP presentation for Secure Access traffic.
- **Resource Connector**–Services that manage Resource Connector Groups and individual Resource Connectors used to provide access to private resources.
- **Support Ticket System** –Provides technical support access, case management, and assistance for Secure Access software and services.
- **Virtual Appliance**–Services related to the deployment, management, and operation of virtual appliances that support Secure Access functionalities.
- **Warn/Block Pages**–Services that display warning or block pages to users when access to certain resources is restricted or blocked based on security policies.
- **Web Security**–Secure web gateway services that inspect and enforce security policies on web traffic accessed through Cisco Secure Access.
- **Zero Trust Access**–Zero Trust Access services that control user access to private applications based on identity, device posture, and policy.

Scheduled Maintenance

Describes Scheduled Maintenance in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access provides details about the scheduled maintenance on the platform services.



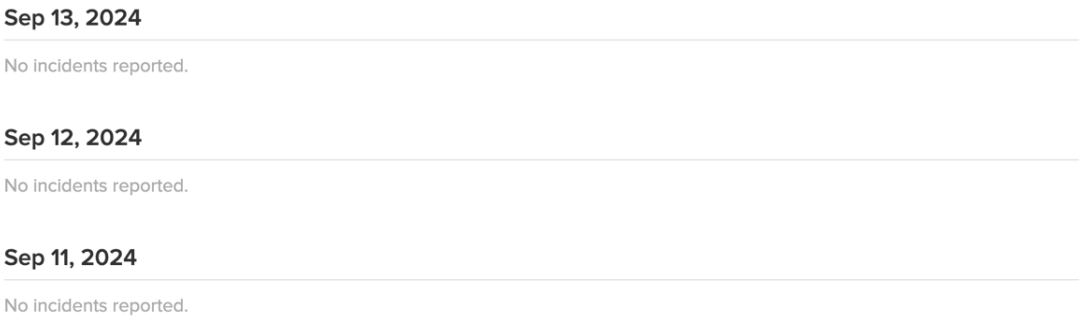
Service Status History

Describes Service Status History in Cisco Secure Access and explains No Incidents Reported and Past Incidents. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access lists the daily status of the platform services. Secure Access reports that no incidents happened for that time period or describes the details about an incident and its resolution.

No Incidents Reported

If no service incidents occurred on the platform during the twenty-four hour time period, Secure Access displays **No incidents reported**.



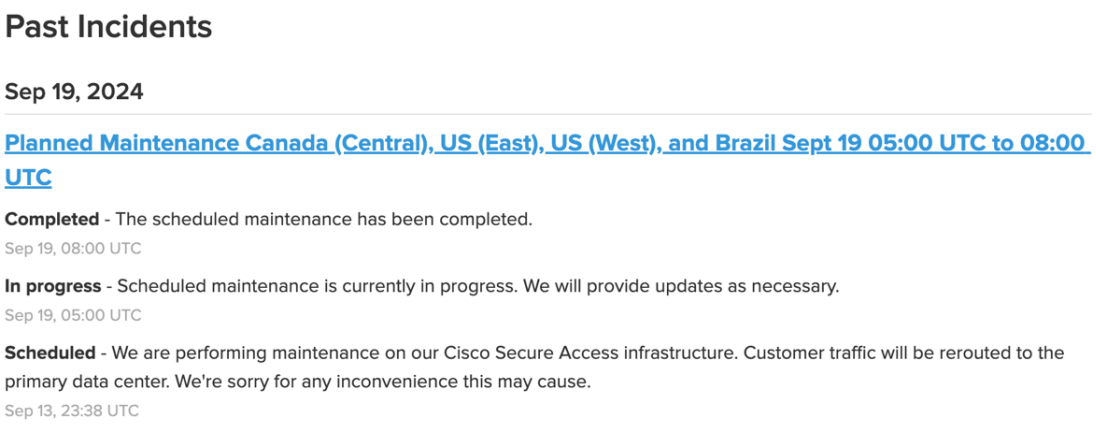
Past Incidents

Secure Access reports the details about an incident or scheduled maintenance on the platform for a twenty-four hour time period.

If an incident occurred, Secure Access displays the sequence of steps taken to resolve the incident on the platform. Secure Access also provides information about the scheduled maintenance on the platform.

Secure Access reports the history of an incident:

- **Investigating**–The service event is under investigation.
- **In progress**–The scheduled maintenance is in progress.
- **Scheduled**–Secure Access is performing maintenance on the platform.
- **Completed**–Secure Access has completed the scheduled maintenance.
- **Identified**–The cause of the service event is known.
- **Update**–An update of the state of the services.
- **Monitoring**–Secure Access resolved the incident and is monitoring the platform services.
- **Resolved**–The service event is resolved.



Manage Outage Notifications

Provides instructions for completing the Manage Outage Notifications workflow in Cisco Secure Access. You can manage outage notifications directly from the Cisco Secure Access Service Status page to receive alerts about service-impacting events.

You can manage outage notifications directly from the Cisco Secure Access Service Status page to receive alerts about service-impacting events.

Procedure

1. Open a web browser and navigate to the Cisco Secure Access Service Status page (https://status.sse.cisco.com).
2. Select **Manage Outage Notifications**.
   The notification management panel opens.
3. Choose one or more notification methods.
   - **Email**–Enter one or more email addresses to receive outage and maintenance updates.
   - **SMS**–Enter a mobile phone number to receive text message alerts.
   - **Slack**–Connect a Slack workspace and select a channel to post notifications.
   - **Webhook**–Provide a webhook URL to receive structured status event payloads.
4. Save your notification settings.
   The selected recipients begin receiving notifications for future status events.
5. To modify or stop notifications, reopen **Manage Outage Notifications**.
   You can add, update, or remove notification methods at any time.

You are subscribed to Cisco Secure Access service status notifications and will receive alerts when outages, incidents, or maintenance events are posted or updated.

3 Cisco Assistant for Secure Access

Topics:

- Get Started with the Cisco Assistant
- Add Rules with the Cisco Assistant
- Find Documented Answers with the Cisco Assistant
- Troubleshoot Access Issues with Private Resources
- Optimize Access Policies
- Messages Generated by the Cisco Assistant
- Create Cisco Support Cases

Provides an overview of Cisco Assistant for Secure Access, including Get Started with the Cisco Assistant, Add Rules with the Cisco Assistant, and Find Documented Answers with the Cisco Assistant. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with the Cisco Assistant

The Cisco Assistant provides AI support for configuring rules, finding documented information, and troubleshooting private resources.

The Cisco Assistant for Secure Access interprets your natural language prompts to do the following:

- Create internet and private access rules on your policy
- Find documented answers to your questions
- Troubleshoot access to private resources

The Cisco Assistant currently supports interactions only in the English language. The Assistant may display inaccurate information. Make sure to verify the responses.

Prerequisites

To use the Cisco Assistant in Secure Accounts, you must have a full admin user role. For more information, see Manage Accounts.

Use the Cisco Assistant

Understand how to prompt and use the Cisco Assistant for Secure Access.

Launch and prompt the Cisco Assistant to add rules to your policy or learn from Secure Access documentation.

Procedure

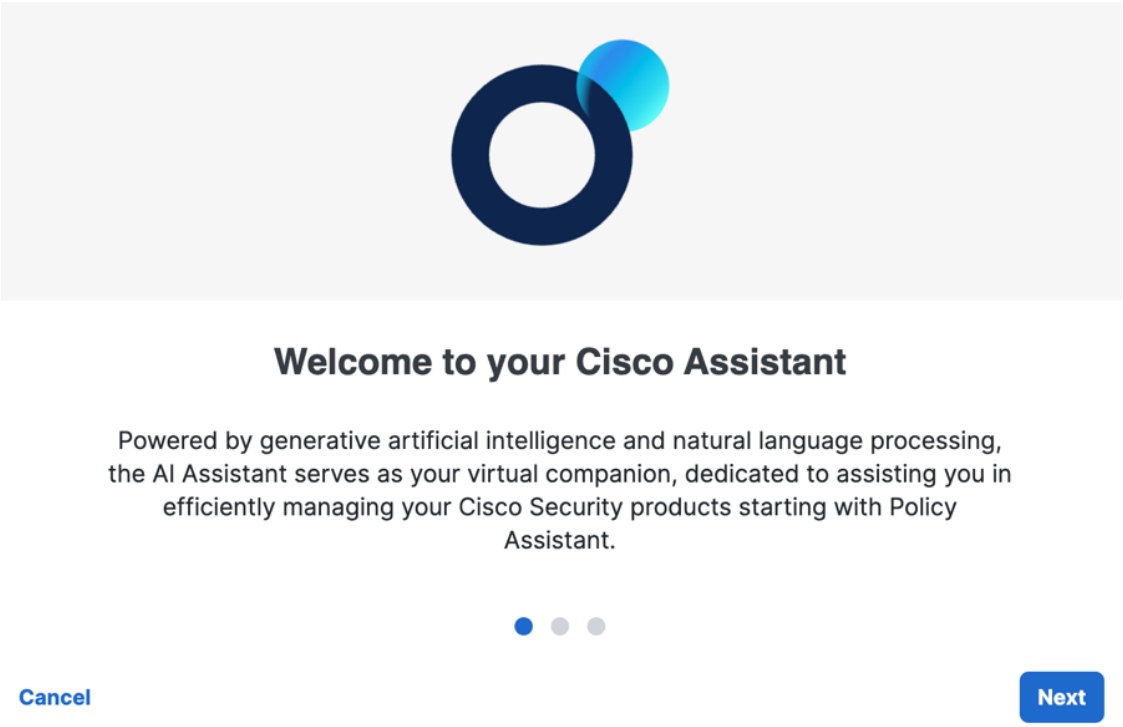
1. Click the Cisco Assistant icon in the Secure Access toolbar to open the AI app.

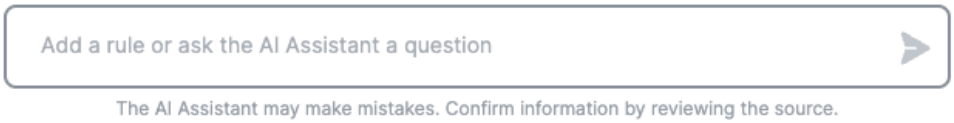
   Find the toolbar at the top of your browser window.

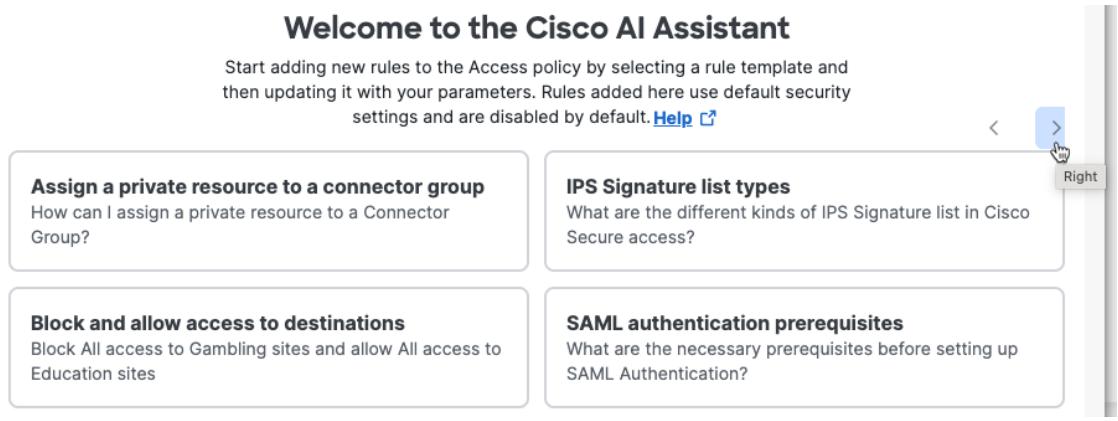
2. You will see the **Welcome to your Cisco Assistant** screen the first time you launch the Cisco Assistant. Click **Next**, review the tips for working with the Cisco Assistant, then click **Launch AI Assistant**.



3. Type your natural language prompt in the Cisco Assistant prompt bar. You can add rules to your policy or ask a question that will be answered with references to Secure Access documentation.

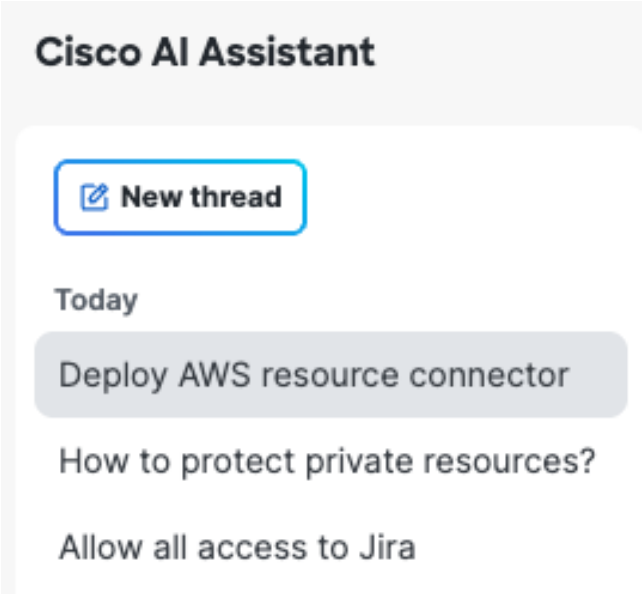


4. The Assistant presents example prompts that you can click to use. New example prompts are generated each time you open the Assistant menu.



- Click **Right** (> or right chevron) and **Left** (< or left chevron) to see all examples.
- Example prompts that ask questions will prompt the Assistant immediately to generate an answer from documentation. For more information, see Find Documented Answers with the Cisco Assistant.
- Example prompts that add a rule will not prompt the Assistant immediately. The Assistant will load the text of the rule prompt in the prompt bar and wait for you to press enter before generating a response. For more information, see Add Rules with the Cisco Assistant.

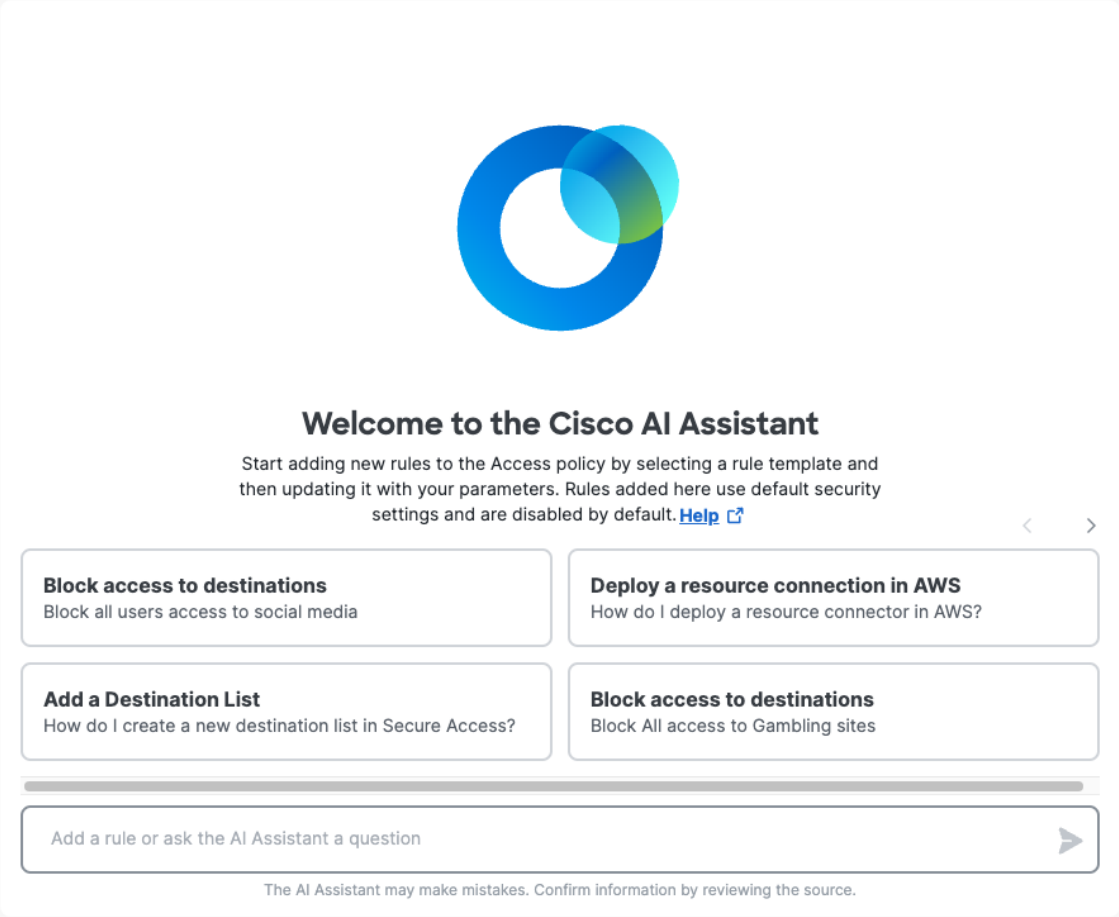
5. Each prompt will start a new thread. Access the history of your threads on the left side of the Assistant menu.



Cisco Assistant Navigation

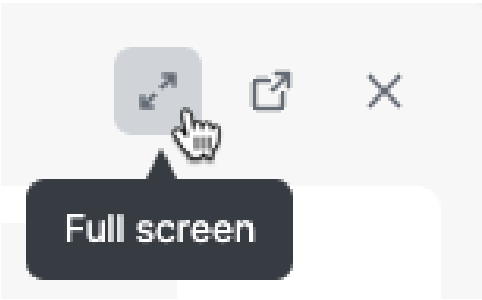
Provides instructions for completing the Cisco Assistant Navigation workflow in Cisco Secure Access. Cisco Assistant navigation tools help you work with the AI app.

Cisco Assistant navigation tools help you work with the AI app. You can find the tools on the Assistant's top and left side navigation menus.

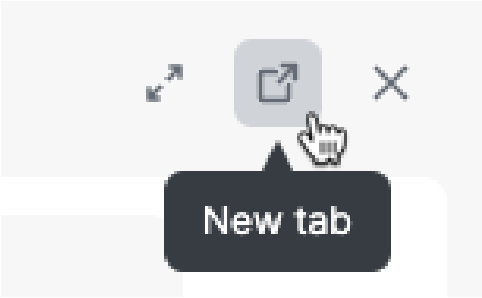


Procedure

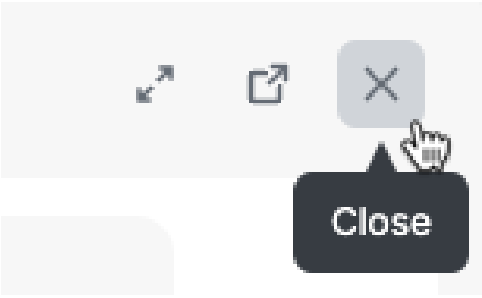
1. Click the **Full screen** icon (outward pointing arrows) to expand the Assistant to the full browser width and height.



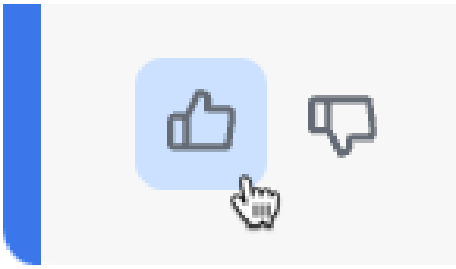
2. Click the **New tab** icon (box with arrow out) to load the Assistant in a new browser tab.



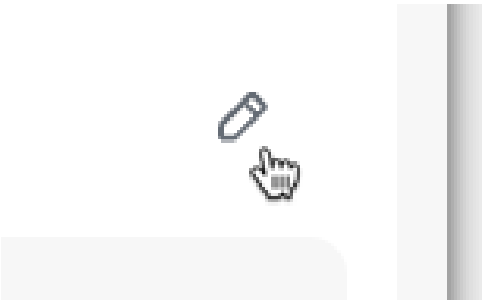
3. Click the **Close** icon (X mark) to close the assistant.



4. Click the **Feedback** icon (thumbs-up or thumbs-down) at the bottom of each Assistant response to approve or disapprove of the response, and optionally to provide additional feedback. We will use your feedback to improve the AI Assistant over time.



5. Click the **Revise** icon (pencil) next to each completed query to rephrase the query and generate a new response.



6. Click the **New Thread** button at the top left to start a new conversation with the Assistant.



Add Rules with the Cisco Assistant

Understand the capabilities, limitations, and built-in safeguards for the Cisco Assistant in Secure Access.

Prompt the Cisco Assistant for Secure Access to add access rules to your organization's policy. Access rules determine whether users and user devices can connect securely to the internet and your organization's private resources. For more information, see Manage the Access Policy.

- **Internet access rules**–Control managed device access to resources on the internet. For more information, see Manage Internet Access Rules

- **Private access rules**–Control access to applications hosted on your data center. For more information, see Get Started With Private Access Rules

To create rules with the Assistant, your natural language prompts must define valid rules and must include include:

- **Source and destination**–Request rules for sources and destinations already configured in your organization or use the Assistant to configure a new source and destination.
- **Rule action**–You must add an action that the rule will apply.

Capabilities

- Interpretation of natural language prompts
- Configuration of internet or private access rules in policy
- Detection of access rule type
- Creation of multiple rules in a single prompt thread
- Spelling suggestions for source and destination names
- Safe and respectful interaction with Secure Access administrators

Limitations

- Cisco Assistant is available in Secure Access to create access rules.
- Cisco Assistant interprets only text-based, in-scope command prompts.
- Cisco Assistant may return false or inaccurate information.
- Cisco Assistant does not interact with or update any other settings, profiles, API keys, network components, or network connectors in the organization.

Safeguards

- Cisco Assistant saves your conversational instructions or prompts and has data protection safeguards built into the application.
- Cisco Assistant does not remove any data from your organization and can not add a policy rule without an administrator's approval.
- Cisco Assistant guarantees that the generated access rule is valid and only contains the correct source and destination components for the policy type with the appropriate rule actions.
- Cisco Assistant is restricted in its generative capabilities and prevents inappropriate interactions with the application.
- Rules created by the Cisco Assistant are disabled by default.
- Secure Access logs the addition of rules to your policy, including rules generated by the Cisco Assistant. For more information, see Admin Audit Log Report.

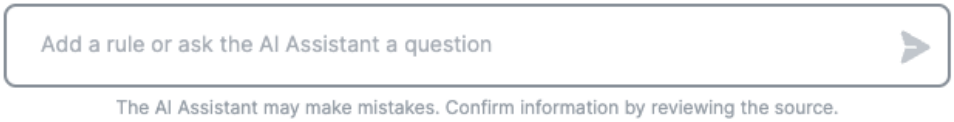
Enter a Natural Language Prompt to Generate Policy Rules

Provides instructions for completing the Enter a Natural Language Prompt to Generate Policy Rules workflow in Cisco Secure Access. Click the Cisco Assistant icon in the Secure Access toolbar, then enter your prompt to create access rules.

Click the Cisco Assistant icon in the Secure Access toolbar, then enter your prompt to create access rules. For more information, see Use the Cisco Assistant on page 91.

Procedure

1. In the prompt bar, enter your natural language instructions to create policy rules.

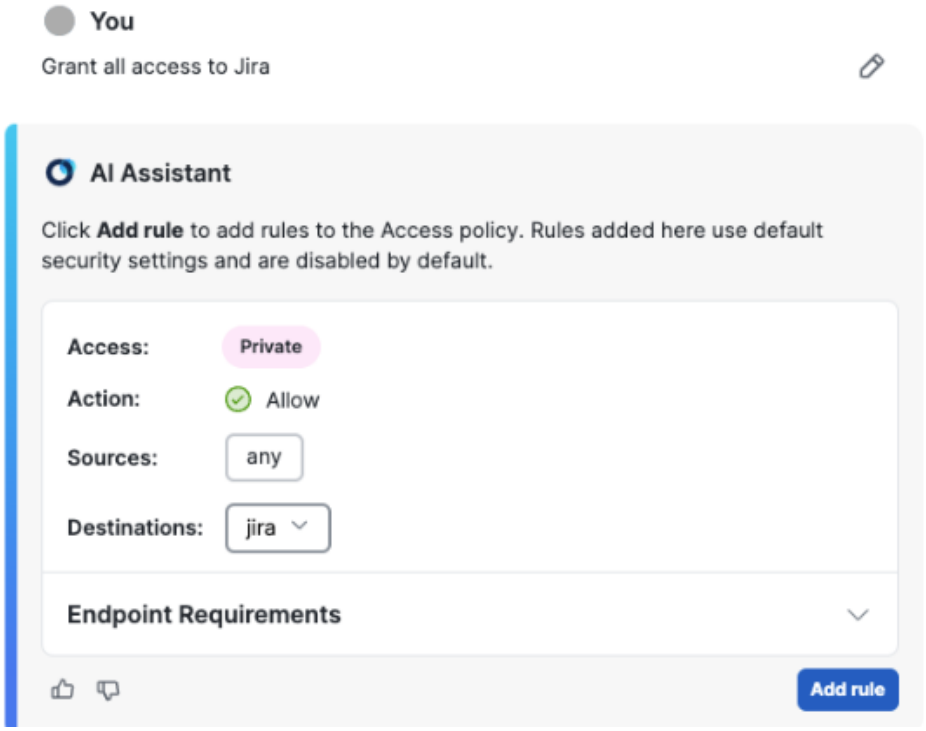


For more information about prompts and generating policy rules, see Cisco Assistant Rule Examples.

Sample Prompt:

```
Grant all access to jira
```

The assistant will reply with a card presenting the interpreted rule access, action, source, and destination. For more information, see the Core Prompt Components section in Cisco Assistant Rule Examples.



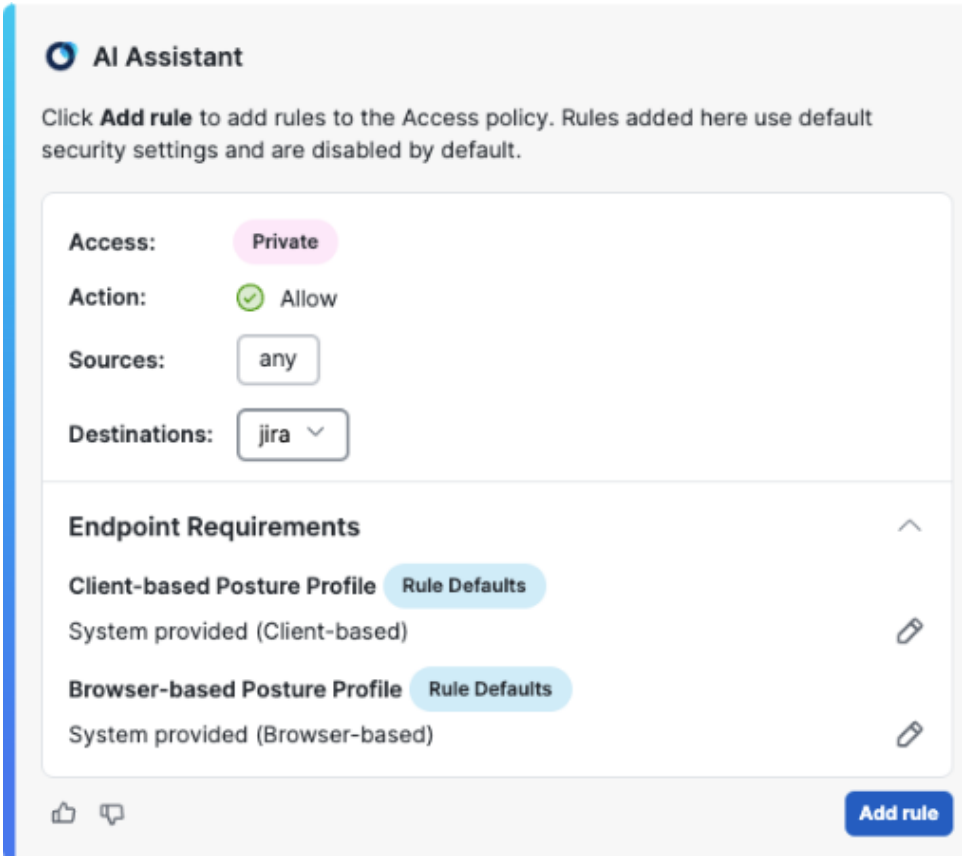
Note

If the assistant is unable to interpret the prompt in a way that it cannot resolve by presenting options, it will reply by explaining that the prompt is invalid. Enter a new prompt in the prompt bar or click the **Revise**icon (pencil) to clarify and resubmit the prompt.

2. Use the options in the reply to clarify the prompt, or click the **Revise** icon (pencil) next to the completed prompt to rephrase it and generate a new response.



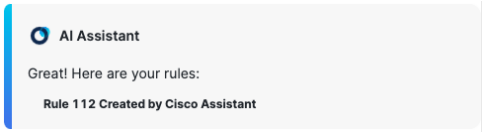
If the prompt action is to allow access to a private resource, the assistant offers options to customize Endpoint Requirements when connecting to the private resource using Zero Trust Access.



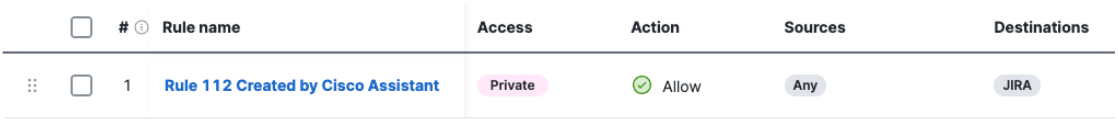
Click the **Revise** icon (pencil) to apply a custom Client-based Posture Profile or Browser-based Posture Profile to your rule.

Endpoint Requirements only apply when the rule action is to allow access to a private resource. For more information, see Manage Zero Trust Access Posture Profiles.

3. The **Add rule** button will become active when the prompt is clear enough for the assistant to interpret it. Click **Add rule**, and Secure Access adds the rule to your policy with the highest priority.



4. Browse to **Secure** > **Access Policy** to view the rule generated by the assistant.



> **Note**
>
> Rules generated by the assistant have a **Rule name** that ends with the phrase: **Created by Cisco Assistant**.

Cisco Assistant Rule Examples

Describes Cisco Assistant Rule Examples in Cisco Secure Access. The Cisco Assistant for Secure Access can create internet and private access rules in your policy from natural language prompts.

The Cisco Assistant for Secure Access can create internet and private access rules in your policy from natural language prompts. The assistant requires that you compose the prompts with your organization's rule components and actions. For more information, see the **Procedure** in Use the Cisco Assistant on page 91.

We recommend that you review the prompt samples before you begin to interact with the assistant and generate access rules.

Core Prompt Components

- **Action**–One of the rule actions to apply on the rule components. The actions available to a rule depends on the type of the rule.
- **Source**–The source components configured in your instance of Secure Access. Various source types are available on each policy rule type.
- **Destination**–The resource components configured in your instance of Secure Access.

Key Words for Prompts

- **Allow**–Action used in a prompt to generate both internet and private access rules.
- **Grant**–Allow the source and destination on the rule.
- **Give**–Allow the source and destination on the rule.
- **Block**, **Prevent**–Action used in a prompt to generate both internet and private access rules.
- **Warn**–Action used in a prompt to generate only internet access rules.
- **Isolate**–Action used in a prompt to generate only internet access rules.
- **Access to**–Use the phrase to complete the connection between the source and destination.
- **From**–Use the preposition to indicate the connection between the source and destination.
- **And**–Operator used in a prompt to generate multiple rules with various components and rule actions. For example: `Allow Thomas and Block John access to Jira`.
- **Not**, **But Not**–Operator used in a prompt to exclude certain components (source or destination) on multiple rules with various components and rule actions. For example: `Allow Suzy not John and Block John access to Jira`.
- **Any User**–Apply the rule to any one of the users in the organization.
- **All Users**–Apply the rule to all of the users in the organization.
- **No User**–Apply the rule to none of the users in the organization.

- **Any Protocol**–Permit the rule to apply to a destination that has any protocol.

> **Note**
>
> Use must include a **port** value with the **Any Protocol** option in the prompt.

- **Any Private Resource**–Permit the rule to apply to any private resource.
- **Create a Rule**–Prefix included before the core components of the prompt.
- **Call Rule**, **Call this Rule**–Use the phrase in a prompt to name the generated rule.

Private Access Rule Examples

Prompts for private access policy rules must include an **Action** to apply to the components on the rule, and **Source** and **Destination** components. The assistant requires these core components to create an appropriate access rule.

```
Allow <source> access to <destination>
```

```
Block <source> from <destination>
```

```
Block <source> from <destination_one> and Allow <source> access to
<destination_two>
```

```
Block <source> not <source> from <destination_one> and Allow <source> access
to <destination_two>
```

Internet Access Rule Examples

Prompts for internet access policy rules must include an **Action** to apply to the components on the rule, and **Source** and **Destination** components. The assistant requires these core components to create an appropriate access rule.

```
Allow <source> access to <destination>
```

```
Block <source> from <destination>
Block <source> access to <destination>
Block <source from <destination> where the rule is 'rule-one'
```

```
Warn <source> from <destination>
```

```
Isolate <source> from <destination>
```

Include an `AND` or `NOT` operator to allow a source and destination set, and block a different source and destination set.

```
Prevent <source_one> from <destination_one> and Allow <source_two> access to
<destination_one>
```

```
Block <source> not <source> from <destination> and Allow <source> access to
<destination>
```

Additional Examples

```
allow 10.1.1.1/16 access to 192.1.2.3/32
```

```
allow 10.1.1.1 access to 192.1.2.3/32 port 8080 , any protocol
```

```
allow 10.1.1.2 access to 192.1.2.3 on port 80 and tcp protocol
```

```
grant access to <destination> for <source>
```

```
create internet rule allow any access to any
```

```
qetest1@cisco.com cannot access shopping
```

```
give dev access to workday and ads
```

```
give p1@cisco.com access to testenv and cisco-test.com
```

```
create private access rule to allow everyone access to jira on port 80, tcp
protocol
```

```
create private access rule to allow everyone access to jira on port 80, protocol
 icmp
```

Contextual Conversations

Describes Contextual Conversations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Cisco Assistant for Secure Access has context awareness within each thread. Once you begin a thread with a prompt, you can continue the conversation with follow-up prompts that the Assistant can interpret by referring to earlier prompts.

Examples of Contextual Conversations for Prompts about Rules
Beginning prompt: Allow Swarna access to Jira
Follow-up prompt: Allow her access to Facebook
Beginning prompt: Allow Prashanth and Renuka access to Jira
Follow-up prompt: Allow them access to social media

The Assistant's context window for prompts about rules is limited to the thread's five most recent prompts and does not include details from the Assistant's responses.

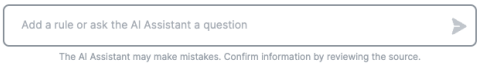
Note

Find Documented Answers with the Cisco Assistant

Understand how to use the Cisco Assistant to find documented answers to your questions.

The Cisco Assistant for Secure Access is an artificial intelligence (AI) app that can interpret your prompts to find and summarize answers from Secure Access documentation.

Click the Cisco Assistant icon in the Secure Access toolbar to open the AI app, then enter your question in the prompt bar to find documented answers. The Assistant will cite Secure Access documentation links to show the source of its answers. For more information, see Use the Cisco Assistant on page 91.



Best Practices for Prompts

Describes Best Practices for Prompts in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Follow these best practices when you prompt the Cisco Assistant for documented answers:

- **Use clear language:** The Assistant uses a natural language processing AI, so it's designed to interpret conversational language. Clearly describe the specific task or information you're looking for.
- **Include keywords:** The Assistant can understand and generate access rules based on the keywords provided in the prompts. Keywords such as 'Users and Groups', 'Registered Networks', and 'Activity Search' will return more precise results.
- **Single task at a time:** The Assistant performs optimally when asked to do a single task at once.
- **Use Suggestions:** If the Assistant finds your prompt unclear, it will provide suggestions or ask for additional corrections. Be sure to respond to maintain the flow of the conversation.
- **Follow the steps:** The Assistant provides a guided procedure for generating and managing access rules. Ensure you follow the steps provided to get the best results.
- **Verify results:** The Assistant provides links to sources with each response. Always review these sources to verify the response.

The Cisco Assistant for Secure Access is limited to published Secure Access documentation. The assistant does not interpret or return results from other sources. For more information, see Get Started with the Cisco Assistant.

Examples of Effective Prompts
How do I deploy a resource connector in AWS?
What is Experience Insights and what are its key capabilities?
How can I assign a private resource to a Connector Group?
How do I use the Search feature in Activity Search report?
What are the different kinds of IPS Signature list in Cisco Secure access?
How do I view the highest risk apps in App Discovery Report?

Contextual Conversations

Describes Contextual Conversations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Cisco Assistant for Secure Access has context awareness within each thread. Once you begin a thread with a prompt, you can continue the conversation with follow-up prompts that the Assistant can interpret by referring to earlier prompts.

Examples of Contextual Conversations for Documentation Prompts
Beginning prompt: What is the Top Destinations Report? Follow-up prompt: How do I view its details?
Beginning prompt: What is a Resource Connector? Follow-up prompt: How do I view its details?

Examples of Contextual Conversations for Documentation Prompts

Beginning prompt: What are Isolated Destinations? Follow-up prompt: How do I configure them in Secure Access?

Note

The Assistant's context window for prompts about documentation is limited to the thread's most recent prompt and response.

Troubleshoot Access Issues with Private Resources

Understand how to use the Cisco Assistant to troubleshoot access issues that your users are having with private resources.

The Cisco Assistant for Secure Access is skilled at interpreting prompts to troubleshoot when users are unable to access private resources. For more information, see Get Started with the Cisco Assistant.

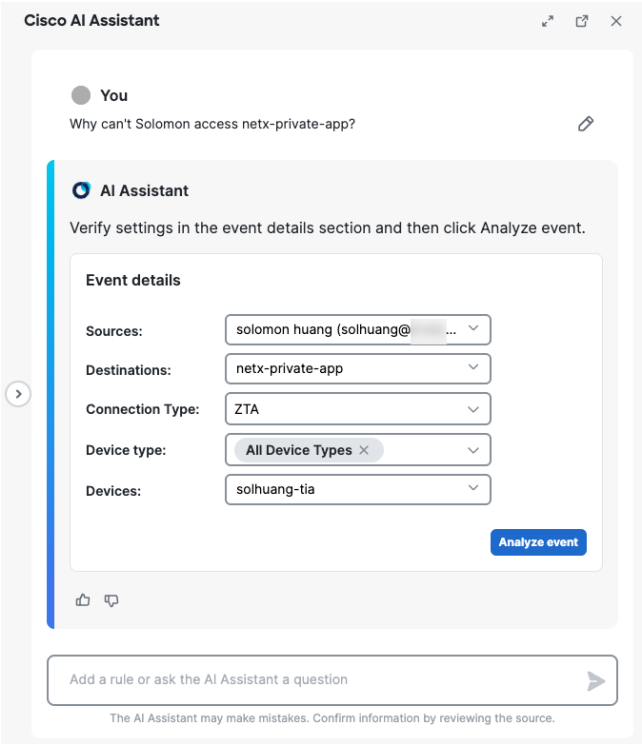
Tip

The Cisco Assistant for Secure Access has context awareness within each thread. Once you begin a thread with a prompt, you can continue the conversation with follow-up prompts that the Assistant can interpret by referring to earlier prompts. The Assistant's context window for troubleshooting prompts is limited to the thread's five most recent prompts and does not include details from the Assistant's responses.

Procedure

1. Craft your prompt – When you craft a prompt to troubleshoot access to private resources, phrase your prompt as follows: `Why can't [Source user] access [Destination]?`

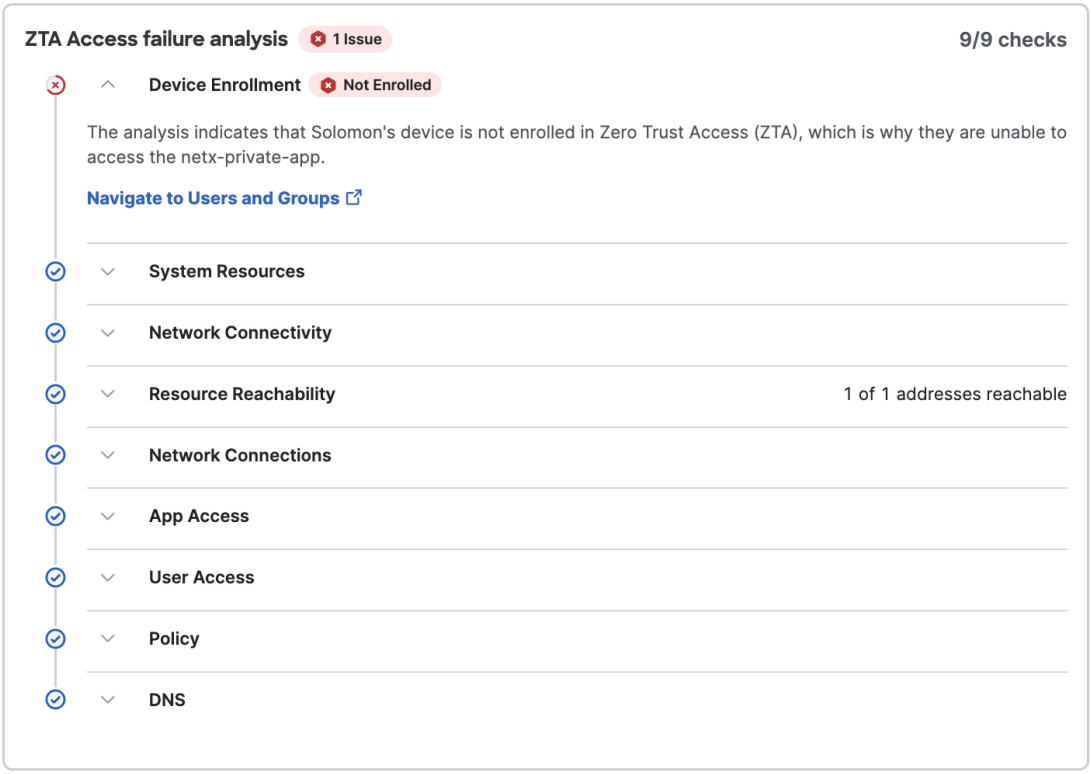
   The Assistant will reply with a card prompting you to verify and add information.



2. Provide the following **Event details**:
   a) **Sources**: The user who is unable to access the private resource.
   b) **Destinations**: The private resource. Private resources are applications, networks, or subnets that your organization controls. These resources are not publicly accessible from outside your network. For more information, see Manage Private Resources.
   c) **Connection Type**: VPN or ZTA. The Assistant can troubleshoot Client-based ZTA but does not support Browser-based ZTA connections. For more information, see Comparison of Client-Based and Browser-Based Zero Trust Access Connections.
   d) **Device type**: Select All Device Types, or select a combination of Chrome OS, iOS, macOS, and Windows.
   e) **Devices**: Select from the list of devices enrolled by the user. For more information, see View User Details.
3. Click **Analyze event**.

   The results include a natural language summary of the Event Analysis and a failure analysis card with details about nine checks.

   When the Assistant confirms that there are issues with access, the failure analysis card includes detailed results of the access checks performed by the Assistant.



What to do next

Review the details to learn more about the access issues. Follow links to navigate to Secure Access menus to troubleshoot failures, issues, and warnings.

For guidance on private access rules and other configuration options for private resources, see Add a Private Resource - What's Next.

Optimize Access Policies

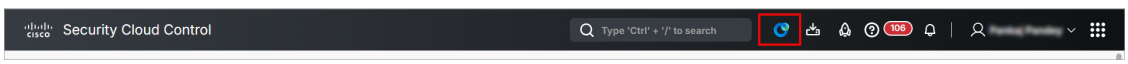
The Policy Optimization feature in Cisco AI Assistant for Secure Access streamlines access policies by detecting duplicate and shadow rules. You can easily scan for these anomalies, review reports, and disable or delete unnecessary rules to enhance policy efficiency.

The Cisco AI Assistant for Secure Access helps you optimize policy by identifying duplicate and shadow rules.

- Duplicate rules are Private Access or Internet Access rules with the same source, destination, or security controls.
- Shadow rules are Private Access or Internet Access rules that match the criteria of a preceding rule.

Procedure

1. Click the Cisco AI Assistant icon in the Secure Access toolbar to open the AI assistant.

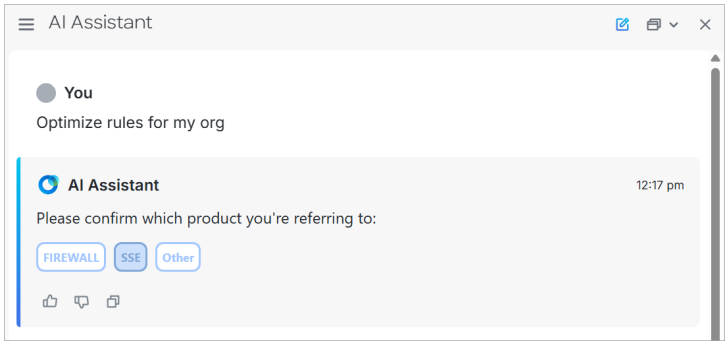


2. Enter a prompt to find duplicate policies or shadow policies.

The following table displays some example prompts and the respective scan type that the AI Assistant performs.

Prompt	Scan Type
Optimize rules for my org	Scan for any duplicate or shadow rule anomalies applied to any source or destination in your Secure Access organization.
Find duplicate policies	Scan for any duplicate rule anomalies applied to any source or destination.
Show me shadow rules for the Engineering group	Scan for any shadow rules applied to users in the Engineering group.
Any rules to optimize for George?	Scan for any rule anomalies rules applied to the user George.

3. The AI Assistant prompts you to confirm the product. Select **SSE** for Cisco Secure Access.



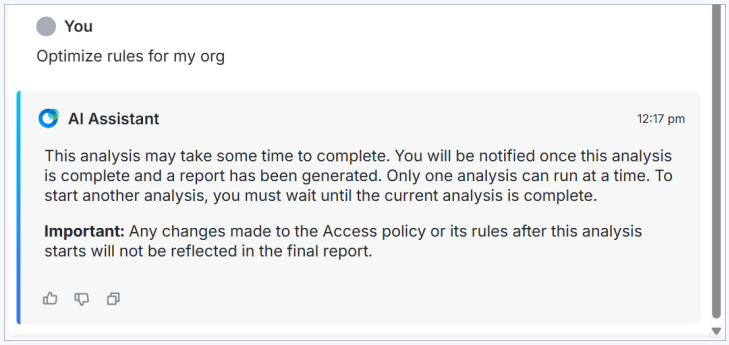
Note

This step is applicable if you are using Cisco AI Assistant within Cisco Security Cloud Control.

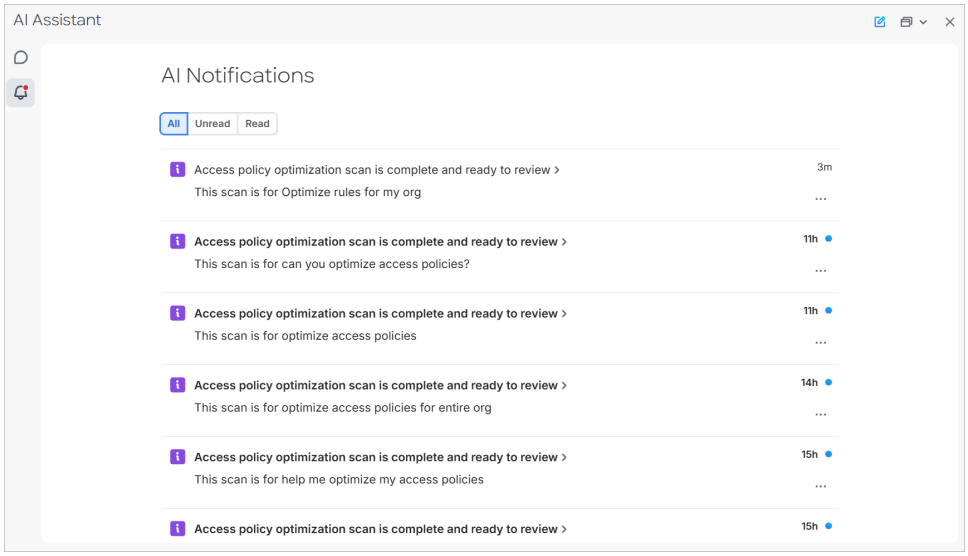
Once the scan begins, the Cisco AI Assistant will inform you that the analysis may take some time to complete.

Note

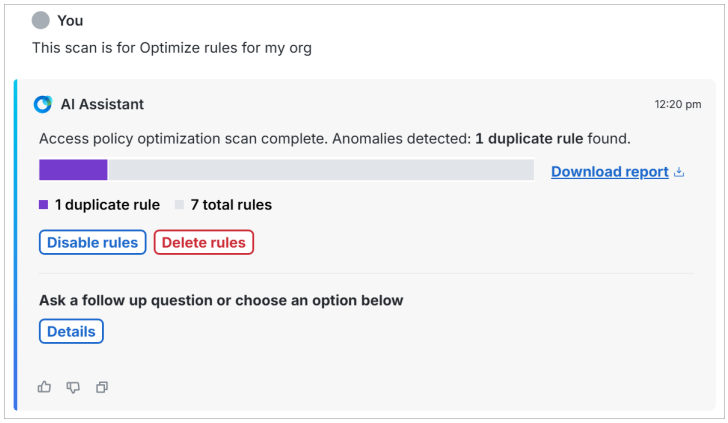
The scan may take some time to complete depending on factors such as the size of your policy set, the number of rules, and the complexity of your organization. Please allow sufficient time for the analysis to finish.



Once the scan is complete, the policy optimization report will be made available in the **AI Notifications** menu. Navigate to the bell icon to review completed policy optimization scans.

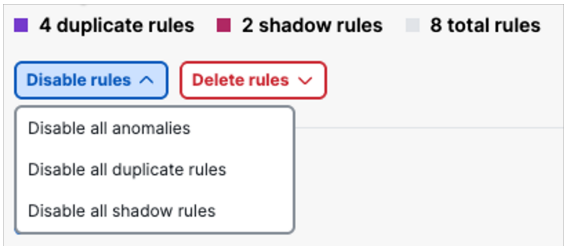


Each scan result shows any duplicate and shadow rules detected for the specific prompt.



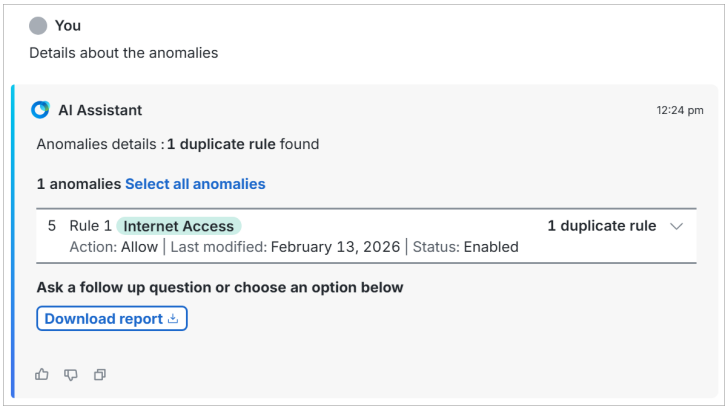
Submit a follow up prompt or question for more detail about the scan, or choose from the options in the completed scan menu:

- **Disable rules** or **Delete rules**: Choose to Disable or delete all anomalies, duplicate rules only, or shadow rules only.

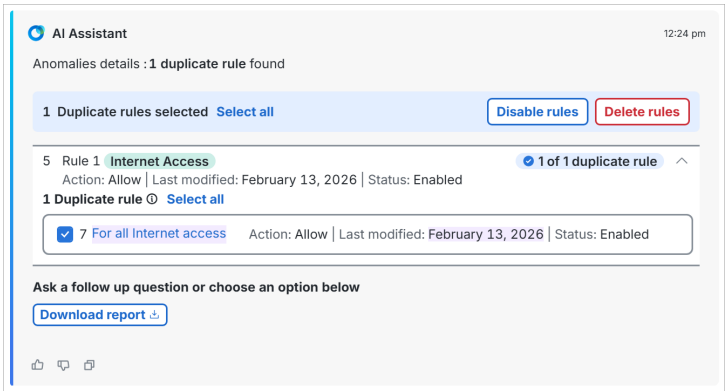


> **Note**
>
> Before disabling or deleting any detected duplicate or shadow rules, assess the potential impact on your access policy. This precaution helps prevent accidental disruptions and ensures that only the intended rules are modified.

- Click **Details** to see more information about rule sources, destinations, types of anomalies, and more.



- Select one or more rules in the anomaly details menu to disable or delete the rules.



- Click **Download report** to export scan results to a tab-separated value (tsv) file that presents results in a table.

Messages Generated by the Cisco Assistant

Understand the responses from the Cisco Assistant and how you can respond to them.

The Cisco Assistant for Secure Access generates responses to your natural language prompts. The responses generated by the assistant depend on the composition of the prompts and the information that you provide in the prompt bar. The exact responses generated by the assistant may vary from the examples below.

Message	Description
Generating.	The Cisco Assistant is reading your prompt to create policy rules.
Great! Here are your rules:	The Cisco Assistant displays the names of the generated rules.
The following rule(s) have been created. These rules are configured with the default security controls and are disabled by default.	The Cisco Assistant generated a rule from the prompt and added it to your policy.
Something isn't quite right. Click highlights to see suggestions, or edit your sentence.	The Cisco Assistant does not have the correct information to create the policy rule.
Your prompt could not be parsed to create a rule. Please enter a valid prompt.	The Cisco Assistant does not have the correct information to create the policy rule.

Message	Description
The prompt you entered is invalid. Please enter a valid input prompt.	You entered an invalid prompt where the prompt is either empty or does not generate a valid policy access rule.
Thank you for your question. However, it's outside the scope of my expertise. I'm specifically oriented to assist with questions and tasks related to Cisco Secure Access.	The prompt asks a question about information that is not available to the Cisco Assistant.
Aborted.	You canceled the request to create the policy rules.

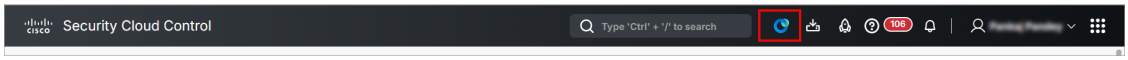
Create Cisco Support Cases

Enter a natural-language description of your issue, review the auto-generated title and case summary, then submit to Cisco Support to receive an instant case number and email confirmation.

The Cisco AI Assistant interprets your natural language prompts to detect when a problem needs support and works with you to create a new case with Secure Access technical support.

Procedure

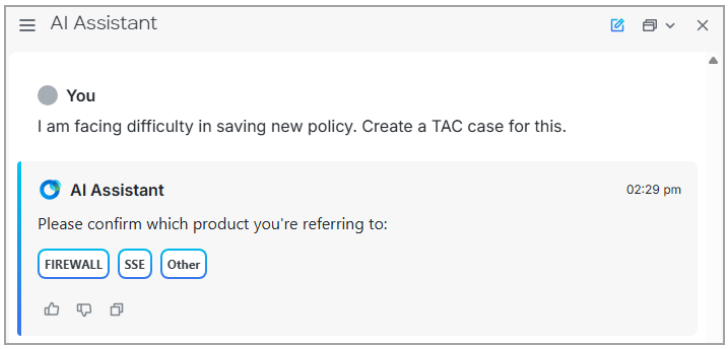
1. Click the Cisco AI Assistant icon in the Secure Access toolbar to open the AI app.



2. Enter a prompt that describes your problem and request opening a TAC case for the issue.

   For example: “I am facing difficulty in saving new policy. Create a TAC case for this.”

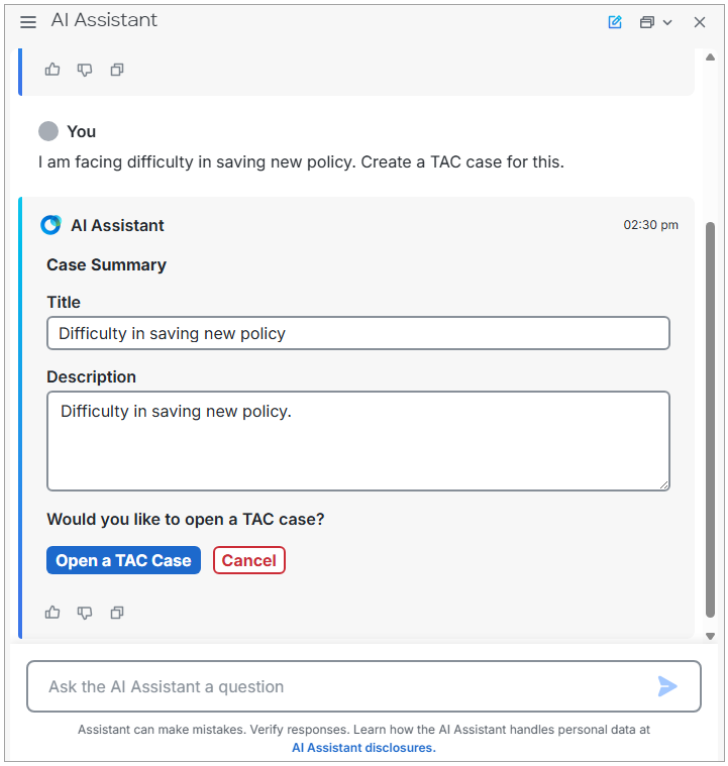
3. The AI Assistant prompts you to confirm the product. Select **SSE** for Cisco Secure Access.



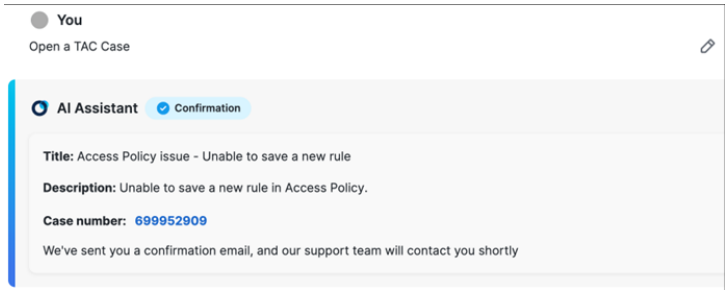
> **Note**
>
> This step is applicable if you are using Cisco AI Assistant within Cisco Security Cloud Control.

   The AI Assistant populates the **Title** and **Description** forms with content based on your original prompt.

4. Ensure the **Title** and **Description** details match what you want to report, then click **Open a TAC Case**.



The Assistant will present a TAC Case number and send a confirmation email.



4 Regions

Topics:

- Secure Access Regions

Provides an overview of Regions in Cisco Secure Access, including Secure Access Regions. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Secure Access Regions

Describes Secure Access Regions. Secure Access has instances of regional network and computing data centers that protect and manage public and private resources.

Secure Access has instances of regional network and computing data centers that protect and manage public and private resources. The regions are located geographically around the world. Network branches, data centers, and user devices can connect to the regions through the secure web gateway (SWG), Zero Trust Access (ZTA), and virtual private networks (VPNs).

For configuring your access control rules, IP addresses and fully-qualified domain names (FQDNs) for the Secure Access cloud services are available by service:

- **Secure Web Gateway**–For more information, see Secure Access Secure Web Gateway Services.
- **Resource Connectors** –For more information, see Allow Resource Connector Traffic to Secure Access.
- **Zero Trust Client**–For more information, see Secure Access Zero Trust Client-Based Proxy Services.
- **IPsec Tunnels** –For more information, see Add a Network Tunnel Group and View Network Tunnel Group Details.

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
Africa	South Africa	Cape Town	Cisco Edge v1	✓	✓	✓			NAPAfrica IX	
Africa	South Africa	Johannesburg	Cisco Edge v1	✓	✓	✓			NAPAfrica IX	
Africa	South Africa	South Africa (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	China	Beijing (Multi-AZ)***	Public Cloud - On-Demand		✓	✓		✓	AWS	
Asia	China	Hong Kong SAR	Cisco Edge v1	✓	✓	✓			HKIX	
Asia	China	Hong Kong SAR (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	China	Ningxia (Multi-AZ)***	Public Cloud - By-Request		✓	✓		✓	AWS	
Asia	India	Chennai	Cisco Edge v1	✓	✓	✓			TBC	
Asia	India	Chennai 2	Cisco Edge v2		✓	✓	✓	✓		

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
Asia	India	Hyderabad (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	India	Mumbai (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	India	Mumbai 2	Cisco Edge v1	✓	✓	✓				
Asia	India	Mumbai 3	Cisco Edge v2		✓	✓	✓	✓		
Asia	Indonesia	Jakarta (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	Japan	Osaka	Cisco Edge v1	✓	✓	✓			JPIX OSAKA / JPNAP Osaka	
Asia	Japan	Osaka 2	Cisco Edge v2		✓	✓	✓	✓		
Asia	Japan	Osaka (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	Japan	Tokyo (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	Japan	Tokyo 1	Cisco Edge v1	✓	✓	✓			JPIX Tokyo / JPNAP Tokyo	
Asia	Japan	Tokyo 2	Cisco Edge v1	✓	✓	✓			Equinix Tokyo / JPIX Tokyo / JPNAP Tokyo	
Asia	Japan	Tokyo 3	Cisco Edge v2		✓	✓	✓	✓		
Asia	Malaysia	Malaysia (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
Asia	Singapore	Singapore	Cisco Edge v1	✓	✓	✓			Equinix Singapore	

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
Asia	Singapore	Singapore (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	South Korea	Seoul	Cisco Edge v1	✓	✓	✓			KINX	
Asia	South Korea	Seoul (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Asia	Thailand	Thailand (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
Europe	Czech Republic	Prague	Cisco Edge v1	✓	✓	✓			NIX.CZ	
Europe	Denmark	Copenhagen	Cisco Edge v1	✓	✓	✓			Netnod IX Copenhagen	
Europe	France	France (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	France	Marseille	Cisco Edge v1	✓	✓	✓				
Europe	France	Paris	Cisco Edge v1	✓	✓	✓			FranceIX	
Europe	Germany	Dusseldorf	Cisco Edge v1	✓						
Europe	Germany	Frankfurt	Cisco Edge v1	✓	✓	✓			DE-CIX	
Europe	Germany	Germany (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	Ireland	Dublin	Cisco Edge v1	✓	✓	✓			INEX	
Europe	Ireland	Ireland (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
Europe	Italy	Milan	Cisco Edge v1	✓	✓	✓			MIX	
Europe	Italy	Milan (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	Netherlands	Amsterdam	Cisco Edge v1	✓	✓	✓			AMS-IX	

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
Europe	Poland	Warsaw	Cisco Edge v1	✓					PLIX	
Europe	Romania	Bucharest	Cisco Edge v1	✓					Interlan	
Europe	Spain	Madrid	Cisco Edge v1	✓	✓	✓			ESPANIX Madrid Lower LAN	
Europe	Spain	Spain (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	Sweden	Stockholm	Cisco Edge v1	✓	✓	✓			Netnod Stockholm	
Europe	Sweden	Stockholm (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	Switzerland	Zurich (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Europe	United Kingdom	London	Cisco Edge v1	✓	✓	✓			LINX / LoNAP	
Europe	United Kingdom	London 3	Cisco Edge v2		✓	✓	✓	✓		
Europe	United Kingdom	Manchester	Cisco Edge v1	✓	✓	✓			LINX Manchester	
Europe	United Kingdom	Manchester 1	Cisco Edge v2		✓	✓	✓	✓		
Europe	United Kingdom	United Kingdom (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Latin America	Brazil	Brazil (Multi-POP)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Latin America	Brazil	Rio de Janeiro	Cisco Edge v1	✓	✓	✓			IX.br Rio de Janeiro	
Latin America	Brazil	Sao Paulo	Cisco Edge v1	✓	✓	✓			IX.br Sao Paulo	
Latin America	Mexico	Mexico (Central) (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
Latin America	Mexico	Queretaro	Cisco Edge v1	✓	✓	✓			Equinix Mexico	
Middle East	Bahrain	Bahrain (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
Middle East	Israel	Tel Aviv	Cisco Edge v1	✓						
Middle East	Israel	Tel Aviv (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	
Middle East	Saudi Arabia	Jeddah	Cisco Edge v2	✓	✓	✓	✓	✓	JEDIX, SAIX	
Middle East	Saudi Arabia	Riyadh	Cisco Edge v2		✓	✓	✓	✓	SAIX	
Middle East	UAE	Dubai	Cisco Edge v1	✓	✓	✓			UAE-IX	
Middle East	UAE	Middle East (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
North America	Canada	Alberta (Multi-PAZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
North America	Canada	Quebec (Multi-PAZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
North America	Canada	Toronto	Cisco Edge v1	✓	✓	✓			TorIX	
North America	Canada	Vancouver	Cisco Edge v1	✓	✓	✓			VANIX	
North America	US	Ashburn	Cisco Edge v1	✓	✓	✓			Equinix Ashburn	
North America	US	Atlanta	Cisco Edge v1	✓	✓	✓			Digital Realty	
North America	US	Boston	Cisco Edge v1	✓					MASS-IX	
North America	US	Chicago	Cisco Edge v1	✓	✓	✓			Equinix Chicago	
North America	US	Dallas 1	Cisco Edge v1	✓	✓	✓			Equinix Dallas	

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
North America	US	Denver 1	Cisco Edge v1	✓	✓	✓			CoreSite Any2 Denver	
North America	US	Dallas 2	Cisco Edge v2		✓	✓	✓	✓	Equinix Dallas	
North America	US	Denver 2	Cisco Edge v2		✓	✓	✓	✓	CoreSite Any2 Denver	
North America	US	GovCloud East (Multi-AZ)	Public Cloud - On-Demand	✓	✓	✓			AWS	
North America	US	Los Angeles 1	Cisco Edge v1	✓	✓	✓			Equinix Los Angeles	
North America	US	Los Angeles 2	Cisco Edge v2	✓	✓	✓	✓	✓	Equinix Los Angeles	
North America	US	Miami 1	Cisco Edge v1	✓	✓	✓			FL-IX	
North America	US	Miami 2	Cisco Edge v2	✓	✓	✓	✓	✓	FL-IX	
North America	US	Minneapolis	Cisco Edge v1	✓	✓	✓				
North America	US	New York	Cisco Edge v1	✓	✓	✓			NYIIX	
North America	US	Northern California (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
North America	US	US Midwest (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
North America	US	Oregon (Multi-AZ)	Public Cloud -On-Demand		✓	✓	✓	✓	AWS	✓
North America	US	Reston 1	Cisco Edge v1	✓	✓	✓			CoreSite Any2	
North America	US	Reston 2	Cisco Edge v2	✓	✓	✓	✓	✓	CoreSite Any2	
North America	US	San Jose 1	Cisco Edge v1	✓	✓	✓			Equinix San Jose / PAIX	

Region	Country	Location	DC Type	DNS	SWG & DLP	Firewall	ZTA	VPN	Peering Fabric	Meraki Auto VPN Support
North America	US	San Jose 2	Cisco Edge v2	✓	✓	✓	✓	✓	Equinix San Jose / PAIX	
North America	US	Seattle	Cisco Edge v1	✓					SIX	
North America	US	Virginia (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓
Oceania	Australia	Melbourne	Cisco Edge v1	✓	✓	✓			MegaIX	
Oceania	Australia	Melbourne (Multi-AZ)	Public Cloud - By-Request		✓	✓	✓	✓	AWS	
Oceania	Australia	Sydney	Cisco Edge v1	✓	✓	✓			Equinix Sydney / MegaIX	
Oceania	Australia	Sydney (Multi-AZ)	Public Cloud - On-Demand		✓	✓	✓	✓	AWS	✓

- Cisco Edge v1 sites serve DNS for all subscriptions. SWG, DLP and Firewall are available to customers with an Umbrella entitlement such as Secure Access Elevate.
- Cisco Edge v2 sites are in private preview. Contact your account team for more information.
- Multi-AZ regions are composed two or more availability zones for redundancy.
- ***Beijing and Ningxia require a separate subscription to Cisco Secure Access China operated by Digital China Cloud Technology (DCC). This subscription is managed by DCC. Contact your account team for more information.

5 Network Requirements

Topics:

- Network requirements for Secure Access
- DNS requirements
- Secure Client requirements
- Transport layer security protocol requirements
- Secure web gateway service requirements
- Realtime DLP secure ICAP requirements
- SaaS tenant requirements
- SAML identity provider requirements
- Virtual private network requirements
- Zero trust access requirements

Provides an overview of Network Requirements in Cisco Secure Access, including Network Requirements for Secure Access, DNS requirements, and Secure Client requirements. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Network requirements for Secure Access

Network requirements to support connections to the Secure Access cloud services and other Secure Access services and applications.

This section describes the network configurations required to support connections to the Secure Access cloud services and other Secure Access services and applications.

For user devices, applications, and network devices to interact with the Secure Access services, an administrator must allow connections from their organization's networks and devices to the Secure Access services. You may have to bypass domains for the Secure Access cloud services and identity provider (IdP) services on the Secure Access secure web gateway (SWG) and configure other device or network settings.

DNS requirements

Network requirements to support DNS in Secure Access.

Your network must meet the following DNS requirements for Secure Access.

Secure Access DNS Resolvers

Describes Secure Access DNS Resolvers. Required by applications or devices connecting to the Secure Access DNS resolvers, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

Required by applications or devices connecting to the Secure Access DNS resolvers, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

IPv4	IPv6	Port/Protocol	Description
208.67.222.222	2620:119:35::35	53 TCP/UDP	Primary
208.67.220.220	2620:119:53::53	53 TCP/UDP	Secondary
208.67.222.220	n/a	53 TCP/UDP	Tertiary
208.67.220.222	n/a	53 TCP/UDP	Quaternary
208.67.221.76	2620:119:17::76	53 TCP/UDP	USA only Primary (For more information, see Best Practices.)
208.67.223.76	2620:119:76::76	53 TCP/UDP	USA only Secondary (For more information, see Best Practices.)
208.67.222.64	2620.119.53::64	53 TCP/UDP	DNS64 Primary (For more information, see Best Practices.)
208.67.220.64	2620:119:53::64	53 TCP/UDP	DNS64 Secondary (For more information, see Best Practices.)
146.112.70.70	2a04:e4c0:170::170	53 TCP/UDP	Saudi Arabia-Alternate Primary
146.112.71.71	2a04:e4c0:171::171	53 TCP/UDP	Saudi Arabia-Alternate Secondary

Best Practices

Describes Best Practices in Cisco Secure Access. You can use either IPv4 or IPv6 DNS addresses as your primary or secondary DNS server.

You can use either IPv4 or IPv6 DNS addresses as your primary or secondary DNS server. You must use both numbers and not the same IP address twice. If your router requires a third or fourth DNS server setting, you can use 208.67.220.222 and 208.67.222.220 or 2620:119:35::35 and 2620:119:53::53 as the third and fourth entry respectively.

DNS64 (RFC 6147) is meant for single-stack IPv6 networks. This is to help with IPv4 to IPv6 transitions. If you are using Secure Access DNS on devices without IPv4 access, these resolvers will synthesize records that can reach those destinations through a NAT64 gateway using the Well-Known Prefix. See details: https://datatracker.ietf.org/doc/html/rfc6147

North America (USA-only) DNS resolvers guarantee only that DNS queries are resolved by a USA-based Secure Access data center. Block pages use global Anycast and may go to any data center, including one located outside of the USA.

If you have an organization with roaming or integrated identities that frequently move across networks owned by different Cisco organizations, DNS queries are resolved under your own organization's policy rather than the policy of the unrelated network you are currently on. DNS queries have unique identifiers such as device ID, GUID, and organization ID embedded into DNS requests. The Secure Access DNS resolvers then enforce the correct security policies based on the embedded identity information, regardless of the network the user is roaming on. This prevents policy misapplication from other Cisco organizations' networks and ensures consistent policy enforcement tied to your organization.

Several systems allow you to specify multiple DNS servers. We recommend that you only use the Cisco Secure Access servers and do not include any other DNS servers.

Cisco Secure Client

Describes Cisco Secure Client in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module uses standard DNS ports 53/UDP and 53/TCP to communicate with Secure Access.

The Cisco Secure Client Umbrella Roaming Security module uses standard DNS ports 53/UDP and 53/TCP to communicate with Secure Access. If you explicitly block access to third-party DNS servers on your corporate or home network, you must allow certain CIDRs on the ports and protocols in your firewall.

In circumstances where third-party DNS servers are blocked, the Cisco Secure Client Umbrella Roaming Security module transitions to a state where it temporarily uses the DHCP-delegated DNS servers for resolution.

Cisco Secure Client and External DNS Resolution

Describes Cisco Secure Client and External DNS Resolution in Cisco Secure Access. In normal circumstances, the Cisco Secure Client Umbrella Roaming Security module functions only on networks where external DNS resolution exists.

In normal circumstances, the Cisco Secure Client Umbrella Roaming Security module functions only on networks where external DNS resolution exists. The Cisco Secure Client Umbrella Roaming Security module can not function successfully if DNS connectivity is broken or blocked on the local network.

Bypass Requirements

For the Cisco Secure Client device registration process to complete, send the following destinations directly and bypass them from any form of authentication, SSL inspection, or filtering:

- crl3.digicert.com
- crl4.digicert.com
- ocsp.digicert.com

DNS Resolution Requirements

For the Cisco Secure Client Umbrella Roaming Security module to enable DNS-layer protection, you must allow the following external DNS names to resolve by the local DNS server. Allow recursive DNS queries to the following domains on the local DNS server:

- **disthost.umbrella.com**
- **api.sse.cisco.com**
- **api.opendns.com** (Required if deployment keys are not used for registration)
- **sync.hydra.opendns.com** (Required if deployment keys are not used for registration)
- **devices.api.sse.cisco.com** (Required for SSE Global region when deployment keys are used)
- **http://r13.c.lencr.org/7.crl**(CRL lookup service for devices.api.sse.cisco.com)
- **crl3.digicert.com**
- **crl4.digicert.com**
- **ocsp.digicert.com**
- **debug.opendns.com**– This domain can receive a response to a TXT record query.

  The Cisco DNS resolvers must answer this DNS request.

> **Note**
>
> `NXDOMAIN` is accepted, however, timeouts may delay or prevent Secure Access DNS-layer security protection on the network interface where this domain query times out.

Secure Access Encrypted DNS Queries

Describes Secure Access Encrypted DNS Queries. Required by applications or devices connecting to the Secure Access DNS resolvers, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

Required by applications or devices connecting to the Secure Access DNS resolvers, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

The Cisco Secure Client Umbrella Roaming Security module supports the encryption of DNS queries sent to Secure Access on port 443 over TCP or UDP. If you would like to ensure encryption is enabled, and use a default deny ruleset in your firewall, allow the following CIDRs on the ports and protocols in your firewall.

Note: The Cisco Secure Client Umbrella Roaming Security module automatically encrypts DNS queries when it senses that 443/UDP is open.

IPv4	IPv6	Port/Protocol	Description
208.67.222.222	2620:119:35::35	443 TCP/UDP	Primary
208.67.220.220	2620:119:53::53	443 TCP/UDP	Secondary

Secure Access DNS, Web, and Block Pages

Describes Secure Access DNS, Web, and Block Pages. Required by applications or devices connecting to the Secure Access DNS-layer security, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

Required by applications or devices connecting to the Secure Access DNS-layer security, including Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security).

We recommend that you allow all traffic on ports 80 and 443 over TCP for the Secure Access DNS-layer, internet security, and Block Page services.

IP	Ports/Protocol
67.215.64.0/19	80/443 TCP
146.112.0.0/16	80/443 TCP
155.190.0.0/16	80/443 TCP
185.60.84.0/22	80/443 TCP
204.194.232.0/21	80/443 TCP
208.67.216.0/21	80/443 TCP
208.69.32.0/21	80/443 TCP

Secure Access DNS and Web – Client Configuration Services

Describes Secure Access DNS and Web – Client Configuration Services. Required by applications or devices connecting to the Secure Access DNS-layer security, including the Secure Access Active Director (AD) Connector and Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security and Web).

Required by applications or devices connecting to the Secure Access DNS-layer security, including the Secure Access Active Director (AD) Connector and Cisco Secure Client deployments with the Umbrella Roaming Security module (DNS-layer security and Web).

We recommend that you allow all traffic on port 443 over TCP for the Secure Access Client Configuration services.

Domains	Port/Protocol	Description
api.opendns.com	443/TCP	Configuration

The Cisco Secure Client Umbrella Roaming Security module uses HTTPS (443/TCP) to communicate with Secure Access for the following uses:

- Initial registration of the Cisco Secure Client Umbrella Roaming Security module upon installation.
- Checking for new versions of the Cisco Secure Client Umbrella Roaming Security module.
- Reporting the status of Cisco Secure Client Umbrella Roaming Security module to Secure Access.
- Checking for new internal domains.

IP Ranges	Port	Protocol
67.215.71.201	443	TCP
67.215.92.210	443	TCP
146.112.255.101	443	TCP
146.112.255.152/29	443	TCP
2620:0:cc1:115::210 (IPv6)	443	TCP

IP Ranges	Port	Protocol
2a04:e4c7:ffff::20/125 (IPv6)	443	TCP

Windows Only

If you utilize an HTTP proxy that is configured at the user-level (normally using GPO), make sure the `SYSTEM` user is also configured to use the proxy.

Secure Access DNS and Web – Client Sync Services

Describes Secure Access DNS and Web – Client Sync Services. Required by devices or applications that are protected by Secure Access DNS or Web security.

Required by devices or applications that are protected by Secure Access DNS or Web security. Includes Cisco Secure Client deployments with the Umbrella Roaming Security module.

Domains	IP Ranges	Port/Protocol	Description
sync.hydra.opendns.com	146.112.63.3 - 146.112.63.9 146.112.63.11 - 146.112.63.13	443/TCP	Syncing data

The **sync.hydra.opendns.com** domain resolves to multiple IP addresses, all within the 146.112.63.0/24 IP range. We recommend that you add this entire range. The IP addresses for **sync.hydra.opendns.com** are Anycast and may change.

Secure Access DNS and Web – Client Certificate Revocation Services

Describes Secure Access DNS and Web – Client Certificate Revocation Services. Required by devices or applications that are protected by Secure Access DNS or Web security.

Required by devices or applications that are protected by Secure Access DNS or Web security. Includes the Secure Access Active Director (AD) Connector and Cisco Secure Client deployments with the Umbrella Roaming Security module.

Domains	Port/Protocol	Description
crl3.digicert.com	80/TCP	CRL
crl4.digicert.com	80/TCP	CRL
ocsp.digicert.com	80/TCP	OCSP
sync.hydra.opendns.com	443/TCP	Registration (without deployment keys)
api.opendns.com	443/TCP	Registration (without deployment keys)
devices.api.sse.cisco.com	443/TCP	Registration (SSE Global region with deployment keys)
r13.c.lencr.org	80/TCP	CRL lookup for devices.api.sse.cisco.com

Note

The Digicert domains resolve to various IP addresses based on a CDN and are subject to change.

Secure Client requirements

Network requirements to support Cisco Secure Client.

If you intend to configure Cisco Secure Client in your Secure Access environment, ensure that your network meets the requirements for your deployment.

Note

Review all network requirements carefully, as some other sections also contain requirements for Cisco Secure Client deployments, such as VPN and zero trust access.

Cisco Secure Client and Captive Portal Detection

Describes Cisco Secure Client and Captive Portal Detection in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module uses multiple techniques to detect captive portals or hotspots.

The Cisco Secure Client Umbrella Roaming Security module uses multiple techniques to detect captive portals or hotspots. Allow these domains on your firewall for the most accurate captive portal detection:

- **connecttest.cisco.io**
- **www.msftconnecttest.com**

Note

The **connecttest.cisco.io** and **www.msftconnecttest.com** domains have dynamic IP addresses.

Cisco Secure Client and Device Hostnames

Describes Cisco Secure Client and Device Hostnames in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module uses hostnames to register the device in Secure Access.

The Cisco Secure Client Umbrella Roaming Security module uses hostnames to register the device in Secure Access. All machines must have a hostname that is unique within your organization.

Transport layer security protocol requirements

Network requirements to support transport layer security (TLS) protocol.

All operating systems of the devices in your orgaization must support at a minimum TLS 1.2.

The TLS 1.0 and TLS 1.1 protocols contain security vulnerabilities and do not support modern cryptographic algorithms.

TLS 1.2 Support in Windows

Describes TLS 1.2 Support in Windows in Cisco Secure Access. We recommend that you disable support for SSL, TLS 1.0, and TLS 1.1 in your Windows operating system.

We recommend that you disable support for SSL, TLS 1.0, and TLS 1.1 in your Windows operating system. You can disable TLS 1.0 and TLS 1.1 in the Windows Registry. For more information, see Configuring Schannel protocols in the Windows Registry.

The latest version of the Cisco Secure Client Umbrella Roaming Security module uses TLS 1.2. Ensure that you have a compatible version of .NET installed with your Windows operating system. Native TLS 1.2 support requires .NET framework 4.6.2+. Prior versions of .NET require registry edits (4.x) or registry edits and manual hot fix patches (3.5).

TLS 1.2 Support in macOS

Describes TLS 1.2 Support in macOS in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module for macOS uses TLS 1.2.

The Cisco Secure Client Umbrella Roaming Security module for macOS uses TLS 1.2.

Secure web gateway service requirements

Network requirements to support secure web gateway services, including network tunnel and PAC file deployments, and Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules.

Required by the Secure Access Network Tunnel and PAC file deployments, and Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules.

Egress IP Addresses for the Secure Web Gateway

Describes Egress IP Addresses for the Secure Web Gateway in Cisco Secure Access. All public web traffic through the SWG egresses from the NATaaS with public addresses from the shared ranges listed under Web Traffic and NAT as a Service.

All public web traffic through the SWG egresses from the NATaaS with public addresses from the shared ranges listed under Web Traffic and NAT as a Service.

Ingress IP Addresses for the Secure Web Gateway

Describes Ingress IP Addresses for the Secure Web Gateway in Cisco Secure Access. To enable connections to the Secure Access Secure Web Gateway, allow the following CIDRs in your firewalls on ports 80 and 443 over TCP.

To enable connections to the Secure Access Secure Web Gateway, allow the following CIDRs in your firewalls on ports 80 and 443 over TCP.

Click to view the regional ingress IP addresses for the Secure Access Secure Web Gateway.

Africa (South Africa)

Africa (South Africa)
13.244.199.120
13.244.218.200
13.244.237.225
13.245.178.189
13.245.192.2

Africa (South Africa)
13.245.201.100
13.246.114.113
13.246.133.19
13.246.135.96
13.246.148.93
13.246.180.179
13.246.218.54
13.246.48.5
13.247.102.235
13.247.115.188
13.247.143.44
13.247.166.228
13.247.44.244
13.247.82.162
16.28.0.195

Asia

Asia Pacific (Hong Kong)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	India (South)	India (West)
16.162.156.15	13.208.132.179	13.124.13.28	13.214.98.31	18.60.194.164	13.126.152.179
16.162.214.98	13.208.52.205	13.125.2.206	13.215.125.242	18.60.248.246	13.126.229.165
16.163.136.232	13.208.71.239	13.209.186.4	13.228.35.51	18.60.35.221	13.127.162.151
18.162.198.132	15.152.126.67	15.165.152.102	18.136.254.192	18.60.94.51	13.127.38.154
18.162.206.128	15.152.137.233	3.34.15.226	18.139.251.40	18.61.109.18	13.200.185.159
18.163.169.209	15.152.182.240	3.34.246.8	18.142.126.162	18.61.192.168	13.200.201.134
18.163.248.233	15.152.189.225	3.36.20.40	18.142.33.94	18.61.218.23	13.200.232.199
18.163.42.219	15.152.239.183	3.37.230.156	18.142.74.94	18.61.222.116	13.232.69.203
18.166.14.134	15.168.104.82	3.37.41.109	18.143.9.34	18.61.239.220	13.233.51.89
18.167.143.158	15.168.181.48	3.37.91.168	3.0.178.57	18.61.46.124	15.207.1.100
18.167.154.183	15.168.205.155	3.38.237.47	3.0.197.90	98.130.21.18	3.109.170.206
18.167.251.6	15.168.205.247	43.201.88.115	3.0.236.175	98.130.23.174	3.109.91.124
18.167.40.135	15.168.208.192	43.202.30.82	3.0.39.255	98.130.27.157	3.111.127.158
18.167.45.52	15.168.220.15	43.202.88.87	3.1.174.140	98.130.31.27	3.111.174.227
18.167.49.16	15.168.224.29	43.202.89.35	47.128.172.134	98.130.38.229	3.111.73.187

Asia Pacific (Hong Kong)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	India (South)	India (West)
43.198.145.86	15.168.225.141	43.203.13.78	47.128.191.7	98.130.39.60	3.6.110.13
43.198.200.190	15.168.36.169	43.203.72.120	52.74.119.66	98.130.75.29	65.0.112.175
43.198.213.27	15.168.42.247	43.203.86.250	52.74.87.15	98.130.76.179	65.1.188.156
43.198.65.196	15.168.79.33	52.78.31.215	52.76.130.198	65.1.87.105	
43.199.5.8	15.168.88.51	52.79.62.202	54.179.86.196	98.130.80.125	65.2.65.37
	151.186.122.0/24	54.116.202.174		163.129.195.0/24	163.129.199.0/24
		54.116.217.159			
		54.116.66.141			

Indonesia (Jakarta)	Israel	Japan (Tokyo)	Middle East (Saudi Arabia)	Middle East (UAE)
108.136.187.213	51.16.148.190	18.176.125.195	151.186.110.0/24	3.28.30.234
108.137.175.7	51.16.195.201	18.177.180.173	151.186.127.0/24	3.29.10.20
16.78.15.57	51.16.196.219	18.178.72.165		3.29.120.102
43.218.195.124	51.16.224.73	18.179.18.63		3.29.251.187
43.218.196.146	51.17.10.222	18.181.113.214		3.29.38.214
43.218.238.209	51.17.102.144	18.181.45.60		3.29.45.234
43.218.252.55	51.17.117.216	3.113.110.233		40.172.32.63
43.218.253.33	51.17.125.59	3.114.181.43		40.172.44.109
43.218.254.184	51.17.148.214	35.75.158.92		40.172.47.132
43.218.8.253	51.17.150.75	35.75.252.128		40.172.58.138
108.136.152.244	51.17.150.81	35.77.152.111		40.172.59.24
108.137.117.124	51.17.153.18	35.78.39.17		40.172.64.122
108.137.143.159	51.17.173.27	52.192.121.95		40.172.67.216
16.78.12.144	51.17.178.175	52.193.133.13		40.172.68.53
43.218.210.218	51.17.181.142	52.194.109.230		40.172.74.42
43.218.214.88	51.17.198.69	52.69.214.33		40.172.75.235
43.218.230.129	51.17.200.93	54.95.128.80		40.172.82.196
43.218.248.115	51.17.57.22	57.180.203.125		51.112.58.162
43.218.248.217	51.17.67.196	57.180.88.2		51.112.85.49
43.218.252.86	51.17.71.123	57.181.86.151		51.112.87.103
		151.186.118.0/24		

Australia

Sydney
13.211.119.9
13.238.112.208
13.238.122.162
13.238.158.129
13.239.130.15
3.104.178.82
3.105.203.162
3.24.10.19
3.24.192.45
52.63.52.169
52.63.79.187
52.64.149.5
52.64.188.53
52.65.120.79
54.153.137.67
54.253.200.7
54.253.204.43
54.253.254.54
54.66.46.188
54.79.82.178

Europe

Germany	Milan	Paris	Spain
18.153.111.87	15.160.53.115	13.36.121.64	18.100.200.197
18.153.141.55	15.161.0.202	15.236.232.91	51.48.173.95
18.153.182.82	15.161.39.207	15.224.5.160	51.48.21.117
18.153.211.50	18.102.153.48	13.38.161.23	51.48.224.26
18.153.226.161	18.102.159.106	13.37.178.207	51.48.227.60
18.197.243.109	18.102.177.57	35.181.109.170	51.48.240.60
18.198.182.51	18.102.182.234	13.36.72.30	51.48.249.41
18.199.59.8	18.102.187.206	13.36.185.51	51.48.62.184
3.120.17.186	18.102.196.17	13.39.168.193	51.49.0.51
3.125.254.147	18.102.45.73	51.44.93.189	51.49.18.44
3.66.137.143	18.102.91.72	13.39.68.213	51.49.4.206

Germany	Milan	Paris	Spain
3.67.16.210	35.152.118.225	15.237.12.254	51.49.43.169
3.67.28.205	35.152.167.13	15.236.115.130	51.49.69.222
3.71.158.156	35.152.213.106	51.44.119.173	51.49.77.144
3.74.137.87	35.152.224.216	51.44.62.204	51.94.12.47
35.158.253.14	35.152.237.192	13.36.17.207	51.94.176.146
35.158.50.0	35.152.244.77	51.45.27.62	51.95.0.89
52.29.71.12	35.152.253.133	35.180.176.136	51.95.53.118
52.58.11.21	51.118.13.211	51.44.89.8	51.95.71.11
52.58.217.77	51.118.7.166	13.39.174.8	51.95.88.136
		13.36.140.148	
		13.39.216.17	

Stockholm	Switzerland (Zurich)	United Kingdom
13.48.0.216	16.62.10.95	13.42.241.158
13.48.163.57	16.63.1.64	18.135.112.200
13.48.51.151	16.63.119.220	18.168.160.22
13.49.210.230	16.63.146.151	18.168.223.23
13.49.82.243	16.63.191.113	18.169.141.252
13.49.99.155	16.63.241.246	18.170.109.89
13.50.188.96	16.63.248.194	18.170.162.124
13.50.219.204	16.63.50.209	18.170.245.252
13.50.60.146	16.63.81.145	18.171.14.50
13.50.82.81	51.96.4.88	3.11.157.254
13.51.227.10	16.62.175.191	3.11.225.126
13.60.111.239	16.62.234.167	3.8.14.231
16.16.140.11	16.63.143.46	3.9.163.167
16.16.181.111	16.63.184.108	35.176.186.56
16.170.127.220	16.63.216.64	35.177.223.97
16.170.176.42	16.63.224.127	35.177.252.178
16.171.77.186	16.63.230.1	35.178.14.215
51.21.138.79	16.63.236.61	35.178.147.15
51.21.34.233	16.63.246.9	35.178.164.29
51.21.83.189	16.63.250.231	35.178.223.106
		163.129.223.0/24
		163.129.235.0/24

North America

Canada (Central)	Canada (West)	LATAM (Mexico)	US East (Miami, Florida)	US East (Reston, Virginia)
15.156.225.124	40.176.7.159	78.12.97.7	151.186.82.0/24	151.186.86.0/24
15.157.147.102	40.176.20.123	78.12.123.164		
15.157.151.0	40.176.67.12	78.12.157.95		
15.157.153.35	40.176.77.82	78.12.172.128		
3.98.225.135	40.176.139.190	78.12.178.148		
3.98.254.97	40.176.153.233	78.12.181.252		
3.99.84.120	40.176.195.231	78.12.202.255		
3.99.95.71	40.176.214.104	78.13.9.47		
35.183.163.199	40.176.226.233	78.13.27.180		
52.60.79.39	40.177.18.235	78.13.29.91		
15.157.113.2	40.177.36.59	78.13.38.110		
15.157.126.225	40.177.55.226	78.13.57.99		
15.157.40.249	40.177.61.136	78.13.70.127		
3.96.39.0	40.177.63.115	78.13.84.179		
3.98.227.70	40.177.92.127	78.13.91.235		
3.99.107.229	40.177.141.16	78.13.149.241		
3.99.3.196	40.177.167.252	78.13.159.132		
3.99.93.31	40.177.208.203	78.13.159.216		
35.183.143.180	40.177.238.210	78.13.161.237		
99.79.90.118	40.177.238.212	78.13.163.195		

US Central (Denver, Colorado)	US Central (Dallas, Texas)	US (Midwest)	US (Pacific Northwest)	US West (Los Angeles, California)	US West (San Jose, California)	US (Virginia)
163.129.227.0/24	163.129.212.0/24	18.190.167.133	100.20.55.128	151.186.94.0/24	151.186.90.0/24	18.207.48.91
		18.220.203.100	34.210.182.194			3.208.132.58
		18.224.162.164	34.211.133.49			3.220.27.92
		18.224.232.77	35.163.230.204			3.224.76.22
		3.128.167.118	35.167.192.160			3.229.59.4
		3.129.236.62	35.82.37.34			3.229.98.228
		3.129.49.88	44.226.181.121			34.199.204.168
		3.13.65.14	44.227.223.79			34.234.106.45
		3.130.93.106	44.227.59.253			35.171.156.209
		3.132.35.188	44.228.41.46			44.205.38.30
		3.135.147.177	44.231.2.184			44.206.168.122

US Central (Denver, Colorado)	US Central (Dallas, Texas)	US (Midwest)	US (Pacific Northwest)	US West (Los Angeles, California)	US West (San Jose, California)	US (Virginia)
		3.138.228.182	44.232.163.156			44.214.98.67
		3.138.240.248	52.10.7.185			44.217.43.177
		3.139.144.205	52.24.201.181			44.221.120.37
		3.141.67.95	52.35.186.20			44.221.97.202
		3.147.235.189	52.36.167.192			52.5.115.214
		3.15.63.151	52.43.252.155			52.86.227.76
		3.16.185.117	54.185.253.229			54.160.164.245
		3.17.22.235	54.68.79.94			54.221.27.20
		52.14.247.224	54.69.85.241			54.227.68.243

South America

Brazil
15.229.180.59
15.229.226.215
15.229.94.133
177.71.157.58
177.71.172.241
18.228.146.29
18.228.72.211
18.229.42.145
18.230.128.190
18.230.248.68
18.231.63.251
52.67.132.185
52.67.148.235
52.67.210.165
52.67.90.227
54.207.19.93
54.207.22.2
54.232.194.234
54.94.213.6
54.94.232.220

Click to view and copy the regional ingress IP addresses for the Secure Access Secure Web Gateway.

```
# Regional Cisco Secure Access Secure Web Gateway Ingress IPs
regions:
 Africa (South Africa):
    ips:
      -  13.244.199.120
      -  13.244.218.200
      -  13.244.237.225
      -  13.245.178.189
      -  13.245.192.2
      -  13.245.201.100
      -  13.246.114.113
      -  13.246.133.19
      -  13.246.135.96
      -  13.246.148.93
      -  13.246.180.179
      -  13.246.218.54
      -  13.246.48.5
      -  13.247.102.235
      -  13.247.115.188
      -  13.247.143.44
      -  13.247.166.228
      -  13.247.44.244
      -  13.247.82.162
      -  16.28.0.195
 Asia Pacific (Hong Kong):
    ips:
      - 16.162.156.15
      - 16.162.214.98
      - 16.163.136.232
      - 18.162.198.132
      - 18.162.206.128
      - 18.163.169.209
      - 18.163.248.233
      - 18.163.42.219
      - 18.166.14.134
      - 18.167.143.158
      - 18.167.154.183
      - 18.167.251.6
      - 18.167.40.135
      - 18.167.45.52
      - 18.167.49.16
      - 43.198.145.86
      - 43.198.200.190
      - 43.198.213.27
      - 43.198.65.196
      - 43.199.5.8
 Asia Pacific (Osaka):
    ips:
      - 13.208.132.179
      - 13.208.52.205
      - 13.208.71.239
      - 15.152.126.67
      - 15.152.137.233
      - 15.152.182.240
      - 15.152.189.225
      - 15.152.239.183
      - 15.168.104.82
      - 15.168.181.48
      - 15.168.205.155
      - 15.168.205.247
      - 15.168.208.192
```

```
      - 15.168.220.15
      - 15.168.224.29
      - 15.168.225.141
      - 15.168.36.169
      - 15.168.42.247
      - 15.168.79.33
      - 151.186.122.0/24
Asia Pacific (Seoul):
   ips:
      - 13.124.13.28
      - 13.125.2.206
      - 13.209.186.4
      - 15.165.152.102
      - 3.34.15.226
      - 3.34.246.8
      - 3.36.20.40
      - 3.37.230.156
      - 3.37.41.109
      - 3.37.91.168
      - 3.38.237.47
      - 43.201.88.115
      - 43.202.30.82
      - 43.202.88.87
      - 43.202.89.35
      - 43.203.13.78
      - 43.203.72.120
      - 43.203.86.250
      - 52.78.31.215
      - 52.79.59.173
      - 52.79.62.202
      - 54.116.202.174
      - 54.116.217.159
      - 54.116.66.141
 Australia (Sydney):
   ips:
      - 13.211.119.9
      - 13.238.112.208
      - 13.238.122.162
      - 13.238.158.129
      - 13.239.130.15
      - 3.104.178.82
      - 3.105.203.162
      - 3.24.10.19
      - 3.24.192.45
      - 52.63.52.169
      - 52.63.79.187
      - 52.64.149.5
      - 52.64.188.53
      - 52.65.120.79
      - 54.153.137.67
      - 54.253.200.7
      - 54.253.204.43
      - 54.253.254.54
      - 54.66.46.188
      - 54.79.82.178
 Brazil:
   ips:
      - 15.229.180.59
      - 15.229.226.215
      - 15.229.94.133
      - 177.71.157.58
      - 177.71.172.241
```

```
      - 18.228.146.29
      - 18.228.72.211
      - 18.229.42.145
      - 18.230.128.190
      - 18.230.248.68
      - 18.231.63.251
      - 52.67.132.185
      - 52.67.148.235
      - 52.67.210.165
      - 52.67.90.227
      - 54.207.19.93
      - 54.207.22.2
      - 54.232.194.234
      - 54.94.213.6
      - 54.94.232.220
  Canada (Central):
    ips:
      - 15.156.225.124
      - 15.157.147.102
      - 15.157.151.0
      - 15.157.153.35
      - 3.98.225.135
      - 3.98.254.97
      - 3.99.84.120
      - 3.99.95.71
      - 35.183.163.199
      - 52.60.79.39
      - 15.157.113.2
      - 15.157.126.225
      - 15.157.40.249
      - 3.96.39.0
      - 3.98.227.70
      - 3.99.107.229
      - 3.99.3.196
      - 3.99.93.31
      - 35.183.143.180
      - 99.79.90.118
  Canada (West):
    ips:
      -  40.176.7.159
      -  40.176.20.123
      -  40.176.67.12
      -  40.176.77.82
      -  40.176.139.190
      -  40.176.153.233
      -  40.176.195.231
      -  40.176.214.104
      -  40.176.226.233
      -  40.177.18.235
      -  40.177.36.59
      -  40.177.55.226
      -  40.177.61.136
      -  40.177.63.115
      -  40.177.92.127
      -  40.177.141.16
      -  40.177.167.252
      -  40.177.208.203
      -  40.177.238.210
      -  40.177.238.212
Europe (Milan):
    ips:
      -  15.160.53.115
```

```
      -  15.161.0.202
      -  15.161.39.207
      -  18.102.153.48
      -  18.102.159.106
      -  18.102.177.57
      -  18.102.182.234
      -  18.102.187.206
      -  18.102.196.17
      -  18.102.45.73
      -  18.102.91.72
      -  35.152.118.225
      -  35.152.167.13
      -  35.152.213.106
      -  35.152.224.216
      -  35.152.237.192
      -  35.152.244.77
      -  35.152.253.133
      -  51.118.13.211
      -  51.118.7.166
Europe (Paris):
   ips:
      - 13.36.121.64
      - 15.236.232.91
      - 15.224.5.160
      - 13.38.161.23
      - 13.37.178.207
      - 35.181.109.170
      - 13.36.72.30
      - 13.36.185.51
      - 13.39.168.193
      - 51.44.93.189
      - 13.39.68.213
      - 15.237.12.254
      - 15.236.115.130
      - 51.44.119.173
      - 51.44.62.204
      - 13.36.17.207
      - 51.45.27.62
      - 35.180.176.136
      - 51.44.89.8
      - 13.39.174.8
      - 13.36.140.148
      - 13.39.216.17
Europe (Spain):
   ips:
      -  18.100.200.197
      -  51.48.173.95
      -  51.48.21.117
      -  51.48.224.26
      -  51.48.227.60
      -  51.48.240.60
      -  51.48.249.41
      -  51.48.62.184
      -  51.49.0.51
      -  51.49.18.44
      -  51.49.4.206
      -  51.49.43.169
      -  51.49.69.222
      -  51.49.77.144
      -  51.94.12.47
      -  51.94.176.146
      -  51.95.0.89
```

```
      -  51.95.53.118
      -  51.95.71.11
      -  51.95.88.136
Europe (Stockholm):
   ips:
     - 13.48.0.216
     - 13.48.163.57
     - 13.48.51.151
     - 13.49.210.230
     - 13.49.82.243
     - 13.49.99.155
     - 13.50.188.96
     - 13.50.219.204
     - 13.50.60.146
     - 13.50.82.81
     - 13.51.227.10
     - 13.60.111.239
     - 16.16.140.11
     - 16.16.181.111
     - 16.170.127.220
     - 16.170.176.42
     - 16.171.77.186
     - 51.21.138.79
     - 51.21.34.233
     - 51.21.83.189
Germany:
   ips:
     - 18.153.111.87
     - 18.153.141.55
     - 18.153.182.82
     - 18.153.211.50
     - 18.153.226.161
     - 18.197.243.109
     - 18.198.182.51
     - 18.199.59.8
     - 3.120.17.186
     - 3.125.254.147
     - 3.66.137.143
     - 3.67.16.210
     - 3.67.28.205
     - 3.71.158.156
     - 3.74.137.87
     - 35.158.253.14
     - 35.158.50.0
     - 52.29.71.12
     - 52.58.11.21
     - 52.58.217.77
 India (South):
   ips:
     - 18.60.194.164
     - 18.60.248.246
     - 18.60.35.221
     - 18.60.94.51
     - 18.61.109.18
     - 18.61.192.168
     - 18.61.218.23
     - 18.61.222.116
     - 18.61.239.220
     - 18.61.46.124
     - 98.130.21.18
     - 98.130.23.174
     - 98.130.27.157
```

```
    - 98.130.31.27
    - 98.130.38.229
    - 98.130.39.60
    - 98.130.75.29
    - 98.130.76.179
    - 98.130.77.91
    - 98.130.80.125
    - 163.129.195.0/24
India (West):
  ips:
    - 13.126.152.179
    - 13.126.229.165
    - 13.127.162.151
    - 13.127.38.154
    - 13.200.185.159
    - 13.200.201.134
    - 13.200.232.199
    - 13.232.69.203
    - 13.233.51.89
    - 15.207.1.100
    - 3.109.170.206
    - 3.109.91.124
    - 3.111.127.158
    - 3.111.174.227
    - 3.111.73.187
    - 3.6.110.13
    - 65.0.112.175
    - 65.1.188.156
    - 65.1.87.105
    - 65.2.65.37
    - 163.129.199.0/24
Indonesia (Jakarta):
  ips:
    - 108.136.187.213
    - 108.137.175.7
    - 16.78.15.57
    - 43.218.195.124
    - 43.218.196.146
    - 43.218.238.209
    - 43.218.252.55
    - 43.218.253.33
    - 43.218.254.184
    - 43.218.8.253
    - 108.136.152.244
    - 108.137.117.124
    - 108.137.143.159
    - 16.78.12.144
    - 43.218.210.218
    - 43.218.214.88
    - 43.218.230.129
    - 43.218.248.115
    - 43.218.248.217
    - 43.218.252.86
Israel:
 ips:
    - 51.16.148.190
    - 51.16.195.201
    - 51.16.196.219
    - 51.16.224.73
    - 51.17.10.222
    - 51.17.102.144
    - 51.17.117.216
```

```
      - 51.17.125.59
      - 51.17.148.214
      - 51.17.150.75
      - 51.17.150.81
      - 51.17.153.18
      - 51.17.173.27
      - 51.17.178.175
      - 51.17.181.142
      - 51.17.198.69
      - 51.17.200.93
      - 51.17.57.22
      - 51.17.67.196
      - 51.17.71.123
 Japan (Tokyo):
   ips:
     - 18.176.125.195
     - 18.177.180.173
     - 18.178.72.165
     - 18.179.18.63
     - 18.181.113.214
     - 18.181.45.60
     - 3.113.110.233
     - 3.114.181.43
     - 35.75.158.92
     - 35.75.252.128
     - 35.77.152.111
     - 35.78.39.17
     - 52.192.121.95
     - 52.193.133.13
     - 52.194.109.230
     - 52.69.214.33
     - 54.95.128.80
     - 57.180.203.125
     - 57.180.88.2
     - 57.181.86.151
     - 151.186.118.0/24
LATAM (Mexico):
   ips:
     -  78.12.97.7
     -  78.12.123.164
     -  78.12.157.95
     -  78.12.172.128
     -  78.12.178.148
     -  78.12.181.252
     -  78.12.202.255
     -  78.13.9.47
     -  78.13.27.180
     -  78.13.29.91
     -  78.13.38.110
     -  78.13.57.99
     -  78.13.70.127
     -  78.13.84.179
     -  78.13.91.235
     -  78.13.149.241
     -  78.13.159.132
     -  78.13.159.216
     -  78.13.161.237
     -  78.13.163.195
Middle East (Saudi Arabia):
   ips:
     - 151.186.110.0/24
     - 151.186.127.0/24
```

```
Middle East (UAE):
   ips:
     - 3.28.30.234
     - 3.29.10.20
     - 3.29.120.102
     - 3.29.251.187
     - 3.29.38.214
     - 3.29.45.234
     - 40.172.32.63
     - 40.172.44.109
     - 40.172.47.132
     - 40.172.58.138
     - 40.172.59.24
     - 40.172.64.122
     - 40.172.67.216
     - 40.172.68.53
     - 40.172.74.42
     - 40.172.75.235
     - 40.172.82.196
     - 51.112.58.162
     - 51.112.85.49
     - 51.112.87.103
Singapore:
   ips:
    - 13.214.98.31
    - 13.215.125.242
    - 13.228.35.51
    - 18.136.254.192
    - 18.139.251.40
    - 18.142.126.162
    - 18.142.33.94
    - 18.142.74.94
    - 18.143.9.34
    - 3.0.178.57
    - 3.0.197.90
    - 3.0.236.175
    - 3.0.39.255
    - 3.1.174.140
    - 47.128.172.134
    - 47.128.191.7
    - 52.74.119.66
    - 52.74.87.15
    - 52.76.130.198
    - 54.179.86.196
 Switzerland (Zurich):
   ips:
    - 16.62.10.95
    - 16.63.1.64
    - 16.63.119.220
    - 16.63.146.151
    - 16.63.191.113
    - 16.63.241.246
    - 16.63.248.194
    - 16.63.50.209
    - 16.63.81.145
    - 51.96.4.88
    - 16.62.175.191
    - 16.62.234.167
    - 16.63.143.46
    - 16.63.184.108
    - 16.63.216.64
    - 16.63.224.127
```

```
    - 16.63.230.1
    - 16.63.236.61
    - 16.63.246.9
    - 16.63.250.231
United Kingdom:
  ips:
    - 13.42.241.158
    - 18.135.112.200
    - 18.168.160.22
    - 18.168.223.23
    - 18.169.141.252
    - 18.170.109.89
    - 18.170.162.124
    - 18.170.245.252
    - 18.171.14.50
    - 3.11.157.254
    - 3.11.225.126
    - 3.8.14.231
    - 3.9.163.167
    - 35.176.186.56
    - 35.177.223.97
    - 35.177.252.178
    - 35.178.14.215
    - 35.178.147.15
    - 35.178.164.29
    - 35.178.223.106
    - 163.129.223.0/24
    - 163.129.235.0/24
US East (Miami, Florida):
  ips:
    - 151.186.82.0/24
US East (Reston, Virginia):
  ips:
    - 151.186.86.0/24
US (Midwest):
  ips:
    - 18.190.167.133
    - 18.220.203.100
    - 18.224.162.164
    - 18.224.232.77
    - 3.128.167.118
    - 3.129.236.62
    - 3.129.49.88
    - 3.13.65.14
    - 3.130.93.106
    - 3.132.35.188
    - 3.135.147.177
    - 3.138.228.182
    - 3.138.240.248
    - 3.139.144.205
    - 3.141.67.95
    - 3.147.235.189
    - 3.15.63.151
    - 3.16.185.117
    - 3.17.22.235
    - 52.14.247.24
US (Pacific Northwest):
  ips:
    - 100.20.55.128
    - 34.210.182.194
    - 34.211.133.49
    - 35.163.230.204
```

```
      - 35.167.192.160
      - 35.82.37.34
      - 44.226.181.121
      - 44.227.223.79
      - 44.227.59.253
      - 44.228.41.46
      - 44.231.2.184
      - 44.232.163.156
      - 52.10.7.185
      - 52.24.201.181
      - 52.35.186.20
      - 52.36.167.192
      - 52.43.252.155
      - 54.185.253.229
      - 54.68.79.94
      - 54.69.85.241
  US (Virginia):
    ips:
      - 18.207.48.91
      - 3.208.132.58
      - 3.220.27.92
      - 3.224.76.22
      - 3.229.59.4
      - 3.229.98.228
      - 34.199.204.168
      - 34.234.106.45
      - 35.171.156.209
      - 44.205.38.30
      - 44.206.168.122
      - 44.214.98.67
      - 44.217.43.177
      - 44.221.120.37
      - 44.221.97.202
      - 52.5.115.214
      - 52.86.227.76
      - 54.160.164.245
      - 54.221.27.20
      - 54.227.68.243
  US West (Los Angeles, California):
    ips:
      - 151.186.94.0/24
  US West (San Jose, California):
    ips:
      - 151.186.90.0/24
```

Realtime DLP secure ICAP requirements

Network requirements to support real time DLP secure ICAP and prevent abuse of the API connection.

If you use ICAP to integrate the Secure Access Realtime DLP with your on-premesis DLP, we recommend you allow only the following IP addresses to your firewall to prevent abuse of the API connection:

- 184.72.63.136
- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

In addition, EU customers should add the following IP addresses to that list:

- 3.120.233.38
- 3.65.158.141
- 18.168.8.192
- 18.132.175

SaaS tenant requirements

Network requirements to support Cisco Secure Client deployments with the Virtual Private Network (VPN) and Umbrella Roaming Security modules, or Secure Access PAC file deployments.

Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) and Umbrella Roaming Security modules, or Secure Access PAC file deployments.

The Cisco Secure Client Zero uses HTTPS to communicate with the Secure Web Gateway proxy services.

Microsoft 365

Describes Microsoft 365 in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Microsoft 365 traffic is sent directly to the Secure Access secure web gateway (SWG) for these deployment methods:

- VPN and Network Tunnels established on a network device
- Cisco Secure Client with the VPN and Umbrella Roaming Security modules
- Secure Access PAC file

To stop network traffic from connecting to the Secure Access SWG, add `External Domain` entries manually or route the traffic direct to the internet from your connecting devices.

If your organization's firewall rules prevent any third-party applications, allow the following IP addresses:

- 52.73.52.135
- 52.71.142.118
- 52.40.204.69
- 52.35.119.173
- 52.27.150.153

SAML identity provider requirements

Network requirements to support Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

If you intend to configure Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML IdPs, ensure that your network meets the requirements for your deployment.

Secure Access SAML Gateway Services

Describes Secure Access SAML Gateway Services. Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules and Secure Access integrations with SAML identity providers (IdPs).

Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules and Secure Access integrations with SAML identity providers (IdPs).

You must deploy either a Network Tunnel or PAC file in your organization to connect user devices to the Secure Access Secure Web Gateway (SWG).

We recommend that you allow all traffic on port 443 over TCP for the Secure Access SAML Gateway services domains.

Unless noted, send **id.sse.cisco.com** requests to the SWG, not directly to the internet.

Domain	Port/Protocol	Description
saml.fg.id.sse.cisco.com	443 TCP	Secure Access SAML Gateway
*.fg.id.sse.cisco.com	443 TCP	Secure Access SAML Gateway (multiple entity IDs)

Active Directory Federation Service SAML Identity Provider

Describes Active Directory Federation Service SAML Identity Provider in Cisco Secure Access. If your organization integrates with SAML Active Directory Federation Service (AD FS) identity provider (IdP), we recommend that you bypass web traffic to *.id.sse.cisco.com on the Secure Access secure web gateway (SWG).

- If your organization integrates with SAML Active Directory Federation Service (AD FS) identity provider (IdP), we recommend that you bypass web traffic to ***.id.sse.cisco.com** on the Secure Access secure web gateway (SWG).

Secure Access SAML Identity Provider Domains

Describes Secure Access SAML Identity Provider Domains. Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

To enable connections to your SAML identity providers (IdPs), allow the following domains in your firewalls on ports 80 and 443 over TCP. Ensure that traffic to your SAML IdP is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.

Domain	Ports/Protocols
ocsp.int-x3.letsencrypt.org	80/443 TCP
isrg.trustid.ocsp.identrust.com	80/443 TCP
*.cisco.com	80/443 TCP
*.opendns.com	80/443 TCP
*.umbrella.com	80/443 TCP
*.sse.cisco.com	80/443 TCP
*.okta.com	80/443 TCP
*.pingidentity.com	80/443 TCP
secure.aadcdn.microsoftonline-p.com	80/443 TCP

Azure AD SAML Identity Provider

Describes Azure AD SAML Identity Provider in Cisco Secure Access. To exclude Azure AD SAML Identity Provider domains from Secure Access SSL Decryption, add the following domain names to your list of bypassed domains.

To exclude Azure AD SAML Identity Provider domains from Secure Access SSL Decryption, add the following domain names to your list of bypassed domains.

Domain	Port/Protocol
login.live.com	80/443 TCP
login.microsoftonline.com	80/443 TCP

Domain	Port/Protocol
msauth.net	80/443 TCP
msftauth.net	80/443 TCP

Secure Access SAML Gateway Client Certificate Revocation Services

Describes Secure Access SAML Gateway Client Certificate Revocation Services. Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

Required by Cisco Secure Client deployments with the Umbrella Roaming Security or Zero Trust modules, and Secure Access integrations with SAML identity providers (IdPs).

We recommend that you allow all traffic on ports 80 over TCP for the Secure Access SAML Gateway Client Certificate Revocation services domains.

Domains	Port/Protocol	Description
validation.identrust.com	80/TCP	Validate SAML certificates

Virtual private network requirements

Network requirements to support virtual private networks (VPN) in Secure Access.

Your network must meet the following requirements for Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

Secure Access VPN Services

Describes Secure Access VPN Services. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

The Cisco Secure Client VPN module uses HTTPS to communicate with the Secure Access VPN client head end services. We recommend that you allow all traffic on ports 443 over TCP or UDP, and ports 500/4500 over IPsec (UDP) for the Secure Access VPN domains.

> **Note**
>
> The Cisco Secure Client VPN module automatically uses TLS 443/UDP when it senses that 443/UDP is open.

Remote access virtual private network (VPN) head end services.

Domain	Port/Protocol
*.vpn.sse.cisco.com	443 TLS (TCP/UDP)
*.vpn.sse.cisco.com	500/4500 IPsec (UDP)

Secure Access VPN Client Certificate Revocation Services

Describes Secure Access VPN Client Certificate Revocation Services. Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

Required by Cisco Secure Client deployments with the Virtual Private Network (VPN) module.

The Cisco Secure Client Zero VPN module uses HTTPS to communicate with the Secure Access VPN client certificate revocation services. We recommend that you allow all traffic on ports 80 over TCP for the Secure Access VPN domains.

Domains	Port/Protocol	Description
*.vpn.sse.cisco.com	80/TCP	Validate VPN certificates

Zero trust access requirements

Network requirements to support zero trust access.

If you intend to configure zero trust access, ensure that your network meets the requirements for your deployment.

Secure Access Zero Trust Client-Based Enrollment Services

Describes Secure Access Zero Trust Client-Based Enrollment Services. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Required by Cisco Secure Client deployments with the Zero Trust module.

The Cisco Secure Client Zero Trust module uses HTTPS to communicate with the Secure Access Zero Trust device enrollment services. We recommend that you allow all traffic on port 443 over TCP for the Secure Access Zero Trust domains.

Domain	Ports/Protocol
ztna.sse.cisco.com	443 TCP
acme.sse.cisco.com	443 TCP
devices.api.umbrella.com	443 TCP
sseposture-routing-commercial.k8s.5c10.org	443 TCP
sseposture-routing-commercial.posture.duosecurity.com	443 TCP

Secure Access Zero Trust Client-Based Proxy Services

Describes Secure Access Zero Trust Client-Based Proxy Services. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Required by Cisco Secure Client deployments with the Zero Trust module.

The Cisco Secure Client Zero Trust module uses HTTPS to communicate with the client-based Secure Access Zero Trust proxy services. We recommend that you allow all traffic on ports 443 for the defined protocols on the Secure Access Zero Trust domains.

Domain	Ports/Protocol
*.ztna.sse.cisco.com	443/TCP
*.zpc.sse.cisco.com	443/TCP and UDP

Domain	Ports/Protocol
*.tia.sse.cisco.com	443/TCP and UDP

Known Network Restrictions for Zero Trust Clients

Describes Known Network Restrictions for Zero Trust Clients in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Secure Access Zero Trust supports any TCP or UDP client applications that do not rely on ICMP or DNS SRV discovery, with the following restrictions:

- The client application must initiate all TCP connections or UDP flows.
- Any protocol requiring a unique client IP address at the server, for example SMBv1, is not supported.

Secure Access Zero Trust Client-Based Proxy – Client Certificate Revocation Services

Describes Secure Access Zero Trust Client-Based Proxy – Client Certificate Revocation Services. Required by Cisco Secure Client deployments with the Zero Trust module.

Required by Cisco Secure Client deployments with the Zero Trust module.

The Cisco Secure Client Zero Trust module uses HTTPS to communicate with the client-based Secure Access Zero Trust client certificate revocation services. We recommend that you allow all traffic on ports 80 and 443 over TCP for the Secure Access Zero Trust Client Certificate Revocation services domains.

Domains	Port/Protocol
*.ztna.sse.cisco.com	443 TCP

Secure Access Zero Trust Proxy Services – Unmanaged Devices

Describes Secure Access Zero Trust Proxy Services – Unmanaged Devices. Required by devices that are on an organization's network, connect to Secure Access with Zero Trust, and do not have the Cisco Secure Client deployed.

Required by devices that are on an organization's network, connect to Secure Access with Zero Trust, and do not have the Cisco Secure Client deployed.

Unmanaged devices with Secure Access Zero Trust enabled use HTTPS to communicate with the Secure Access Zero Trust proxy services for unmanaged devices. We recommend that you allow all traffic on ports 80 and 443 over TCP for the Secure Access Zero Trust proxy services domains.

Domains	Port/Protocol
*.ztna.sse.cisco.com	443 TCP

Secure Access Zero Trust Services and Connector Groups

Describes Secure Access Zero Trust Services and Connector Groups. Required by the Secure Access Zero Trust and Connector Groups deployments in an organization.

Required by the Secure Access Zero Trust and Connector Groups deployments in an organization.

The following IP addresses are reserved for use by Secure Access services for Resource Connectors and must not be used elsewhere on your network.

IP Range
100.64.0.0/10

6 Secure Access Onboarding

Topics:

- Get Started
- Secure Access Onboarding Workflow
- Hybrid Private Access Workflow
- Quickstarts
- Additional Onboarding Resources

Provides an overview of Secure Access Onboarding, including Get Started, Secure Access Onboarding Workflow, and Hybrid Private Access Workflow. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started

Describes Get Started in Cisco Secure Access. Cisco Secure Access provides flexible secure connectivity to the internet, Software-as-a-Service (SaaS) applications, and your private digital and network resources.

Cisco Secure Access provides flexible secure connectivity to the internet, Software-as-a-Service (SaaS) applications, and your private digital and network resources. Secure Access enables you to connect seamlessly to on-premises data centers, public clouds, or private networks from both remote and on-network locations.

Secure Access supports various network configurations and security controls through policy rules. The Secure Access policy defines how your organization manages network traffic, which sources can reach available resources. In a policy rule, you can combine settings from security profiles, posture profiles, and resource access configurations (content categories, application lists, destination lists, security settings), and indicate if the rule is high priority. Rules are organized and controlled entirely by your organization. For more information about policy rules, see Manage the Access Policy.

Prerequisites

- Sign in to Secure Access with single sign-on (SSO) authentication. For more information, see Sign Into Secure Access with Security Cloud Sign On.
- Locate your organization ID through your dashboard URL. For more information, see Find Your Organization ID.
- Learn about the product features in your Cisco Secure Access subscription. For more information, see Determine Your Current Package.

What's Next

- Begin the **Get Started with Cisco Secure Access** workflow. Provision your organization's network connections and users and groups, and set up integrations with SAML identity providers (IdPs). For more information, see Begin Secure Access Onboarding Workflow.

Secure Access Onboarding Workflow

The Get Started with Secure Access onboading workflow guides you through the initial setup of Secure Access.

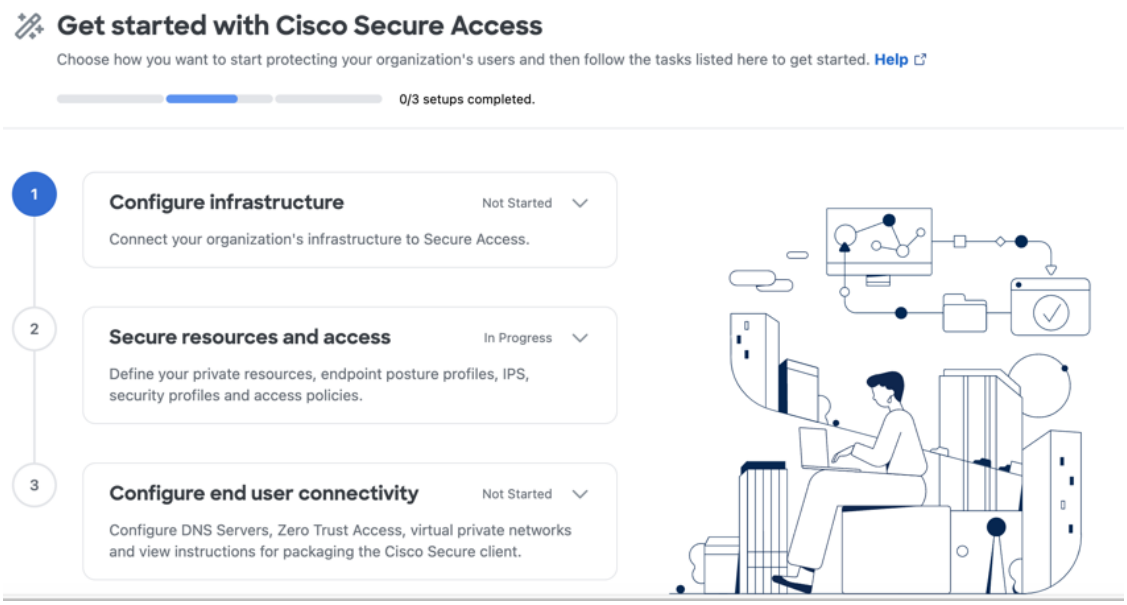
The **Get Started with Cisco Secure Access** workflow guides you through the initial setup of Secure Access.

Sign in to Secure Access and navigate to **Workflows**. The first step in the Get Started workflow takes you through the setup of your organization's network connections–network tunnel groups and network tunnels. At the same time, you can provision users and groups from your organization in Secure Access and set up integrations with Security Assertion Markup Language (SAML) identity providers (IdPs).

After you establish network connections, begin the **Secure resources and access** step in the workflow that includes:

- designing endpoint posture profiles
- IPS and security profiles
- policy rules

Then, in the **Configure end user connectivity** step, define traffic patterns for remote user connections to resources–configure DNS servers, Zero Trust, virtual private networks (VPNs), and internet security settings.



As an administrator, review and audit connections and traffic events in the Secure Access logs and reports. Start with the Secure Access Overview Dashboard. For more information, see Secure Access Overview Dashboard.

- Step 1 - Configure Network Connections
- Step 2 - Configure Access to Resources
- Step 3 - Configure End User Connectivity
- Step 4 - Configure Endpoints and Network Sources

Step 1 – Configure network connections

Step 1 of the Get Started with Cisco Secure Access workflow guides you through the tasks to configure resource connector groups and resource connectors, and then configure network tunnel groups and establish network tunnels to Secure Access.

The **Get Started with Cisco Secure Access** workflow guides you through the tasks in the **Configure Infrastructure** step–configure Resource Connector Groups and Resource Connectors, and configure Network Tunnel Groups and establish network tunnels to Secure Access. After you complete the network connections deployment steps, provision users and groups from your organization in Secure Access and configure integrations with SAML identity providers (IdPs). For more information, see Manage Network Connections.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Task 1 – Add Network Connections

Describes Task 1 - Add Network Connections in Cisco Secure Access. Add Network Tunnel Groups to your organization and deploy and manage IPsec tunnels.

Add Network Tunnel Groups

Add Network Tunnel Groups to your organization and deploy and manage IPsec tunnels. A deployed IPsec tunnel supports connections over a virtual private network (VPN) to resources on the network, or connections secured by Zero Trust Network Access (ZTNA) to the private resources on the network.

- Manage Network Tunnels

Add Resource Connectors and Connector Groups

Add Resource Connector Groups to your organization where a connector group includes at least two Resource Connectors. A Resource Connector Group supports remote network connections using Zero Trust Network Access (ZTNA) to private resources running in private clouds or on-premises data centers.

- Manage Resource Connectors and Connector Groups

Task 2 – Provision Users and Groups

Describes Task 2 - Provision Users and Groups in Cisco Secure Access. Provision users and groups from your organization in Secure Access.

Provision users and groups from your organization in Secure Access. You can configure users and groups though integrations with identity providers (IdPs) or by manually importing a list of users and groups from a comma-separated values (CSV) file. Once you provision users, you can configure and manage users in profiles that secure and route traffic from user devices. For more information, see Manage Users, Groups and Endpoint Devices.

- Import Users and Groups from CSV File
- Provision Users and Groups from Okta
- Provision Users and Groups from Microsoft Entra ID
- Provision Users and Groups from Active Directory

Task 3 – Configure Integrations with SAML Identity Providers

Describes Task 3 - Configure Integrations with SAML Identity Providers in Cisco Secure Access. Integrate SAML identity providers (IdPs) and users in your organization in Secure Access.

Integrate SAML identity providers (IdPs) and users in your organization in Secure Access. For more information, see Configure Integrations with SAML Identity Providers.

- Configure Azure AD for SAML
- Configure Okta for SAML
- Configure AD FS for SAML
- Configure Duo Security for SAML
- Configure PingID for SAML
- Configure OpenAM for SAML

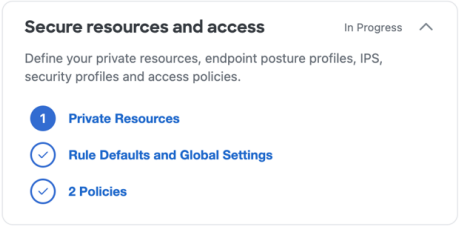
What's Next

- Step 2 - Configure Access to Resources

Step 2 – Configure access to resources

Step 2 of the Get Started with Cisco Secure Access workflow guides you through the tasks to secure your private resources, enable access controls on resources, and create policy rules.

The **Get Started with Secure Access** workflow guides you through the tasks in the **Secure Resources and Access** step–secure your private resources, enable access controls on resources, and create policy rules. For more information, see Manage Private Resources.



Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Task 1 – Set Up Private Resources

Describes Task 1 – Set Up Private Resources in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Configure access to private resources for your users. Private resources are private subnets (IPv4 routes) and applications deployed and managed by your organization.

- Manage Private Resources

Task 2 – Configure Rule Defaults and Global Settings

Describes Task 2 – Configure Rule Defaults and Global Settings in Cisco Secure Access. Set up Secure Access rule defaults and global settings to access private resources.

Set up Secure Access rule defaults and global settings to access private resources.

Manage Rule Defaults

- Manage IPS Profiles
- Manage Security Profiles
- Manage Zero Trust Access Posture Profiles
- Manage VPN Connection Posture Profiles
- Manage Tenant Controls
- Manage Certificates
- Manage Threat Categories

Manage Global Settings

Manage the settings that apply to all policy rules. The Secure Access policy has both global and default settings.

Global Settings:

- Global Settings for Private Access Rules
- Global Settings for Internet Access Rules

Default Settings:

- Default Settings for Private Access Rules
- Default Settings for Internet Access Rules

Task 3 – Add a Policy Rule

Describes Task 3 – Add a Policy Rule in Cisco Secure Access. Configure and add rules to the Secure Access policy.

Configure and add rules to the Secure Access policy.

- Manage the Access Policy

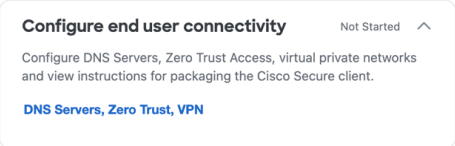
What's Next

- Step 3 – Configure End User Connectivity

Step 3 - Configure end user connectivity

Step 3 of the Get Started with Cisco Secure Access workflow guides you through the tasks to configure DNS servers, internet security, virtual private networks (VPNs), and zero trust (ZT) access for user devices.

The **Get Started with Secure Access** workflow guides you through the tasks in the **Configure End User Connectivity** step—configure DNS servers, internet security, virtual private networks (VPNs), and Zero Trust (ZT) access for user devices.



Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Task 1 – Configure Zero Trust

Configure connections to private resources from user devices.

- Manage Traffic Steering for Cisco Secure Client Connections
- Enable Pre or Post-login authentication to establish zero trust sessions with private or public resources prior to a user logging into the device or continuous authentication post-login.

Task 2 – Configure Virtual Private Networks

Set up virtual private networks (VPNs) settings.

- Manage Virtual Private Networks

Task 3 – Configure Internet Security

Add DNS servers, add domains to internal domains list, configure internet security settings for the Cisco Secure Client.

- Add DNS Servers
- Manage Internet Security

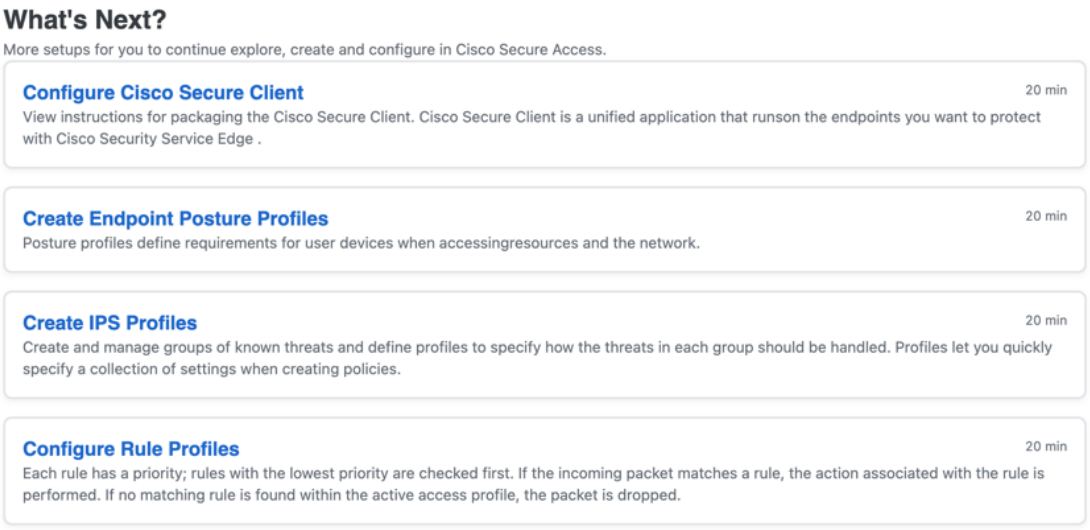
Configure Endpoints and Networks

- Step 4 - Configure Endpoints and Network Sources

Step 4 – Configure endpoints and network sources

Step 4 of the Get Started with Cisco Secure Access workflow guides you through the tasks to configure your organization's user devices, add registered and internal networks to Secure Access, and configure IPS and endpoint posture profiles in policy rules.

The **Get Started with Secure Access** workflow guides you through the tasks in the **What's Next** step—configure your organization's user devices, add registered and internal networks to Secure Access, and configure IPS and endpoint posture profiles in policy rules.



Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Add Networks to Secure Access

- Manage Registered Networks
- Manage Internal Networks

Set Up the Cisco Secure Client

- Download the Cisco Secure Client
- Download the OrgInfo.json File
- Download the VPN XML File
- Install the Cisco Secure Client
- Manage Zero Trust Access on Cisco Secure Client

Add IPS Profiles

- Manage IPS Profiles

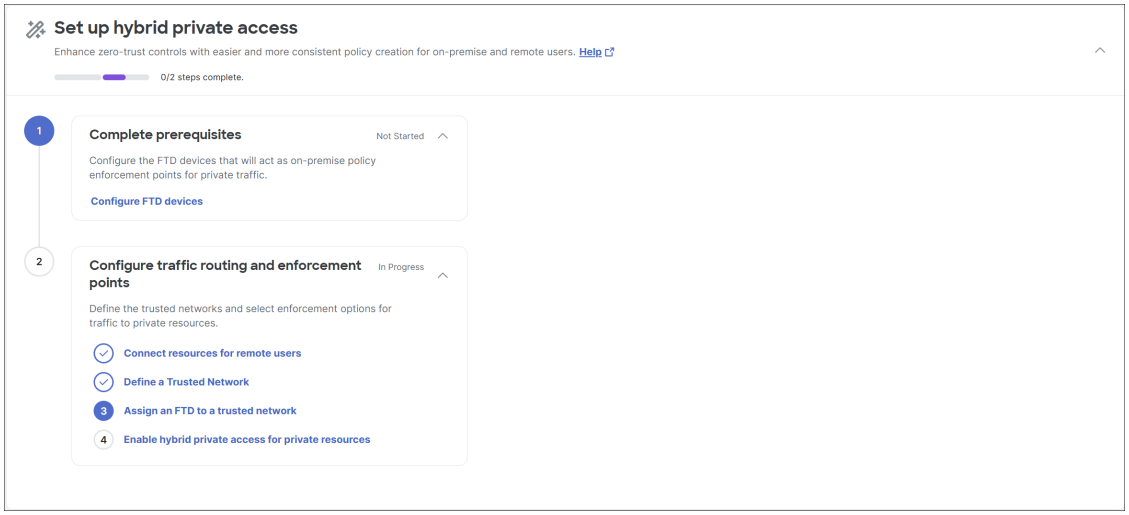
Configure Rule Profiles

- Manage the Access Policy

Hybrid Private Access Workflow

The set up hybrid private access workflow enables you to configure universal Zero Trust Network Access (ZTNA).

The set up hybrid private access workflow walks you through configuring universal Zero Trust Network Access (ZTNA). Note that you can modify any part of the configuration, as required.



The Set up hybrid private access workflow consists of these broad steps:

1. Configure FTD devices: This step guides you through the process of configuring the Firewall Threat Defense devices in Security Cloud Control to enable universal Zero Trust Network Access. After configuration, the Threat Defense devices are displayed in Secure Access under Connect > Network Connections > FTDs, from where you can configure traffic routing and enforcement points.
2. Configure traffic routing and enforcement points. This step consists of four tasks:
   a. Connect resources for remote users: This task guides you through the process of adding resource connector groups or network tunnel groups. A resource connector group supports remote network connections using Zero Trust Network Access to private resources.
   b. Define a trusted network: This task guides you through the process of adding trusted networks. These networks enable the system to recognize when an endpoint device is connected to a predefined trusted network, allowing the system to enforce security policies and control access to associated private resources.
   c. Assign an FTD to a trusted network: This task guides you through the process of assigning trusted networks to a Threat Defense device. In turn, the Threat Defense device enforces policies for the private resources associated with the assigned trusted network.
   d. Enable hybrid private access for private resources: This task guides you through the process of associating private resources with a Threat Defense device to ensure on-premises rule enforcement instead of on-cloud enforcement.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. To perform the steps in this wizard, you must have the Full Admin user role.

This procedure describes in detail, the steps listed in **Set up hybrid private access**.

Before you begin

To perform the steps in this wizard, you must have the Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Sign in to Security Cloud Control and navigate to **Secure Access > Home**.
2. Click Complete prerequisites.
3. Click Configure FTD devices.

The Onboard FTD Device page opens in a new tab.

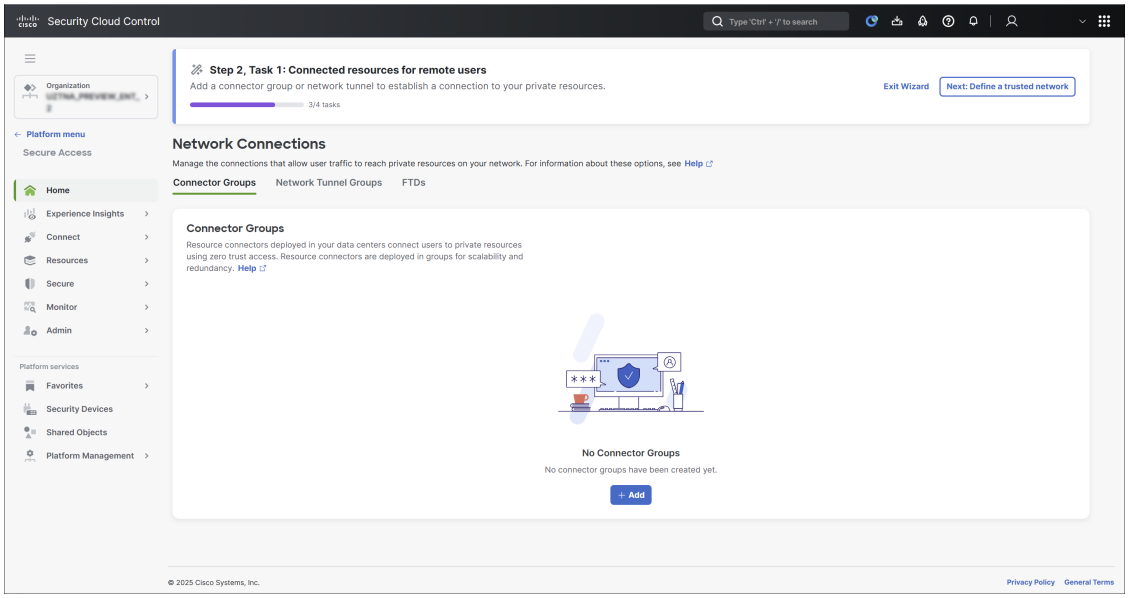
4. Configure the Firewall Threat Defense devices to be used for universal ZTNA.

   For more information about onboarding Firewall Threat Defense devices using Firewall Management Center, see the "Register With the Management Center" section of the "Device Management" chapter in the Secure Firewall Management Center Device Configuration Guide.

   For more information about onboarding Firewall Threat Defense devices using Cloud-Delivered Firewall Management Center(cdFMC), see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control.

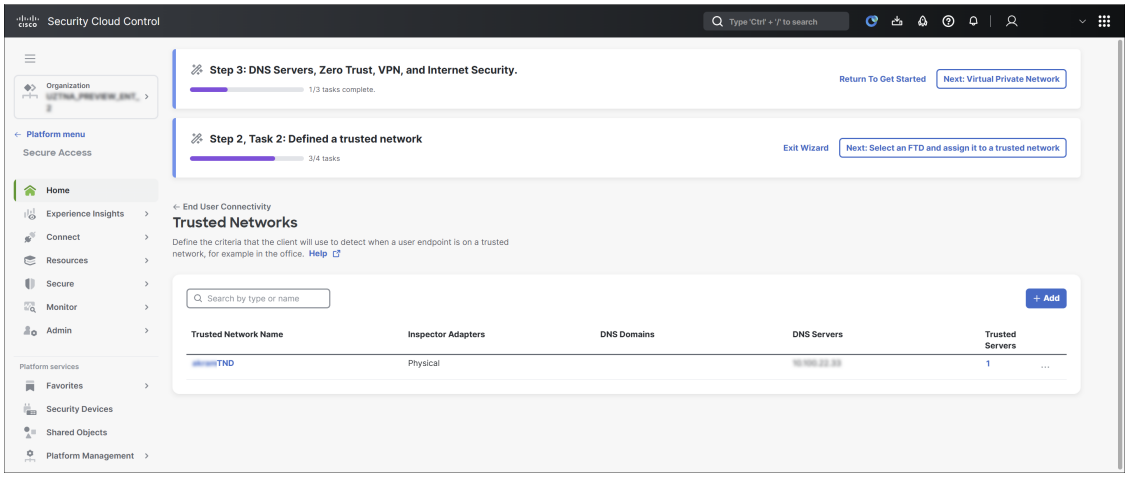
   For more information on configuring Firewall Threat Defense devices for universal ZTNA, see Configure Firewall in Security Cloud Control.

5. Click **Configure traffic routing and enforcement points.**
6. Click **Connect resources for remote users**.
7. Add the required connector groups or network tunnel groups.



   For more information on adding connector groups, see Manage Resource Connectors and Connector Groups.

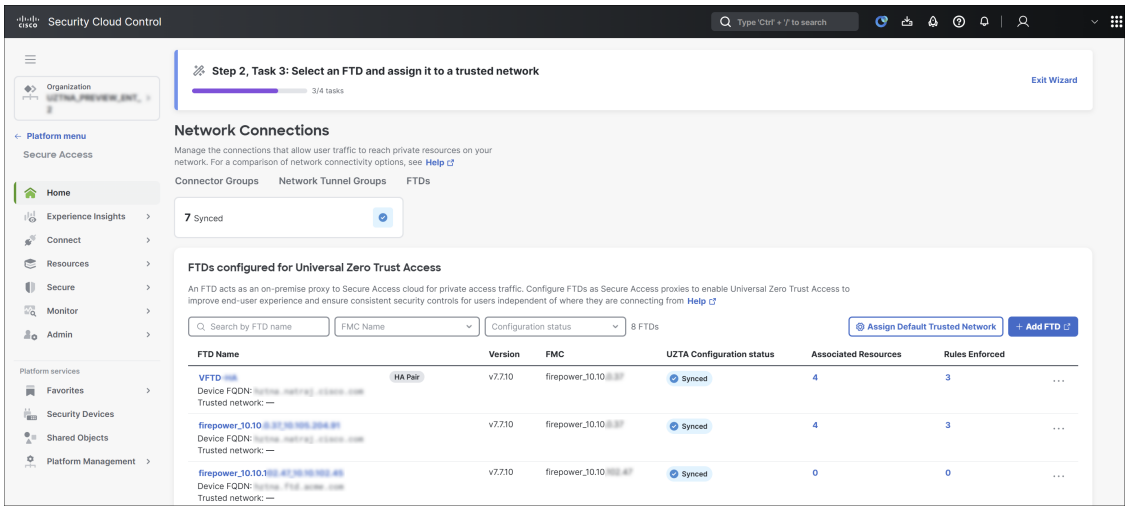
8. Click **Next: Define a trusted network**.
9. Define the required trusted networks.



   For more information on defining a trusted network, see Trusted Networks for Zero Trust Access Connections.

10. Click **Next: Select an FTD and assign it to a trusted network**.
11. Assign trusted networks to the Threat Defense devices.

    For more information on assigning trusted networks to Threat Defense devices, see Assign a Trusted Network to Threat Defense devices.
12. Associate private resources with Threat Defense devices.



    For more information on associating private resources with Threat Defense devices, see Associate Private Resources with Threat Defense Devices.
13. Click **Exit Wizard** to close the wizard.

Quickstarts

Quickstarts walk you through the recommended order of tasks to set up a specific deployment, linking out to the procedures for completing them.

Quickstart tasks are designed as individual onboarding workflows. A workflow describes how to connect users in your organization securely to private, Software as a Service (SaaS), and public internet resources using various deployments.

A user device can connect securely to resources through the following types of deployments:

- Cisco Secure Client deployed with the zero trust access module. For more information, see Quickstart - Cisco Secure Client with Zero Trust.
- Cisco Secure Client deployed with virtual private networks (VPNs). For more information, see Quickstart - Cisco Secure Client with Virtual Private Network.
- Cisco Secure Client deployed with Internet Security. For more information, see Quickstart - Cisco Secure Client with Internet Security.
- A browser on a user device with a deployed PAC file. Configure a Secure Access security profile for internet access and enable SAML authentication. For more information, see Quickstart - Browser with SAML Authentication.
- An unmanaged device connecting with zero trust (ZT). For more information, see Quickstart - Bring Your Own Device with Zero Trust.

Prerequisites for Quickstarts

- Sign in to Secure Access with single sign-on (SSO) authentication. For more information, see Sign Into Secure Access with Security Cloud Sign On.
- Locate your organization ID through your Secure Access URL. For more information, see Find Your Organization ID.
- Learn about the product features in your Cisco Secure Access subscription. For more information, see Determine Your Current Package.

Quickstart – Cisco Secure Client with Zero Trust Access

Provides instructions for completing the Quickstart - Cisco Secure Client with Zero Trust Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Cisco Secure Client with Zero Trust Access connects user devices securely to private resources in on-premises data centers managed by your organization and resources in private and public clouds. Cisco Secure Access Zero supports visibility into user and device identities, network connectivity, and security posture.

User devices must have the Cisco Secure Client with Zero Trust Access deployed and configure a Secure Access Zero Trust Access endpoint posture profile. Users are members of the organization who manages their devices. An administrator must configure the Zero Trust Access endpoint posture profiles in Secure Access and apply a policy rule that includes the Zero Trust Access profiles to the user devices.

The procedure to start onboarding user devices in an organization with the Secure Client and Zero Trust Access should take no more than ten minutes.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy connector groups in Secure Access. For more information, see Manage Resource Connectors and Connector Groups.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create Zero Trust (ZT) posture profiles for the user devices in the organization. For more information, see Manage Zero Trust Access Posture Profile.
5. Create a policy rule or add an ZT posture profile to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with Zero Trust on user devices.
   - Download the Cisco Secure Client
   - Install the Cisco Secure Client
   - Invite Users to Enroll in Zero Trust Access for Secure Client

What to do next

- Check that you can reach private resources protected by Secure Access.

Quickstart – Cisco Secure Client with Virtual Private Network

Provides instructions for completing the Quickstart - Cisco Secure Client with Virtual Private Network workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Client with VPN connects user devices securely to private resources in data centers managed by your organization and software as a service (SaaS) resources in private and public clouds. The procedure to start onboarding user devices in an organization with the Cisco Secure Client and VPN access should take no more than ten minutes.

A VPN provides a point-to-point, private network between a user device and a resource where the traffic sent over the network is encrypted and the IP address of the source is hidden.

User devices must have the Secure Client deployed with the VPN module and VPN XML metadata file, and configure a Secure Access VPN endpoint posture profile. Users are members of the Secure Access organization that manages their devices. An administrator must configure the network connections–Network Tunnel Groups or Resource Connector Groups–for the organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy connector groups in Secure Access. For more information, see Manage Resource Connectors and Connector Groups.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a VPN endpoint posture profile for the user devices. For more information, see Add a VPN Connection Posture Profile.
5. Create a policy rule or add a VPN endpoint posture profile for the user devices to an existing Secure Access rule. For more information, see About the Access Policy.
6. Deploy Cisco Secure Client with VPN on user devices in the organization.
   - Download the Cisco Secure Client
   - Download the VPN XML File
   - Install the Cisco Secure Client

What to do next

- Check that you can reach private, SaaS, and internet resources protected by Secure Access.

Quickstart – Cisco Secure Client with Internet Security

Provides instructions for completing the Quickstart - Cisco Secure Client with Internet Security workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Cisco Secure Client with Internet Security—DNS-layer security and Secure Web Gateway (SWG)—connects user devices securely to internet resources. The procedure to start onboarding user devices in an organization with the Cisco Secure Client and Internet Security access should take no more than ten minutes.

User devices must have the Cisco Secure Client deployed with the Umbrella module. Users are members of the organization that manages their devices. An administrator must configure the network connections—Network Tunnel Groups—and add Registered Networks and Internal Networks to their Secure Access organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create a Web posture profile for the user devices. For more information, see Add a Web Profile.
5. Create a policy rule or add a Web profile for the user devices to an existing Secure Access rule. For more information, see Manage the Access Policy.
6. Deploy Cisco Secure Client with Umbrella on user devices in the organization.
   - Download the Cisco Secure Client
   - Download the OrgInfo.json File
   - Install the Cisco Secure Client

What to do next

- Check that you can reach internet resources protected by Secure Access.

Quickstart – Browser with SAML Authentication

Provides instructions for completing the Quickstart - Browser with SAML Authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This Quickstart guide describes how to connect user devices securely to internet resources from a browser. The onboarding procedure should take no more than 10 minutes.

User devices must have a browser installed and configure a Secure Access Web profile. Users are members of the organization that manages their devices.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Provision users and groups in Secure Access. For more information, see Manage Users and Groups.
2. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
3. Create a Secure Access Web profile that includes the user devices. For more information, see Add a Web Profile.
4. Set up a Secure Access PAC file. For more information, see Manage PAC Files.
5. Create a policy rule or add a Web profile to an existing Secure Access rule. For more information, see Manage the Access Policy.

What to do next

- Check that you can reach internet resources protected by Secure Access.

Quickstart – Bring Your Own Device with Zero Trust

Provides instructions for completing the Quickstart – Bring Your Own Device with Zero Trust workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access Zero Trust Access can connect unmanaged devices securely to private resources in on-premises data centers managed by your organization and in private and public clouds. Secure Access ZT provides visibility into user and device identities, supports network connectivity, and manages the security posture of unmanaged devices.

Bring your own devices (BYODs) are devices that are not managed by your organization, but are devices that are permitted by your organization to connect to certain private resources. An administrator shares an organization's private resource URL to the user of a BYOD device. An administrator must include the BYOD device in the Secure Access ZT endpoint posture profile and users of the devices are members of the organization.

The procedure to start onboarding unmanaged devices with Secure Access Zero Trust in an organization should take no more than ten minutes.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Deploy network connectors in Secure Access.
   - Deploy connector groups in Secure Access. For more information, see Manage Resource Connectors and Connector Groups.
   - Deploy network tunnel groups in Secure Access. For more information, see Manage Network Tunnel Groups.
   - Configure a network tunnel on a network device from within your data center or public network. For more information, see Device Compatibility and Network Tunnels.
2. Provision users and groups in Secure Access. For more information, see Manage Users and Groups.
3. Configure SAML integrations with identity providers (IdPs). For more information, see Configure Integrations with SAML Identity Providers.
4. Create Zero Trust (ZT) posture profiles for the user devices in the organization. For more information, see Manage Zero Trust Access Posture Profile.

5. Provide Secure Access private resource URLs to users on unmanaged devices.
6. Create a policy rule or add an ZT posture profile to an existing Secure Access rule. For more information, see Manage the Access Policy.

What to do next

- Check that you can reach private resources protected by Secure Access.

Additional Onboarding Resources

Information about and links to additional resources that may help you with onboarding into Secure Access.

To help you get started efficiently, Cisco offers a comprehensive set of onboarding resources.

Cisco Secure Access Pre-Onboarding Checklist

Use this checklist to guide you through items needed before signing into Secure Access for the first time. See, Cisco Secure Access Pre-Onboarding Checklist.

Begin Secure Access Onboarding Workflow

The Get Started with Cisco Secure Access workflow helps you set up Secure Access by guiding you through configuring your network connections, adding users and groups, and integrating with SAML identity providers. It begins after you sign in and navigate to Workflows. See, Begin Secure Access Onboarding Workflow.

Cisco Secure Access Live Demo

Register for one of our live demos and learn how to use Secure Access. Sign up for the next Cisco Secure Access Live Demo.

Cisco Community

The Cisco Community offers videos and information about Secure Access features and implementations. Explore Security videos and look for the **Secure Access** label among Cisco products.

7 Basic Network Setup

Topics:

- Fully Qualified Domain Names for Network Connections
- Manage Registered Networks
- Clear Your DNS Cache
- Manage Internal Networks
- Manage Sites

Provides an overview of Basic Network Setup in Cisco Secure Access, including FQDNs for Network Connections, Manage Registered Networks, and Clear Your DNS Cache. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Fully Qualified Domain Names for Network Connections

Understand how to configure Fully Qualified Domain Names (FQDNs) in Secure Access.

A fully qualified domain name (FQDN) refers to the complete and unique address of an internet presence. It consists of the host name and the domain, and is used to locate specific hosts online and access them using name resolution.

FQDN adds an extra layer of flexibility and precision when you create VPN profiles and access rules, providing enhanced security and simplifying network management. Secure Access offers a robust set of features to safeguard your infrastructure, and among them is the fully qualified domain name (FQDN) feature.

In the context of Secure Access remote access VPNs, FQDN enables you to create VPN profiles based on domain names rather than just IP addresses. This introduces a more flexible approach to controlling network traffic, as it allows for profiles to be defined based on specific services or applications hosted on those domains even when associated IP addresses change dynamically.

About Fully Qualified Domain Names (FQDNs)

Describes About Fully Qualified Domain Names (FQDNs) in Cisco Secure Access. “Fully qualified” refers to the unique identification that guarantees that all of the domain levels are specified.

“Fully qualified” refers to the unique identification that guarantees that all of the domain levels are specified. The fully qualified domain name consists of three or more labels: The top level domain, the domain names, optional subdomains, and the host name. If a domain name doesn't specify all of the labels that are required for the FQDN, then this is called a “Partially Qualified Domain Name” (PQDN). This often means that only the host name is given. The generic name or the FQDN and its IP address is the “Fully Qualified Host Name” (FQHN).

The structure of an FQDN is predefined by the domain name system (DNS). The names of the individual levels in the domain name area are called “labels” and are separated from one another by dots. Each label must consist of 1 to 63 characters and the total FQDN may not exceed 255 characters in total. Only letters, numbers, or dashes can be used. Each label has to have either a letter or a number at the beginning.

The benefits of using FQDN include:

- FQDNs offer more reliability because they don't change when the underlying IP addresses change, such as traffic that's routed through load balancers. This can help to reduce downtime and improve the reliability of your cloud workloads.
- FQDNs are more human-readable and easier to remember than IP addresses. This can make your VPN profiles and policies more readable and easier to maintain.
- FQDNs can help to improve the security of your applications by making it more difficult for DNS spoofing attacks.

Secure Access FQDN objects can be used within hierarchical, global, and regional network VPN policies to regulate traffic to or from specific domains, as discussed in the following sections.

Global FQDN

Describes Global FQDN in Cisco Secure Access. The global aspect of an FQDN refers to its role in the global DNS, which makes it a universally recognized and unique address.

The global aspect of an FQDN refers to its role in the global DNS, which makes it a universally recognized and unique address. It allows your browser or email client to precisely locate a specific server on the internet. Your organization is assigned a global FQDN available to copy and paste as needed. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** to find the global FQDN.

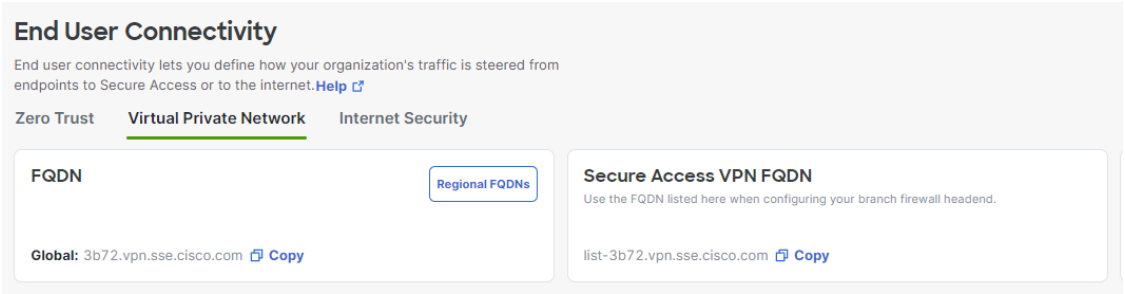
Regional FQDNs

Describes Regional FQDNs in Cisco Secure Access. Regional FQDNs let you create and enforce consistent VPN profiles across all subnetworks within a region in your Secure Access network.

Regional FQDNs let you create and enforce consistent VPN profiles across all subnetworks within a region in your Secure Access network. These profiles contain settings that can determine how VPN traffic traverses your network, including destination exceptions and DNS mode.

When creating a VPN profile, you can opt to automatically add a region-specific FQDN to the hostname, which provides flexibility to clients when connecting to their VPN headend; see Step 1: General Settings of the **Add VPN Profiles** topic.

Your Secure Access regional FQDNs are also available to copy and paste as needed. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** and click **Regional FQDNs** from the global **FQDN** card to view the available regional FQDNs.



VPN Headend FQDN

Describes VPN Headend FQDN in Cisco Secure Access. A VPN headend is a dedicated service that manages multiple concurrent VPN connections between an end user and an enterprise network.

A VPN headend is a dedicated service that manages multiple concurrent VPN connections between an end user and an enterprise network. This function performs encryption for secure communication, security posture checks to verify devices accessing the network, and network segmentation. Your organization is assigned a VPN FQDN to use when configuring your branch firewall headend. This FQDN is available to copy and paste as needed. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** to find the **Secure Access VPN FQDN** card.

Manage Registered Networks

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both IPv4 and IPv6 static IP addresses and dynamic IP addresses over IPv4.

A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules. Secure Access can support high-level entities within your organization—for example, registered or internal networks —or very granular entities—for example, a single user logged into Microsoft o365. For more information about policy rules, see Manage the Access Policy.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both IPv4 and IPv6 static IP addresses and dynamic IP addresses over IPv4. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

To start protecting the networks in your organization, see Add Network Resources.

Add Network Resources

Describes Add Network Resources in Cisco Secure Access. A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both IPv4 and IPv6 for static IP addresses and only IPv4 for dynamic IP addresses. In Secure

Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

To start protecting your public networks managed by your organization, add network resources to Secure Access. Once you've configured and added a network resource, build policy rules to extend Secure Access's protection to any device that connects to the internet from behind that network. For more information about Secure Access policy rules, see Manage the Access Policy.

> **Note**
>
> The Secure Access policy supports the use of PAC files with a public static network. For more information about PAC files, see Manage PAC Files.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Your network's IP address is unique within Secure Access.

Dynamic IP Address—IPv4 Only

Secure Access supports dynamic IP addresses only over IPv4. Most home, small school, and small business networks are provisioned typically by Internet Service Providers (ISPs) with a dynamic IP address (IPv4) when defining each unique internet network.

If you have a dynamic IP address, the public IP of your network changes over time when the lease for that IP address changes. An internet service provider (ISP) provides a dynamic IP address to your device temporarily. Your IP may stay the same for some time period, but the lease eventually expires and is given to another customer of your ISP. When your IP address registered with Secure Access changes, Secure Access's security settings no longer apply. These settings no longer match your account information and you must update the network resource's IP.

Secure Access allows networks with dynamic IPv4 addresses but does not automatically track or update IP changes. When the public IP changes for a dynamic IPv4 address, the access rules in the Access policy no longer apply to the network traffic. You must update a dynamic IPv4 address manually or use a public static IP address.

> **Note**
>
> You cannot use the Umbrella Dynamic Network Update API to modify a dynamic IP address for a Secure Access network resource. Secure Access does not support integrations with Dynamic DNS (DDNS) clients.

Get Started with Network Resources

Add a network resource where the network has a public static IP address or IP address range, or a dynamic IP address.

Note

We recommend that you register all of your organization's networks with Secure Access at the same time. Pre-registering networks ensures that all IP spaces that belong to your organization are added to Secure Access. If you have more than one public egress IP in your organization, configure a network resource for each IP address. You must point your network's DNS to the Secure Access DNS global resolvers. Until your DNS traffic is connected to the Secure Access DNS resolvers, your networks are not protected and traffic is not logged in the Activity Search report.

- Step 1 – Select the Network
- Step 2 – Configure the Network Resource
- Step 3 – Change the DNS Settings on Your Relevant Network Device
- Step 4 – Apply a Policy Rule to the Network Resource
- Step 5 – Test Your Network

Step 1 – Select the Network

Provides instructions for completing the Step 1 – Select the Network workflow in Cisco Secure Access. First, determine the IP address of your network.

First, determine the IP address of your network.

Procedure

1. Go to http://www.whatismyip.com.

   Your IPv4 and IPv6 IP addresses and location are displayed.

2. Use the IP addresses of your network in Step 2 – Configure the Network Resource.

What to do next

Note

Depending on your package, if you attempt to add a network other than the one currently being used to access Secure Access, Secure Access may prompt you to contact Support for manual verification. If this occurs, you'll also need manual verification from Support for IPv4 ranges larger than a /29 network and IPv6 ranges larger than a /56 network. Verification cases are created automatically and you'll receive an update as soon as it's reviewed. For more information about your current package, see Determine Your Current Package.

Step 2 – Configure the Network Resource

Provides instructions for completing the Step 2 – Configure the Network Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access only supports dynamic IP addresses for IPv4. Most home, small school, and small business networks are provisioned typically by Internet Service Providers (ISPs) with a dynamic IP address (IPv4) when defining each unique internet network.

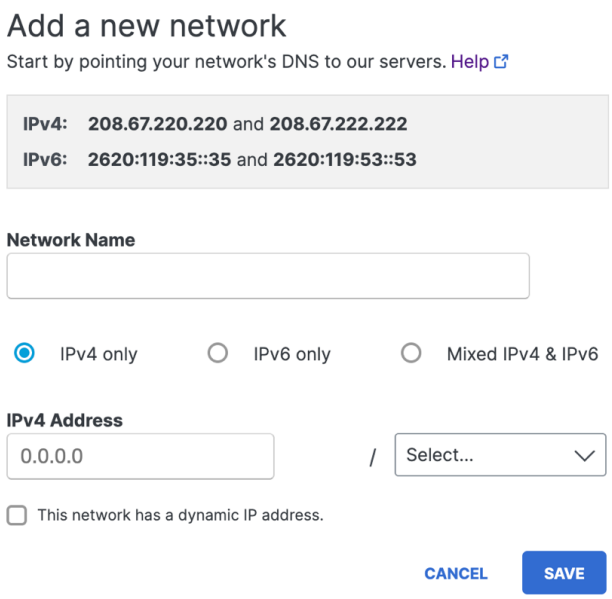
> **Note**
>
> If possible, add the network resource from the IP address used to sign into Secure Access. Otherwise, Secure Access sends an email to the user account and requires that you visit a link from the IP address of the network that you are registering.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Your network's IP address is unique within Secure Access.
- Determine if you have an IPv4 address. For more information, see Add Network Resources.

Procedure

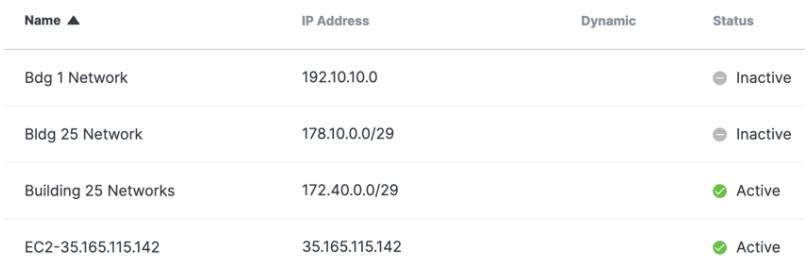
1. Navigate to **Resources** > **Registered Networks** and click **Add**.
2. Give your network resource a descriptive **Network Name**.



3. Choose an internet protocol: **IPv4**, **IPv6**, or **Mixed IPv4 & IPv6**.

   Select a protocol based on the IP address where you have configured your router.
4. Add the network's IP address and choose a subnet mask.
5. For IPv4 only, if you have a dynamic IP address, check **This network has a dynamic IP address**.
6. Click **Save**.

   Once Secure Access validates your IP address, the network resource is listed at **Resources** > **Registered Networks**. Initially, Secure Access lists the status of your network as **Inactive**. When Secure Access receives DNS traffic from the network, the network resource's status changes to **Active**.



Name ▲	IP Address	Dynamic	Status
Bdg 1 Network	192.10.10.0		Inactive
Bldg 25 Network	178.10.0.0/29		Inactive
Building 25 Networks	172.40.0.0/29		Active
EC2-35.165.115.142	35.165.115.142		Active

Step 3 – Change the DNS Settings on Your Relevant Network Device

Describes Step 3 – Change the DNS Settings on Your Relevant Network Device in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You only need to change the DNS settings on your edge DNS equipment, typically a DNS or DHCP server, or a router—a DSL router or cable modem if that's the only router in your network. For information about how to configure devices including laptops or routers, see Point Your DNS to Cisco Secure Access.

Note

The device where you test the network must have retrieved a new set of DNS servers from the DNS/DHCP server or router, or you must change the device's DNS settings manually before verifying the configuration of the network resource.

Step 4 – Apply a Policy Rule to the Network Resource

Describes Step 4 – Apply a Policy Rule to the Network Resource in Cisco Secure Access. Add the network resource to an existing Secure Access policy rule or create a new policy rule and apply the rule to the network resource.

Add the network resource to an existing Secure Access policy rule or create a new policy rule and apply the rule to the network resource. If you do not add the network resource to a policy rule, Secure Access applies the Default policy rule to protect the network resource.

Step 5 – Test Your Network

Describes Step 5 – Test Your Network in Cisco Secure Access. Verify that your network's DNS connections are routed through Cisco Secure Access's global network.You may need to restart your client's network interface or your device.

Verify that your network's DNS connections are routed through Cisco Secure Access's global network.

Note

You may need to restart your client's network interface or your device.

Update a Network Resource

Understand how to update registered network resources, including adding a name and changing IPv4 and IPv6 addresses.

After you add a Registered Network resource—a public static or dynamic IP network—to Cisco Secure Access, you can update the resource.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Edit the Registered Network Resource Name

Provides instructions for completing the Edit the Registered Network Resource Name workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Registered Networks**.
2. Click the pencil icon to edit the Network resource **Name**.
3. Enter a descriptive name for the network and then click **Save**.

Update the Registered Network Resource

Provides instructions for completing the Update the Registered Network Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

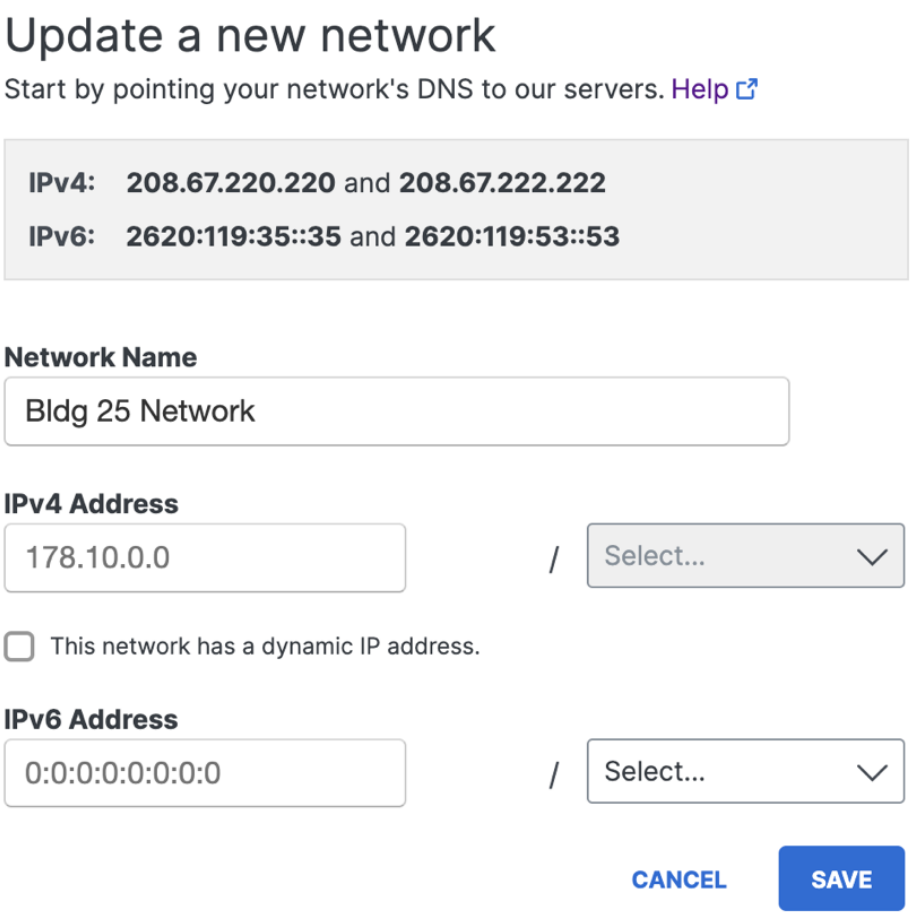
Procedure

1. Navigate to **Resources** > **Registered Networks**.
2. Hover over a network resource and click the **+** to open the configuration dialog.

   The **+** icon does not appear until you hover over the Network resource.

Name ▲	IP Address	Dynamic	Status
Bdg 1 Network	192.10.10.0		Inactive
Bldg 25 Network	178.10.0.0/29		Inactive
Building 25 Networks	172.40.0.0/29		Active
EC2-35.165.115.142	35.165.115.142		Active

3. Follow the steps in Add Network Resources to update the Registered Network resource.



Delete a Network Resource

Provides instructions for completing the Delete a Network Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Once you add a Registered Network resource—a public static or dynamic IP network—to Cisco Secure Access, you can remove the Network resource from Secure Access. After you delete a Network resource, you can no longer apply a policy rule to the resource and the network is not protected by Secure Access.

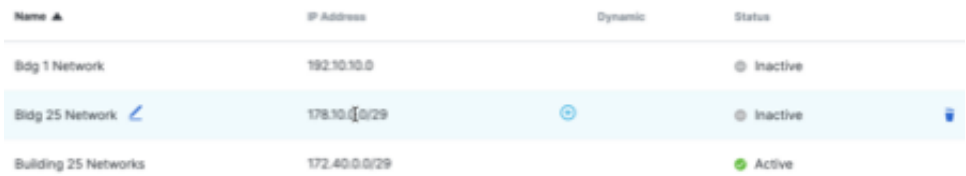
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

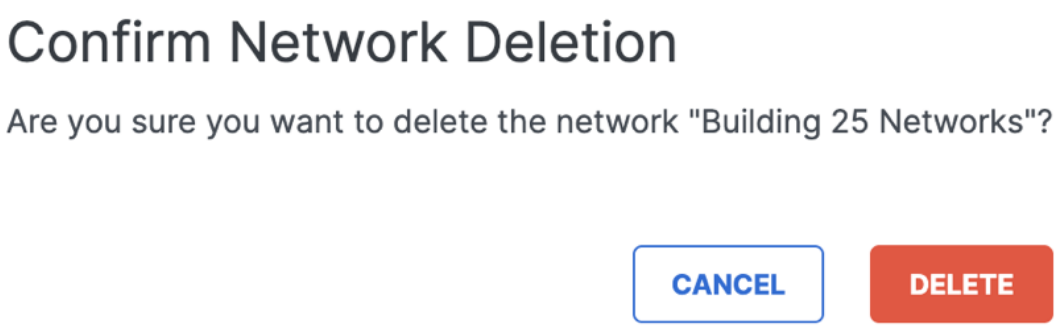
1. Navigate to **Resources** > **Registered Networks**.
2. Hover over a network resource and click the trash can icon (**Delete**).

> **Note**
>
> The trash can icon does not appear until you hover over the Network resource.



3. Click **Delete** to confirm.

   The Network resource is deleted from Secure Access and is removed from any policy rules.



Point Your DNS to Cisco Secure Access

Describes Point Your DNS to Cisco Secure Access. Configure your DNS to direct traffic from your network to the Cisco Secure Access global network.

Configure your DNS to direct traffic from your network to the Cisco Secure Access global network. When a request to resolve a hostname on the internet is made from a network pointed at our DNS addresses, Secure Access applies the security settings configured in your policy rules.

To have Secure Access protect your networks, you need to explicitly change the DNS settings in your operating system or hardware firewall or router to Secure Access's name server IP addresses and turn off the automatic DNS servers provided by your ISP. Secure Access supports both IPv4 and IPv6 addresses.

> **Note**
>
> Several systems allow you to specify multiple DNS servers. We recommend that you only use the Cisco Secure Access DNS servers and do not include any other DNS servers.

Prerequisites

- Administrative privileges on the device or server where the DNS is configured.

Note

We recommend that only users who have administrative access to the router, DNS server, or their own computer attempt to use these instructions as you need this level of access to complete these steps.

Cisco Secure Access DNS Resolvers – IP addresses

Describes Cisco Secure Access DNS Resolvers - IP addresses. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

IPv4	IPv6
208.67.222.222	2620:119:35::35
208.67.220.220	2620:119:53::53

Cisco Secure Access DNS Resolvers – Anycast IP Addresses

Describes Cisco Secure Access DNS Resolvers - Anycast IP Addresses. North America (USA-only) DNS resolvers guarantee only that DNS queries are resolved by a USA-based Secure Access data center.

North America (USA-only) DNS resolvers guarantee only that DNS queries are resolved by a USA-based Secure Access data center. Block pages use global Anycast and may go to any data center, including one located outside of the USA.

IPv4	IPv6	Port/Protocol	Description
208.67.222.222	2620:119:35::35	53 TCP/UDP	Primary
208.67.220.220	2620:119:53::53	53 TCP/UDP	Secondary
208.67.220.222	n/a	53 TCP/UDP	Tertiary
208.67.222.220	n/a	53 TCP/UDP	Quaternary
208.67.221.76	2620:119:17::76	53 TCP/UDP	USA only Primary
208.67.223.76	2620:119:76::76	53 TCP/UDP	USA only Secondary

Procedure for Pointing Your DNS to Cisco Secure Access

Describes Procedure for Pointing Your DNS to Cisco Secure Access. Change the DNS server addresses to Cisco Secure Access DNS server addresses.

Change the DNS server addresses to Cisco Secure Access DNS server addresses.

- Step 1 - Identify Where Your Public DNS Server Addresses Are Configured
- Step 2 - Log Into the Server or Router Where DNS is Configured
- Step 3 - Change Your DNS Server Addresses
- Step 4 - Test Your New DNS Settings

Prerequisites

- Administrative privileges on the device or server where the DNS is configured.

Note

We recommend that only users who have administrative access to the router, DNS server, or their own computer attempt to use these instructions as you need this level of access to complete these steps.

Step 1 – Identify Where Your Public DNS Server Addresses are Configured

Describes Step 1 - Identify Where Your Public DNS Server Addresses are Configured in Cisco Secure Access. Determine which device or server on your network maintains the addresses of your public DNS servers—most often a router or DNS server.

Determine which device or server on your network maintains the addresses of your public DNS servers—most often a router or DNS server. Typically, the device that provides an internal non-routable IP address (DHCP) or the device that serves as your default gateway is also where you configure public DNS servers.

Step 2 – Log Into the Server or Router Where DNS is Configured

Provides instructions for completing the Step 2 - Log Into the Server or Router Where DNS is Configured workflow in Cisco Secure Access. Log into the server or router where the DNS settings are configured.

Procedure

1. Log into the server or router where the DNS settings are configured.
2. Locate the DNS settings for this device. If you are unsure of where these settings are and require guidance on configuring a server or router, see Step 3 - Change Your DNS Server Addresses.

Step 3 – Change Your DNS Server Addresses

Provides instructions for completing the Step 3 - Change Your DNS Server Addresses workflow in Cisco Secure Access. Before you change your DNS settings to use Secure Access, record the current DNS server addresses or settings (for example, write them down on a piece of paper).

Before you change your DNS settings to use Secure Access, record the current DNS server addresses or settings (for example, write them down on a piece of paper). Retain a copy of these DNS settings in case you need to revert to them at a later date.

Some ISPs hard-code their DNS servers into the equipment they provide. If you are using such a device, you can not configure it to use Secure Access. Instead, you can configure each of your computers by installing the Cisco Secure Client or configuring the DNS server addresses on each computer. For more information about configuring a Windows, macOS, or Linux computer, see Computer Configuration.

The process for changing your DNS settings varies according to the operating system and version (Windows, Mac, or Linux) or the device (DNS server, router, or mobile device). This procedure might not apply to your OS, router, or device. For authoritative information, see the vendor documentation.

To change your settings on a typical router:

Procedure

1. In your browser, enter the IP address to access the router's user interface and enter your password.
2. Find the area of configuration in which DNS server settings are specified and replace those addresses with the Cisco Secure Access IP addresses.

IPv4	IPv6
208.67.222.222	2620:119:35::35
208.67.220.220	2620:119:53::53

Primary and Secondary Servers

Provides instructions for completing the Primary and Secondary Servers workflow in Cisco Secure Access. You can use either an IPv4 or IPv6 DNS address as your primary or secondary DNS server.

You can use either an IPv4 or IPv6 DNS address as your primary or secondary DNS server. You must use both numbers and not the same IP address twice. If your router requires a third or fourth DNS server setting, you can use **208.67.220.222** and **208.67.222.220** or **2620:119:35::35** and **2620:119:53::53** as the third and fourth entry respectively.

Procedure

1. Save your changes and exit your router's user interface.
2. Flush your DNS cache.
3. Confirm that your DNS is set as static.
4. Test that your setup is working correctly. See Step 4 – Test Your New DNS Settings.

> **Tip**
>
> When you make changes to DNS, you may have cached results that affect service. Flush your DNS cache to ensure that you're receiving only the latest DNS results. For information on how to flush your DNS cache, see Clear Your DNS Cache.

> **Note**
>
> Email servers have unique DNS configurations. We don't recommend that you configure your email servers to point to Secure Access DNS.

Step 4 – Test Your New DNS Settings

Describes Step 4 – Test Your New DNS Settings in Cisco Secure Access. If you have trouble getting web pages to load, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

If you have trouble getting web pages to load, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Clear Your DNS Cache

Understand how to clear your DNS cache on servers and browsers after you configure your DNS to direct traffic to Secure Access DNS resolvers.

After you configure your DNS to direct traffic from your network to the Cisco Secure Access global DNS resolvers, you may need to clear the DNS cache on your computers, servers, and browsers in your organization.

Prerequisites

- Administrative privileges on the device or server where the DNS is configured and user devices in the organization running browsers.

Clear Your DNS Cache on Computers and Servers

Describes Clear Your DNS Cache on Computers and Servers in Cisco Secure Access. Choose the operating system version of the devices in your organization and follow the steps to clear the DNS cache on the devices.

Choose the operating system version of the devices in your organization and follow the steps to clear the DNS cache on the devices.

Windows 7 and Earlier

Provides instructions for completing the Windows 7 and Earlier workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Click the Start Menu.
2. Navigate to **All Programs**.
3. Choose **Accessories** and right-click **Command Prompt**.
4. Choose **Run as Administrator**.
5. Run the following command in the command line and press enter.

```
ipconfig /flushdns
```

Windows 8 and Newer

Provides instructions for completing the Windows 8 and Newer workflow in Cisco Secure Access. Press the Windows Key or hover over the bottom left corner, and then click the Windows icon.

Procedure

1. Press the Windows Key or hover over the bottom left corner, and then click the Windows icon.
2. Begin typing Command Prompt.
3. Right-click the application and select **Run as Administrator**.
4. Run the following command in the command line and press enter.

```
ipconfig /flushdns
```

OS X 10.4 TIGER

Provides instructions for completing the OS X 10.4 TIGER workflow in Cisco Secure Access. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under **Application/Utilities/Terminal**.
2. Run the following command in the command line and hit enter.

```
lookupd -flushcache
```

OS X 10.5 and 10.6 LEOPARD

Provides instructions for completing the OS X 10.5 and 10.6 LEOPARD workflow in Cisco Secure Access. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under **Application/Utilities/Terminal**.
2. Run the following command in the command line and press enter.

```
dscacheutil -flushcache
```

OS X 10.7 and 10.8 Lion

Provides instructions for completing the OS X 10.7 and 10.8 Lion workflow in Cisco Secure Access. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under **Application/Utilities/Terminal**.
2. Run the following command in the command line and press enter.

```
sudo killall -HUP mDNSResponder
```

OS X 10.9 and 10.10

Provides instructions for completing the OS X 10.9 and 10.10 workflow in Cisco Secure Access. Click the Terminal icon in the dock or in Finder under Application/Utilities/Terminal.

Procedure

1. Click the **Terminal** icon in the dock or in Finder under **Application/Utilities/Terminal**.
2. Run the following command in the command line and press enter.

```
dscacheutil -flushcache;sudo killall -HUP mDNSResponder
```

Linux

Provides instructions for completing the Linux workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Open a terminal window.
2. Run the following command in the command line and press enter.

```
sudo /etc/init.d/nscd restart
```

Ubuntu Linux

Provides instructions for completing the Ubuntu Linux workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Open a terminal window.
2. Run the following command on the command line and press enter.

```
sudo service network-manager restart
```

Clear Your DNS Cache on Browsers

Describes Clear Your DNS Cache on Browsers in Cisco Secure Access. Choose the browser and operating system version of the devices in your organization and follow the steps to clear the DNS cache on the browsers.

Choose the browser and operating system version of the devices in your organization and follow the steps to clear the DNS cache on the browsers.

Internet Explorer 8 and Newer – Windows

Provides instructions for completing the Internet Explorer 8 and Newer – Windows workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to the **History** menu.
2. Select **Delete Browsing History**.
3. Check all boxes except passwords and then click **Delete**.

Mozilla Firefox – Windows

Provides instructions for completing the Mozilla Firefox – Windows workflow in Cisco Secure Access. Click Firefox at the top left of your browser.

Procedure

1. Click Firefox at the top left of your browser.
2. Navigate to the **History** menu.
3. Select **Clear Recent History** and check all boxes.
4. Under **Time range to clear**, select all options except passwords, and then click **Clear Now**.

Apple Safari – macOS

Provides instructions for completing the Apple Safari – macOS workflow in Cisco Secure Access. Expand the cog icon in the upper right corner.

Procedure

1. Expand the cog icon in the upper right corner.
2. Select **Reset Safari**.
3. Check all boxes and then click **Reset**.

Google Chrome – Windows

Provides instructions for completing the Google Chrome – Windows workflow in Cisco Secure Access. Expand the wrench icon in the upper right corner.

Procedure

1. Expand the wrench icon in the upper right corner.
2. Select **History** and check all boxes.
3. Select **Clear data for this time period**, and then choose all options except passwords.
4. Click **Clear Data**.

Google Chrome – macOS

Provides instructions for completing the Google Chrome – macOS workflow in Cisco Secure Access. Navigate to the Chrome menu, and then select More Tools.

Procedure

1. Navigate to the Chrome menu, and then select **More Tools**.
2. Select **Clear Browsing Data**, and then choose all options except passwords.
3. Click **Clear Data**.

Manage Internal Networks

An Internal Network resource represents a private address space of IP addresses that is managed by your organization and is non-routable. Internal networks include local area networks (LANs) found in branch or residential offices.

A resource is an internet capable entity that is managed by your organization. After you add a resource to Cisco Secure Access, your resource is protected against threats and attacks through security configurations defined in policy rules. Secure Access can support high-level entities within your organization—for example, registered or internal networks —or very granular entities—for example, a single user logged into Microsoft o365. For more information about policy rules, see Manage the Access Policy.

An Internal Network resource represents a private address space of IP addresses. Internal networks are managed by your organization and are non-routable. Some examples of internal networks are: local area networks (LANs) found in branch or residential offices. Internal Network resources have Sites, Registered Networks, or Network Tunnel Groups that forward DNS traffic from your organization's internal network to Secure Access.

Add Resources to Associate with Internal Networks

- **Network Tunnel Group**—For more information, see Manage Network Tunnel Groups.
- **Registered Network**—For more information, see Manage Registered Networks.
- **Site**—For more information, see Manage Sites.

To start protecting the internal networks in your organization, see Add Internal Network Resources.

Add Internal Network Resources

Provides instructions for completing the Add Internal Network Resources workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

An Internal Network resource represents a private address space of IP addresses. Internal networks are managed by your organization and are non-routable or RFC1918 compliant. You must configure an Internal Network resource with either a Cisco Secure Access Site, Registered Network, or Network Tunnel Group. The associated Site, Networks, or Network tunnel groups forward DNS traffic from devices on your organization's internal network to Secure Access.

To start protecting an internal network, add an Internal Network resource to Secure Access. Once added, you can apply an existing policy rule to the internal network resource or add a new rule to protect the resource. Build rules to extend Secure Access's protection to any device that connects to the internet from behind the internal network. For more information about Secure Access policy rules, see Manage the Access Policy.

In Secure Access, all traffic originating from the IP of the site, network, or network tunnel group resource is identified as coming from the Internal Network. The private IP space or IP range defines the scope of the resource. The traffic sent from user devices on your organization's Internal Network is visible in the Secure Access Activity Search report.

Add Resources to Associate with Internal Networks

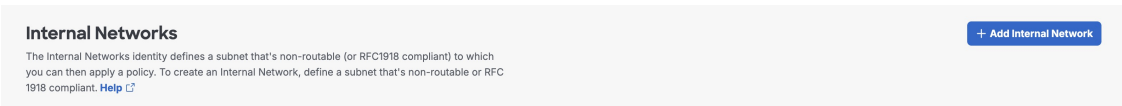
- **Site**—For more information, see Manage Sites.
- **Registered Network**—For more information, see Manage Registered Networks.
- **Network Tunnel Group**—For more information, see Manage Network Tunnel Groups.

Before you begin

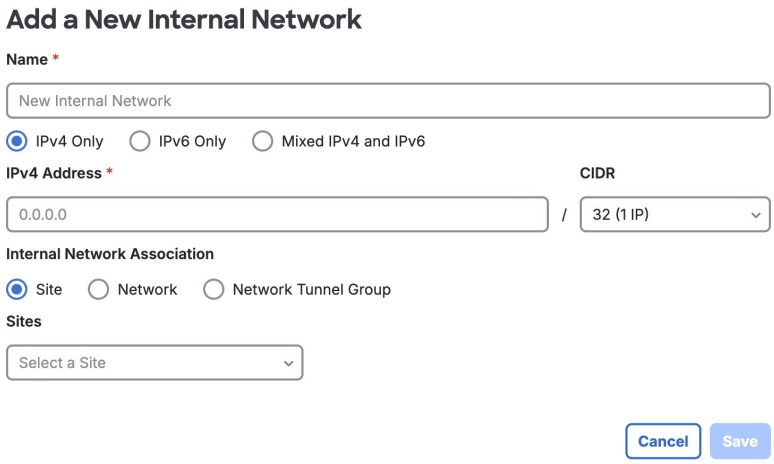
- Full Admin user role. For more information, see Manage Accounts.

Procedure

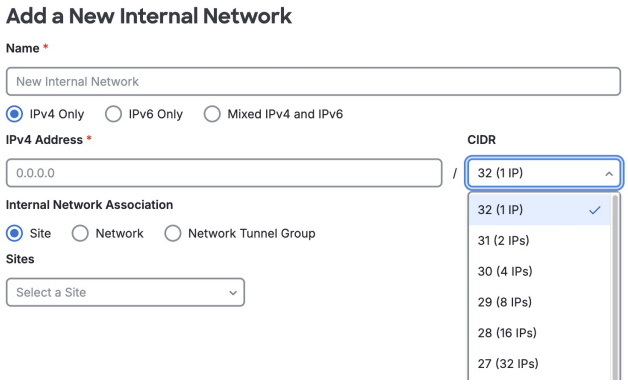
1. Navigate to **Resources** > **Internal Networks** and click **Add**.



2. For **Name**, enter a descriptive name for the internal network.

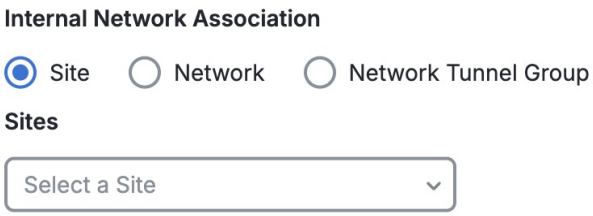


3. For **IPv4 Address**, enter an IPv4 address and choose a range.

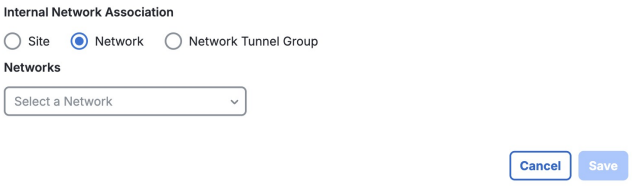


4. For **Internal Network Association**, choose **Site**, **Network**, or **Network Tunnel Group**.

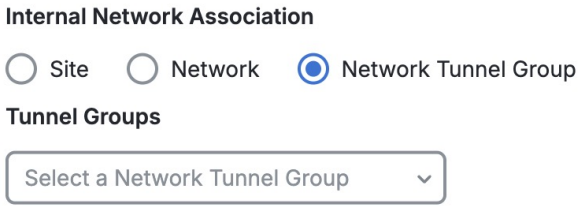
   a. Expand **Sites**, and then select the Site to associate with the Internal Network.



   b. Expand **Networks**, and then select the Network resources to associate with the Internal Network resource.



   c. Expand **Network Tunnel Group**, and then select the Network Tunnel Groups to associate with the Internal Network resource.



Update an Internal Network Resource

Provides instructions for completing the Update an Internal Network Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

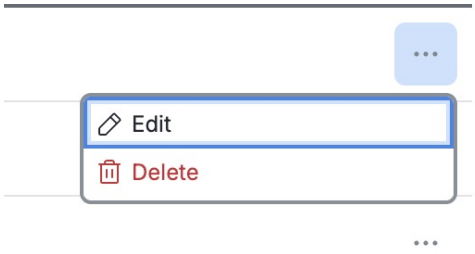
Once you add an Internal Network resource in Cisco Secure Access, you can edit the internal network's name, and IP address and address range.

Before you begin

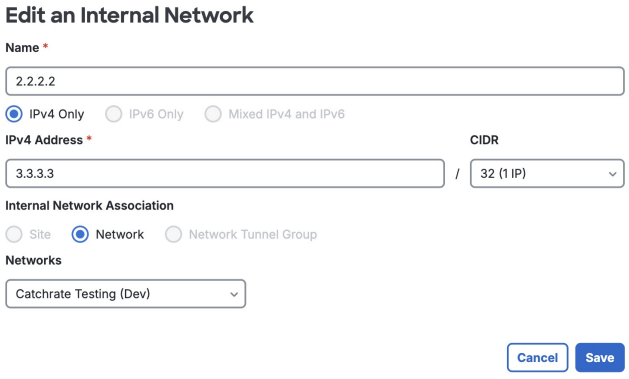
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internal Networks**.
2. Navigate to an Internal Network resource, click the ellipsis (**...**), and then choose **Edit** to update the Internal Network resource.



3. For **Name**, modify the name of the Internal Network resource.
4. Update the IP address and address range.
   a. For **IPv4 Address**, update the IPv4 address and choose the IP address range.



b. For **IPv6 Address**, update the IPv6 address and choose the IP address range.

5. Click **Save**.

Delete an Internal Network Resource

Describes Delete an Internal Network Resource in Cisco Secure Access. Once you add an Internal Network resource in Cisco Secure Access, you can remove the resource from your Secure Access organization.

Once you add an Internal Network resource in Cisco Secure Access, you can remove the resource from your Secure Access organization. Then, the deleted Internal Network resource is not available to select on your access rules and the internal network is not protected by Secure Access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Manage Sites

Sites are separate unique locations or private networks, which do not have a direct connection to your other locations or networks. You can configure a site for each deployed virtual appliance in Secure Access.

A Cisco Secure Access Site is a resource that you can associate with the Internal Networks in your organization.

You can add a Site for a deployed Secure Access Virtual Appliance (VA) in Secure Access. Once you add a Site, add an Internal Network in Secure Access and associate the Internal Network's private IP address with the Site.

Prerequisites for Sites

You must have at least one VA deployed in your environment to add a Site in Secure Access.

How to Add and Associate Sites in Secure Access

Sites refer to separate unique locations or private networks, which do not have a direct connection to your other locations or networks.

1. First, deploy a Virtual Appliance with Secure Access.
   - For more information, see Get Started with Virtual Appliances.
2. Add Sites for the Virtual Appliances deployed in the organization.
   - For more information, see Manage Site for Virtual Appliance.

     You can manage the Site for an integrated AD deployment. For more information, see Manage AD Components.
3. Then, add an Internal Network and select the Site to associate with the private network or subnet.
   - For more information, see Manage Internal Networks.
4. Select the configured Site in your internet access rules. For more information, see Components for Internet Access Rules.

Part II

Core Platform Administration

Topics:

- Accounts
- Network Infrastructure
- Network Tunnels by Device
- DNS and DDNS Servers
- Resource Connectors and Connector Groups
- Roaming Devices
- Private Resources
- Connections to Private Destinations
- Network and Service Objects
- Manage API Keys

Adminstering daily operations, managing roles and permissions, and configuring core platform features.

8 Accounts

Topics:

- Accounts Overview
- Hide sources with de-identification

Provides an overview of Accounts in Cisco Secure Access, including Accounts Overview and Hide Sources with De-identification. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Provides an overview of Accounts in Cisco Secure Access

Accounts Overview

Understand how to manage accounts in Secure Access.

You can share access to Cisco Secure Access with other people in your organization by inviting them to create an account.

You can manage accounts by navigating to **Admin** > **Accounts**. At a glance, you can see all of the accounts that have access to Secure Access, including their name, assigned role, whether they have two-factor authentication enabled, and their account status.

When you create an account for another administrator, you assign a role that defines what type of access they have to Secure Access. You can allow multiple users to view Secure Access while restricting the ability to make changes to a select few administrators.

Add a New Account

Provides instructions for completing the Add a New Account workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

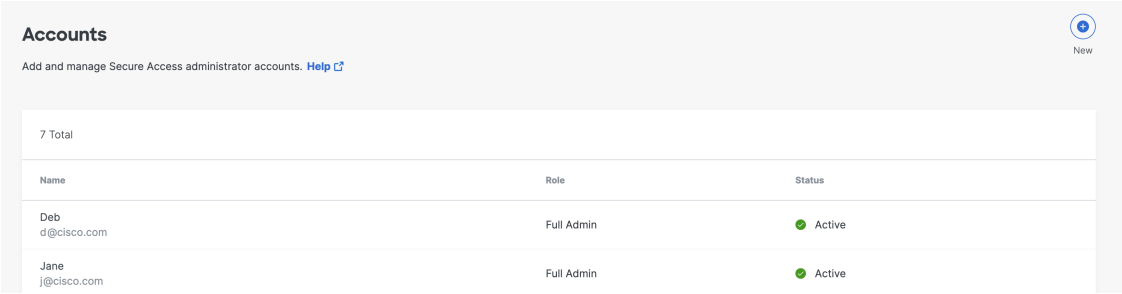
You can add users to your instance of Cisco Secure Access by adding a new account. Each account is assigned a role that sets that account's permissions to view, write, change, and delete Secure Access configurations.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

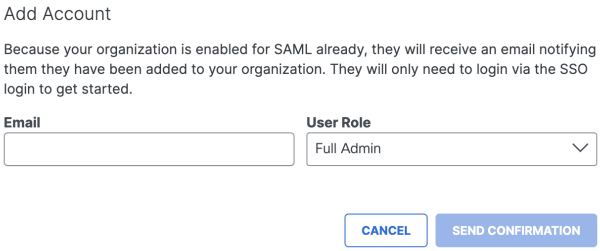
1. Navigate to **Admin** > **Accounts** and click **New**.



2. Enter the user's email address, choose a **User Role**, and then click **Send Confirmation**.

   User roles are:

   - **Full Admin**–Grants full access to Secure Access. This includes the ability to add users and assign roles.
   - **Read-Only**–Grants limited access to Secure Access. A Read-Only administrator can only view pages and reports. Functionality, including buttons, may not be displayed or available.
   - **Security Administrator**–Grants the same access as the **Full Admin** role, but does not have access to Data Loss Prevention (DLP) classifications, DLP policies, or the DLP Report.

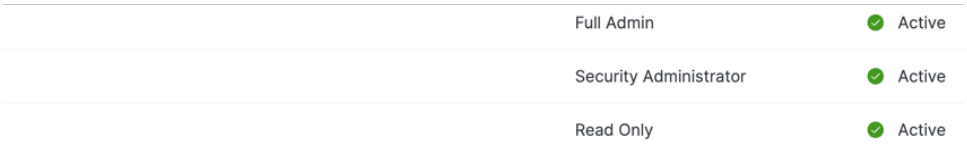


Secure Access sends a message to the new user's email address with instructions for setting a password.

> **Note**
>
> When the new user clicks **Confirm Invite**, Secure Access redirects them to the Secure Access login page.

After a user creates a password and signs in, the user has access to your instance of Secure Access. The user's role controls their level of access.

Once the account is added, its status is **Active** and you can edit the account. For more information, see Edit Account Settings.



Edit Account Settings

Provides instructions for completing the Edit Account Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

With administrator rights, you can change an account's settings at any time.

Before you begin

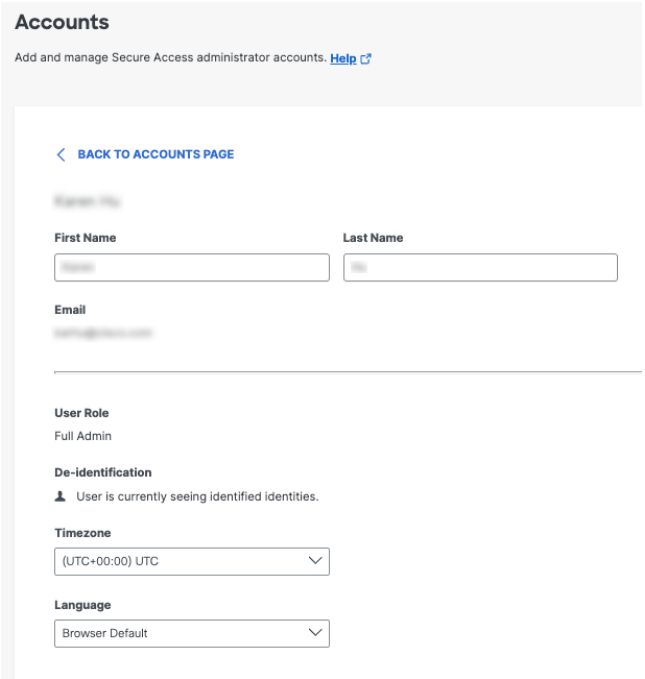
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Accounts** and click a listed account entry.



2. Update the settings on the user account.



- **First Name and Last Name**–The first name and last name of the user.
- **User Role**–The user role of the account. Only accounts that have the role of Full Admin can change user roles.
- **Timezone**–The timezone used in activity and reporting data shown within the dashboard. The timezone selection is unique to each account.
- **Language**– The language used for all text within the dashboard.
  - **You can only edit your own language setting.**
  - By default, your browser's language setting is used
  - The language selection is unique to each account
  - Product names will continue to appear in English, and new features will be in English for approximately one to two weeks
  - Language drop-down list includes Browser Default, English, and Japanese
- **Remove Account**–Delete the user account from Secure Access.

Delete an Account

Provides instructions for completing the Delete an Account workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

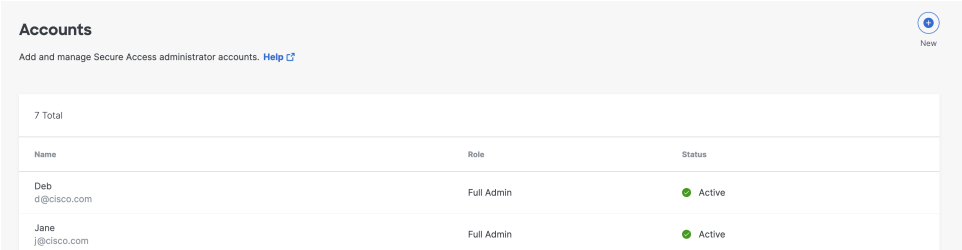
After adding a user to your instance of Secure Access, you can delete their account at any time. For information on how to add an account, see Add a New Account.

Before you begin

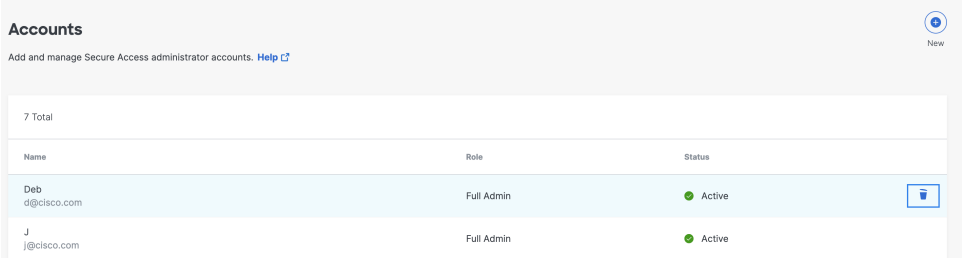
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Accounts**.



2. Hover over the account that you want to delete and then click the delete icon next to the account.



Hide sources with de-identification

De-identification helps protect user privacy by hiding source identities in Cisco Secure Access reports and activity data. When you enable de-identification, you can investigate security activity without unnecessarily exposing personally identifiable source details.

Some regions or organizations require restrictions to hide the sources of users making internet requests. To comply with these restrictions, you can hide source names when generating a report by enabling de-identification for a user. When enabled, a hash unique to that source replaces the source (identity) name.

Identity	Internal IP
fd90b6d53d205d60051946cca54995b6354a7a67	
465dae55fdc826ae81b8a3c1cb4d4bc7a80dc9d7	
b2d1f9c5524d5ad9c7125d9e1a1071d8e7fee6b2	3ac1e140a26b912baab0bc2fe5190d2de0229cc5
c76acef928dbf1c74b8705ac95ff899c4dae04a0	eea0b58f1ceec612d3f6e2b3973a0e48cd3f44e6
c76acef928dbf1c74b8705ac95ff899c4dae04a0	eea0b58f1ceec612d3f6e2b3973a0e48cd3f44e6
465dae55fdc826ae81b8a3c1cb4d4bc7a80dc9d7	

Note

You cannot enable or disable de-identification on your own account. At least two administrators are required to use this feature and any administrator can turn it on or off for another account.

Source Types

The following source types are de-identified in Secure Access:

- AD usernames
- computer/hostnames
- internal IP addresses
- Chromebook identities
- mobile identities
- GSuite users and groups
- SAML-obtained users and groups
- internal IP addresses

Limitations

Because the purpose of de-identification is to remove the visibility of the identity names for the user, de-identification includes the following limitations:

- The scheduling and exporting of reports is unavailable.
- The Application Discovery report is unavailable.
- You cannot search by an active directory username, roaming computer name, or internal IP name.

  However, you can click the hash name to view the source's (identity) details.
- There is no access to API key management and creation.
- There is no access to S3 Log Management (self-managed or Cisco-managed).
- Full administrators with the De-identification option enabled will see encoded information in all reports except for the Data Loss Prevention Report.

Enable De-identification

Provides instructions for completing the Enable De-identification workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Enable the De-identification option in Secure Access.

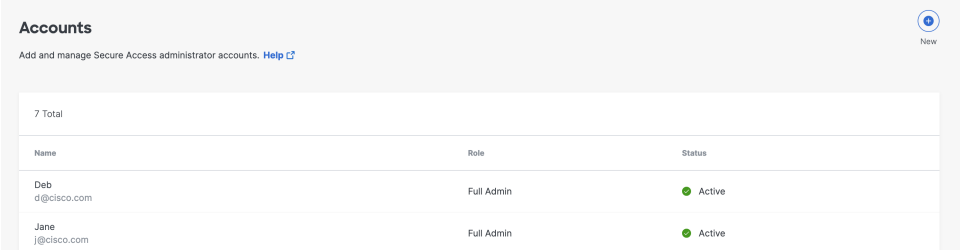
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

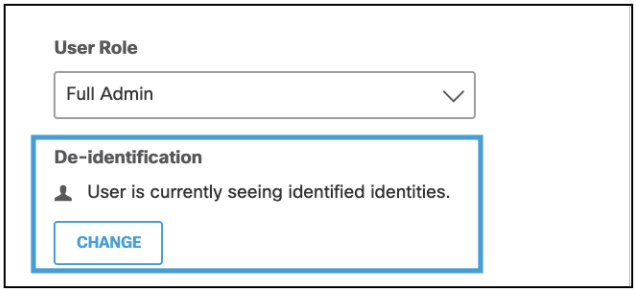
Procedure

1. Navigate to **Admin** > **Accounts** and click an account name.

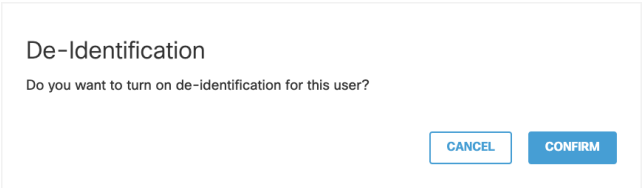
> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



De-identification is enabled and source (identity) names are replaced with a hash.

Disable De-identification

Provides instructions for completing the Disable De-identification workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Disable the De-identification option in Secure Access.

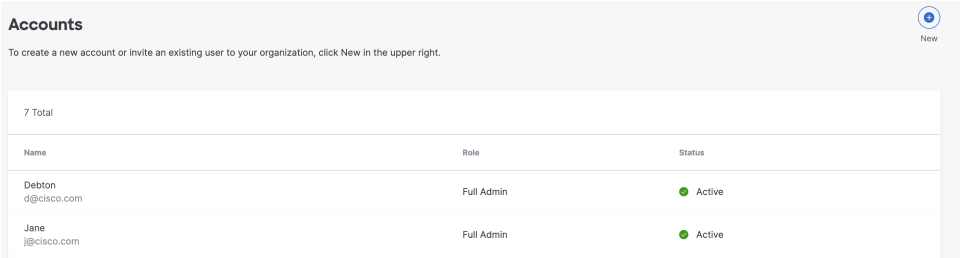
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

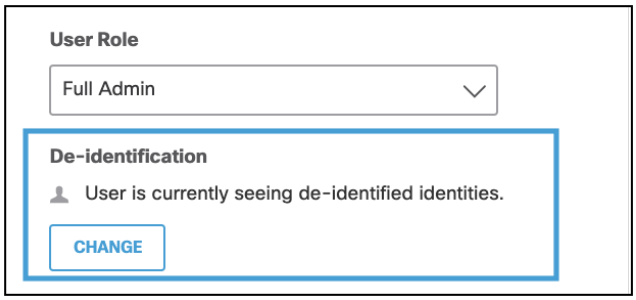
Procedure

1. Navigate to **Admin** > **Accounts** and click an account name.

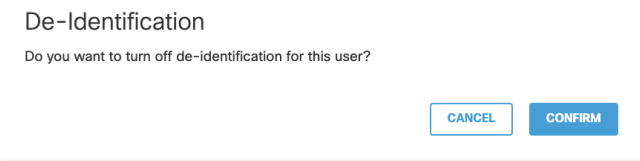
> **Note**
>
> You cannot enable de-identification for your own account.



2. Under **De-identification** click **Change**.



3. Click **Confirm**.



De-identification is disabled and the account can view identity names.

9 Network Infrastructure

Topics:

- Manage Network Devices
- Secure Access NAT as a Service
- Network Connections
- Network Tunnel Groups
- Routing Options and Guidelines for Network Tunnel Groups

Provides an overview of Network Infrastructure in Cisco Secure Access, including Manage Network Devices, Secure Access NAT as a Service, and Network Connections. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Network Devices

Describes Manage Network Devices in Cisco Secure Access. In Cisco Secure Access, you can add a hardware or virtual network device—for example, a router, switch, access point, or firewall—that routes DNS traffic to Secure Access's recursive DNS servers.

In Cisco Secure Access, you can add a hardware or virtual network device—for example, a router, switch, access point, or firewall—that routes DNS traffic to Secure Access's recursive DNS servers. Some network devices may also:

- Encrypt DNS traffic.
- Add internal IP addresses to DNS requests.
- Enable a policy for traffic by network segment or service set identifier (SSID).

After you add the network device in Secure Access, you can select the network device as a source component on the internet access rules in the Access policy. For more information, see Add an Internet Access Rule. You can also view the properties of a network device, and edit or remove the device in Secure Access.

> **Note**
>
> You can only deploy a network device when the device is on-network. You may deploy a network device as an alternative to a Secure Access Virtual Appliance (VA).

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Add the network device in Secure Access. For more information, see How to Add a Network Device in Secure Access.

How to Add a Network Device in Secure Access

Provides instructions for completing the How to Add a Network Device in Secure Access workflow in Cisco Secure Access. Create a Secure Access API key with the Deployments Network Devices key scope.

Procedure

1. Create a Secure Access API key with the **Deployments** > **Network Devices** key scope. For more information, see Manage API Keys.
2. Before you register the network device in Secure Access, add your username and password or Secure Access Network Devices API key and secret to the device.
3. On the device, use the Cisco Secure Access Network Devices API to add the network device in Secure Access. For more information, see Secure Access Network Devices API.

Procedure for Managing Network Devices

Describes Procedure for Managing Network Devices in Cisco Secure Access. After you add a network device in Secure Access, you can view the properties of the device and edit or remove the device.

After you add a network device in Secure Access, you can view the properties of the device and edit or remove the device.

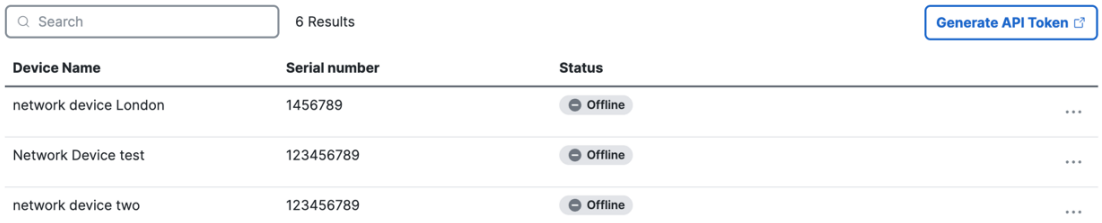
- View the Network Devices in Secure Access
- Edit a Network Device
- Remove a Network Device

View the Network Devices in Secure Access

Provides instructions for completing the View the Network Devices in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device. The properties of the network device are:
   - **Device Name**–The name of the network device.
   - **Serial number**–The serial number of the network device.
   - **Status**–The status of the network device: **Online** or **Offline**.

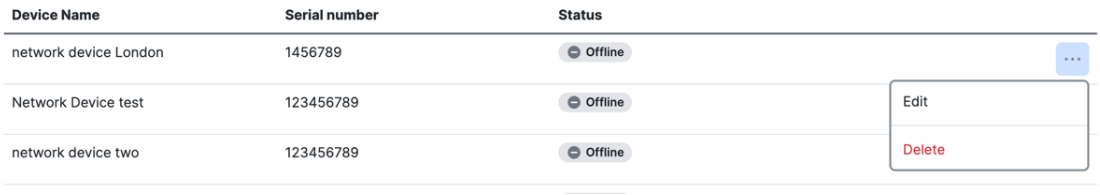


Edit a Network Device

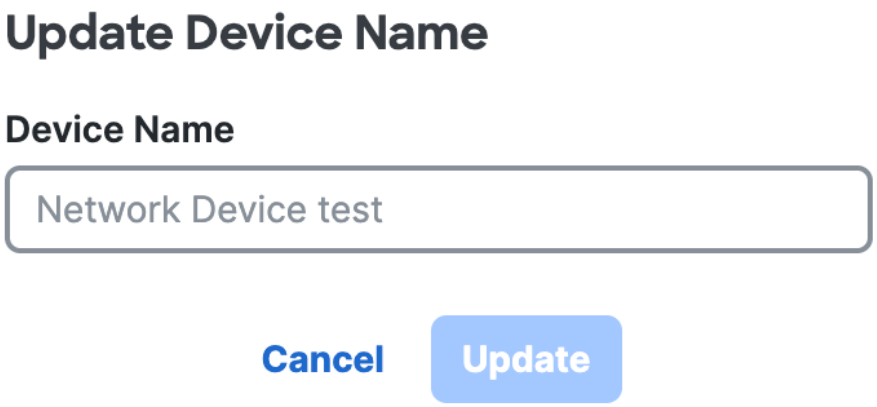
Provides instructions for completing the Edit a Network Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device, click on the ellipsis (**...**), and then choose **Edit**.



3. For **Device Name**, enter a descriptive name for the network device. The device's name must be unique for all network devices in the organization.



4. Click **Update**.

Remove a Network Device

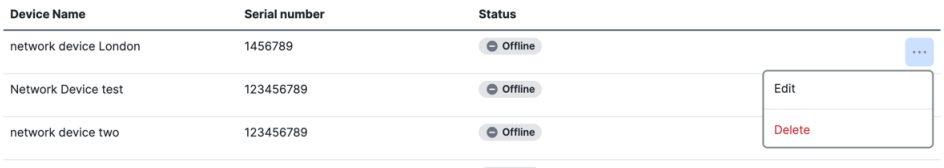
Provides instructions for completing the Remove a Network Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Deleting a network device in Secure Access does not prevent the device from sending traffic to Secure Access. To remove a network device fully, remove the authentication (username and password or API token) from the device first. If you are decommissioning the device, take the device offline. Otherwise, even if it is deleted in Secure Access, the device reappears when the network device sends additional traffic.

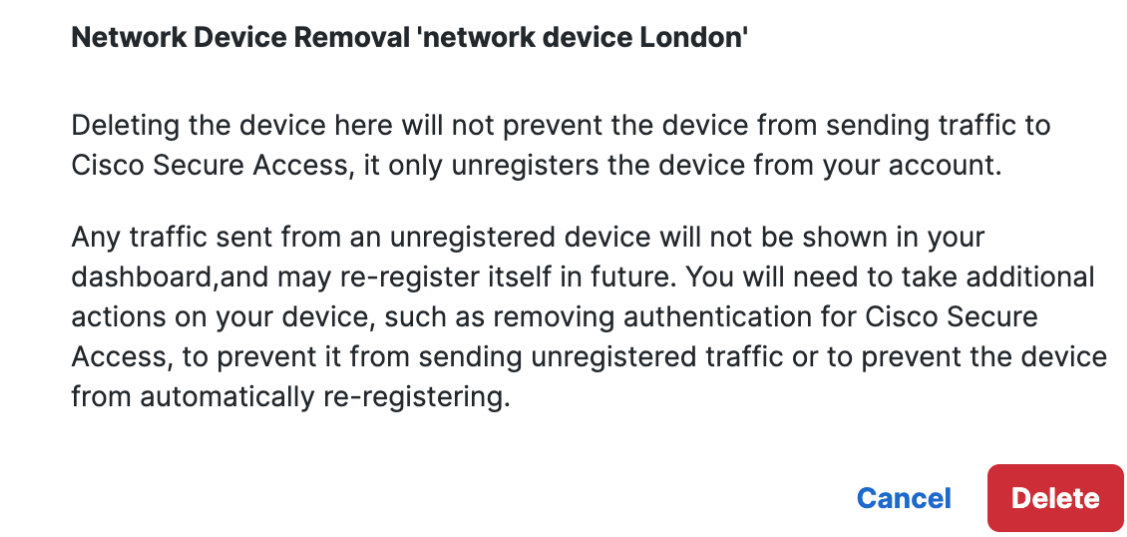
Procedure

---

1. Navigate to **Resources** > **Network Devices**.
2. Navigate to a network device, click on the ellipsis (**...**), and then choose **Delete**.



3. Click **Delete** to confirm the removal of the network device.



Secure Access NAT as a Service

Secure Access NAT as a Services (NATaaS) provides secure, efficient connections to internet destinations through assignments of public IP addresses to internet-bound traffic.

Secure Access secure web gateway (SWG) traffic that is bound for internet destinations takes the Secure Access NAT as a Service (NATaaS) as its egress point. NATaaS provides secure, efficient connections to internet destinations. NATaaS assigns public IP addresses to internet-bound traffic from a shared pool of IPv4 and IPv6 addresses, or from a single IPv4 address reserved for each geographic region where your Secure Access organization is deployed.

For more information on reserving your IPv4 address, see Reserved IP.

Web Traffic and NATaaS

Describes Web Traffic and NATaaS in Cisco Secure Access. An IP address available from the NATaaS enables you to register your traffic for allow lists maintained by internet sites and services.

An IP address available from the NATaaS enables you to register your traffic for allow lists maintained by internet sites and services. An IP address available from the NATaaS affects only the source IP for your internet-bound traffic. It does not affect the IP address that you use to establish the IPsec tunnel between your network and Secure Access.

The NATaaS will use an IP address from the shared ranges below. If you connect to websites or SaaS applications that implement IP allow-listing, provide these IP address ranges. If you require a dedicated IP address, see Reserved IP.

For more information, see Network Requirements for Secure Access.

IPv4 Shared Ranges

Public IP web traffic through the Secure Web Gateway egresses from NATaaS. Secure Access can use IPv4 addresses from the following shared egress ranges:

- 151.186.0.0/16
- 163.129.128.0/17
- 9.240.0.0/15

Where access to a destination is restricted by source IP address, ensure that the applicable allow list includes all three ranges. Cisco can introduce addresses from these ranges in new or existing Secure Access regions.

IPv6 Shared Ranges

- 2603:5004::/32

Machine-readable Cisco SSE egress IP geolocation feed

For automated consumers that need the current coarse geographic location of deployed Cisco Secure Service Edge (SSE) egress IP prefixes, use Cisco's RFC 8805 geolocation feed for SSE: https://geofeed.network.strln.net/. The feed includes deployed egress prefixes for Cisco SSE products, including Secure Access and Umbrella.

The feed maps deployed prefix locations and can change as capacity is added or moved. It does not define product allow-list ranges, Secure Access region availability, traffic type, or Reserved IP assignments.

Non-Web Traffic and NATaaS

Describes Non-Web Traffic and NATaaS in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Public IP non-web traffic egresses from NATaaS. Secure Access can use IPv4 addresses from the following shared egress ranges:

- 151.186.0.0/16
- 163.129.128.0/17
- 9.240.0.0/15

Where access to a destination is restricted by source IP address, ensure that the applicable allow list includes all three ranges. Cisco can introduce addresses from these ranges in new or existing Secure Access regions.

Best Practices for NATaaS

Describes Best Practices for NATaaS in Cisco Secure Access. You cannot combine the NATaaS IP address range (151.186.176.0/20) with the Secure Access IP address range (151.186.192.0/20) into a larger /19 range.

- You cannot combine the NATaaS IP address range (**151.186.176.0/20**) with the Secure Access IP address range (**151.186.192.0/20**) into a larger **/19** range. One range is at the end of the larger first block and the other range is at the beginning of the larger second block.

Reserved IP Addresses

Describes Reserved IP Addresses in Cisco Secure Access. A reserved IP address is a single-tenant public IP address deployed on Cisco Secure Access.

A reserved IP address is a single-tenant public IP address deployed on Cisco Secure Access. The reserved IP maps to a unique source IP address for your organization's web traffic and is not shared with any other Secure Access instance. Secure Access NAT as a Service (NATaaS) manages the web traffic egressing from the secure web gateway on your reserved IP.

For more information, see Deployment of the Reserved IP.

Network Requirements for Reserved IPs

Describes Network Requirements for Reserved IPs in Cisco Secure Access. For Reserved IP, Secure Access designates an IPv4 address only for your organization's web traffic from the secure web gateway.

For Reserved IP, Secure Access designates an IPv4 address only for your organization's web traffic from the secure web gateway. For more information about the Secure Access IP address range for web traffic, see Secure Access NAT as a Service.

Destination IP allow lists

For each newly assigned Reserved IP, add the exact `/32` to every applicable destination allow list before Cisco activates it. Do not assume that the new address will be in the same `/24` as the shared egress IP previously allowed by that destination or in one of the older shared `/20` ranges. An address assigned from the `151.186.0.0/16` expansion remains within that `/16`. Existing Reserved IP assignments are not renumbered.

Best Practices for Reserved IPs

Describes Best Practices for Reserved IPs in Cisco Secure Access. To ensure that your organization's network traffic reaches the data center where Secure Access provisioned the reserved IP, we recommend that you use the Secure Access DNS servers.

To ensure that your organization's network traffic reaches the data center where Secure Access provisioned the reserved IP, we recommend that you use the Secure Access DNS servers.

Set up your organization's DNS to resolve queries to the Secure Access DNS servers. For information about the Secure Access DNS servers, see Secure Access DNS Resolvers.

- To get help with setting up the Secure Access DNS servers on your network, contact Cisco Support. For more information, see https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.
- If you cannot use the Secure Access DNS servers on your network, contact Cisco Support to enable the provisioning of Reserved IP with your organization's DNS.

Known Limitations of Reserved IPs

Describes Known Limitations of Reserved IPs in Cisco Secure Access. Secure Access has known limitations for the use of Reserved IP.

Secure Access has known limitations for the use of Reserved IP.

IPv6

IPv6 addresses are not supported by Reserved IP. Traffic from sources that use IPv6 will be assigned public addresses from the Secure Access NATaaS shared IPv6 ranges.

Remote Browser Isolation

Remote Browser Isolation (RBI) is not supported by Reserved IP. Applications or services that require a reserved IP address should not use remote browser isolation.

Reserved IP Surrender

When an organization surrenders one or more reserved IPs back to Cisco, the reserved IPs become available to other organizations for provisioning. Reserved IP addresses are not transferable from one AWS region to another. For more information, see Reserved IP Supplemental Terms.

Port Exhaustion

Port exhaustion is unlikely to occur. However, if port exhaustion does occur, the session is dropped and the client on the user device retries the connection.

Deployment of the Reserved IP

Describes the deployment process and key considerations for reserved IP addresses in Cisco Secure Access, including ordering requirements, usage limitations, recommended sizing per user and traffic volume, and region-specific limits.

> **Note**
>
> Before Cisco can assign the reserved IP address to your organization, you must contact your Cisco partner or sales representative and order your reserved IP address.

- Reserved IP is available only for web traffic protected by the Secure Access secure web gateway.
- Reserved IP is available only for IPv4.
- We recommend one reserved IP per every 5,000 to 10,000 users per region (or about 8 Gbps of traffic). High availability is built-in.
- Each region supports a maximum of 20 reserved IPs per organization (approximately 200,000 users or 160 Gbps of traffic).
- Reserved IP is not supported for the Intelligent Proxy traffic.
- Secure Access does not support reserving contiguous IP addresses.
- Once Secure Access deploys the reserved IP for your organization, any web traffic that is forwarded to the provisioned cloud provider region uses the reserved IP for all web traffic.

For more information, refer to Secure Access Regions.

Reporting and Reserved IP

Describes Reporting and Reserved IP in Cisco Secure Access. The Activity Search report has two filters associated with Reserved IP.

The Activity Search report has two filters associated with Reserved IP.

- **Egress IP Type**–The egress IPv4 type, choose either **Shared** or **Reserved**.
- **Egress Data Center**–The list of available Secure Access data centers.

To filter by **Egress IP Address**, use the **IP Address** filter field. For more information, see Advanced Search.

Calculate Your Maximum Sessions

Describes Calculate Your Maximum Sessions in Cisco Secure Access and explains Example. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Determine the maximum sessions available in a Secure Access instance.

This formula illustrates the way in which Reserved IP maps sessions to a single reserved IP.

```
sIP x sP x dIP x dP x nP
```

- **sIP (Source IP)**– A single source IPv4 address. For example, use a value of `1`. Secure Access supports more than one source IPv4 address at a time. The source IPv4 address is the egress IP from your organization's premises or from a roaming user device.
- **sP (Source Ports)**–We do not restrict source ports. Use the value of `65536` for the full port range of 65,536 potential source ports.
- **dIP (Destination IPs)**–The total number of destination IPs, which clients can use to establish a session. To determine the greatest number of sessions supported, use the total possible number of public IPv4 addresses

3,706,452,992. To determine the fewest number of sessions supported, use 1. A value of `1` emulates a fully qualified domain name (FQDN) that only supports a single IP address. All clients establish a session with the same FQDN.

- **dP (Destination Ports)**–We do not restrict ports. Use the value of `65536` for the full port range of 65,536 destination ports.
- **nP (Number of Protocols)**–Secure Access only supports TCP. Use a value of `1` for TCP.

Example

```
1 x 65536 x 1 x 65536 x 1 = 4294967296
```

Troubleshooting Reserved IPs

Describes Troubleshooting Reserved IPs in Cisco Secure Access. If the network traffic for the organization is not using the reserved IP that Secure Access assigned to your organization, we recommend that you review your Secure Access deployments, configuration settings, and policy rules.

If the network traffic for the organization is not using the reserved IP that Secure Access assigned to your organization, we recommend that you review your Secure Access deployments, configuration settings, and policy rules.

- Ensure that destinations are not added in policy rules where you enabled remote browser isolation (RBI).
- Ensure that destinations are available on HTTP/TCP port 80 or HTTPS/TCP 443.

> **Note**
>
> Secure Access does not provide reserved IPs for web sites that load over QUIC.

- Ensure that web traffic on the reserved IP appears in the Activity Search report, and that the traffic egresses through the region of data centers where Secure Access provisioned the organization's reserved IP.
  - Some 'find my IP' sites read the original IP in the proxy's HTTP X-Forwarded-For (XFF) header and show that IP instead of the organization's reserved IP. We recommend that you use the Activity Search report to verify that the network traffic is using the organization's reserved IP.
- Be aware that Secure Access excludes Microsoft Update traffic on the organization's reserved IP.
- Ensure that the organization's network connects to the region of data centers where Secure Access provisioned the reserved IP.

Reserved IP Supplemental Terms

Describes Reserved IP Supplemental Terms in Cisco Secure Access and explains Cisco Secure Access Reserved IP Supplemental Terms, 1. Scope of Use of Reserved IP, and 2. Third Party Notifications. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Secure Access Reserved IP Supplemental Terms

Effective January 31, 2024

1. Scope of Use of Reserved IP

1.1. The Cisco Secure Access Reserved IP Service provides the applicable end customer (each a “Customer”) with one or more public, static Internet Protocol (IP) address/es based on purchased quantity, assigned to Customer (each a “Reserved IP”). Customer is authorized to use a Reserved IP assigned to it solely with its Secure Access subscription

during the term of Customer's subscription. Customer's right to use a Reserved IP assigned to it shall immediately cease upon the earlier of (i) expiration or termination of Customer's Secure Access subscription, (ii) Customer's surrender of the Reserved IP back to Cisco, or (iii) the date such Reserved IP is reclaimed by Cisco as described below.

1.2. Reserved IPs are designated for use with a specific cloud provider region provided for Cisco Secure Access and is not portable to another region. Customer web traffic configured to forward to the applicable region will egress through the Reserved IP assigned to that region while web traffic not configured to forward to the applicable region will egress through a shared IP.

1.3. If a Customer's Reserved IP is associated with a country other than the country where such Customer's traffic originates, the Customer may request that the Reserved IP be updated in Cisco's geofeed. In such case, Cisco will use commercially reasonable efforts to update its geofeed to associate the Reserved IP with the country where the Customer's traffic originates. Cisco cannot guarantee that third parties will honor the Cisco geofeed designation.

2. Third Party Notifications

If Customer registers the Reserved IP with any third-party site, Customer is solely responsible for notifying all such third parties immediately upon expiration, termination, surrender, or reclamation of its right to use the Reserved IP. Customer acknowledges that the Reserved IP will be assigned to another customer and Customer assumes the risks associated with its failure to notify the applicable third parties that such Reserved IP is no longer in use by Customer.

3. Ownership; Right to Reclaim

3.1 Public static IP addresses are a limited resource. Cisco reserves the right to cap the number of Reserved IPs per Customer. Cisco owns the Reserved IP, and Customer does not own nor have any property interest in the Reserved IP. As stated above, Customer's right to use the Reserved IP expires on expiration or termination of Customer's Secure Access subscription, upon Customer's surrender of the Reserved IP to Cisco, or upon Cisco reclaiming a Reserved IP as contemplated below.

3.2 Cisco shall have an unrestricted right with thirty (30) days advance written notice to Customer to reclaim any Reserved IP (other than Customer's designated failover Reserved IP) during the Customer's subscription if its usage is less than 5% of Customer's aggregate secure web gateway (SWG) bandwidth usage during any year of Customer's subscription unless Customer provides reasonable evidence to Cisco of its use or planned use of such Reserved IP within 15 days of Cisco's written notification. In the event Cisco reclaims a Reserved IP, Cisco will refund a prorated portion of the prepaid fee paid to Cisco for the Reserved IP for the remainder of the unexpired subscription term.

4. Right to Modify or Discontinue

Cisco reserves the right to modify or discontinue the provision of public, static IP addresses at any time with or without notice.

5. Compliance with Policies and Assistance

Customer must comply with all policies and procedures established by Cisco for the assignment and setup of all public static IP addresses. Cisco may modify such policies and procedures without notice. Customer shall provide any information and assistance as may be reasonably requested by Cisco related to the setup, maintenance, and termination of any public static IP addresses.

Network Connections

Understand the network connections that Secure Access supports to direct traffic to internet and private resources.

Cisco Secure Access supports multiple ways to direct traffic to internet and private resources. Depending on your deployment, you can configure either method or both methods.

- Use **network tunnel groups** to route traffic from remote users, on-premises users, and branch locations to the internet and to private destinations managed by your organization. Network tunnel groups also support branch-to-branch traffic.

- Use **resource connector groups** to provide Zero Trust Access connectivity between user devices and your organization's private resources.

For connections to configured private resources, Secure Access supports multiple ways to direct traffic from your users: Network Tunnel Groups and Resource Connector Groups. Both involve virtual machine instances deployed on your network.

For help choosing a connection method, see Comparison of Network Connection Methods.

For configuration tasks, refer to:

- Manage Network Tunnel Groups
- Manage Resource Connectors and Connector Groups

Comparison of Network Connection Methods

Describes Comparison of Network Connection Methods in Cisco Secure Access and explains If both methods are configured for the same private resource. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports two methods for directing user traffic to private destinations:

- **Resource Connectors** (deployed in connector groups)
- **Network Tunnels** (deployed in network tunnel groups)

Choose the method based on the traffic you need to route, the connection types you support, and your network design.

Feature	Resource Connectors	Network Tunnels
Traffic destination	Private resources only	Private resources and internet-bound traffic
Supported connection types	Zero Trust Access connections (client-based and browser-based)	VPN, branch-to-branch, and Zero Trust Access connections (client-based and browser-based)
Deployment model	Virtual machine instances deployed in groups	IPsec-capable network devices on supported virtual or hardware platforms
Connectivity requirement	Require only outbound connections from your network	Require devices that can initiate IPsec IKEv2 tunnels
Routing requirement	Additional routing configuration is typically not required	Network routing configuration is required
Overlapping IP ranges	Supported when the resource is defined and accessed by FQDN	See network tunnel documentation for your deployment design
Exposure model	Expose only specified private resources to Secure Access	Extend your network to the Secure Access cloud
Scaling model	Scale by deploying additional connectors in a group	Uses your existing tunnel-capable network infrastructure
Best fit	Private-resource access with Zero Trust Access	Broader traffic routing, including internet-bound and branch-to-branch traffic

If both methods are configured for the same private resource

If both a network tunnel group and a connector group with connectors are properly configured to support the same connection, a connector forwards Zero Trust Access traffic by default.

If all connectors in the connector group are unreachable, the network tunnel routes the traffic.

If the connector group is reachable but the request fails, traffic does not fall back to the tunnel and the connection fails.

For configuration tasks, refer to:

- Manage Network Tunnel Groups
- Manage Resource Connectors and Connector Groups

Network Tunnels in Secure Access

Describes Network Tunnels in Secure Access. Network tunnel groups use IPsec IKEv2 tunnels to connect your network to Secure Access data centers.

Network tunnel groups use IPsec IKEv2 tunnels to connect your network to Secure Access data centers.

Network devices that support IPsec IKEv2 can forward traffic through these tunnels to Secure Access. Use network tunnel groups when you need to route traffic to private resources, route internet-bound traffic, or support VPN, branch-to-branch, or Zero Trust Access connections.

For configuration details, refer to Manage Network Tunnel Groups.

Resource Connectors in Secure Access

Describes Resource Connectors in Secure Access. Resource connectors are virtual machine instances that you provision in Secure Access and deploy inside your network.

Resource connectors are virtual machine instances that you provision in Secure Access and deploy inside your network. You manage resource connectors in groups.

Use resource connector groups to provide Zero Trust Access connectivity between user devices and your organization's private resources.

Resource connectors require only outbound connections from your network and expose only the private resources that you define.

For configuration details, refer to Manage Resource Connectors and Connector Groups.

Network Tunnel Groups

Network tunnel groups organize IPsec tunnels from supported network devices so traffic can connect securely to Secure Access through shared regional hubs. They provide redundant, highly available tunnel connectivity by pairing tunnels with primary and secondary data center hubs that can be monitored and managed as a group.

Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access. Supported network devices capable of establishing an IPsec tunnel can join a network tunnel group.

- Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.
- Network devices that are capable of establishing IPsec tunnels forward traffic to one of the Secure Access data centers where the tunnel head end is located.
- User devices can read, write, and update private resources by setting up virtual private networks (VPNs) or zero trust access (ZTA) connections to Secure Access through these IPsec tunnels.

- A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the internet and private resources.

Provisioning high-availability network tunnel groups at a hub site allows a group of tunnels to share a primary and secondary hub. Each data center hub in a network tunnel group can connect to multiple tunnels. A hub configured for NAT can support up to 100 tunnels. A hub that is not configured for NAT is limited to 10 tunnels.

Failover for Branch Connections in Secure Access Data Centers

For high availability, customer branch devices must connect to both the primary and secondary hubs in Cisco Secure Access data centers. They must have tunnel auto-reconnect enabled on the branch device and have a failure detection mechanism like Dead Peer Detection (DPD), IP SLA, or BGP timeout, depending on their use case. If you configure only a primary tunnel, you will experience interruption of service during regular maintenance windows or unplanned outages.

Under normal conditions, traffic flows through the primary data center. If the primary data center fails, traffic routes through the secondary data center. Switchover time depends on the nature of the primary tunnel failure and various timers.

Primary traffic failover to secondary can occur instantaneously if the Secure Access or customer branch device initiates and successfully terminates the IKE tunnel or BGP session.

> **Note**
>
> Terminating the IKE tunnel also terminates BGP.

In cases of communication failure between the branch device and Secure Access, traffic switches to the secondary only under the following conditions:

- The Secure Access side DPD timeout occurs or the BGP hold timer expires.
- The customer's DPD timeout is not effective in this situation because it does not result in tunnel termination on the Secure Access side.
- The shorter of the Secure Access DPD timeout (156 seconds maximum; default and non-negotiable) and the BGP hold timer (90 seconds; default and negotiable) applies. For example, with a DPD timeout of 156 seconds and a BGP hold timer of 90 seconds, it takes at least 90 seconds for traffic to switch to the secondary tunnel.

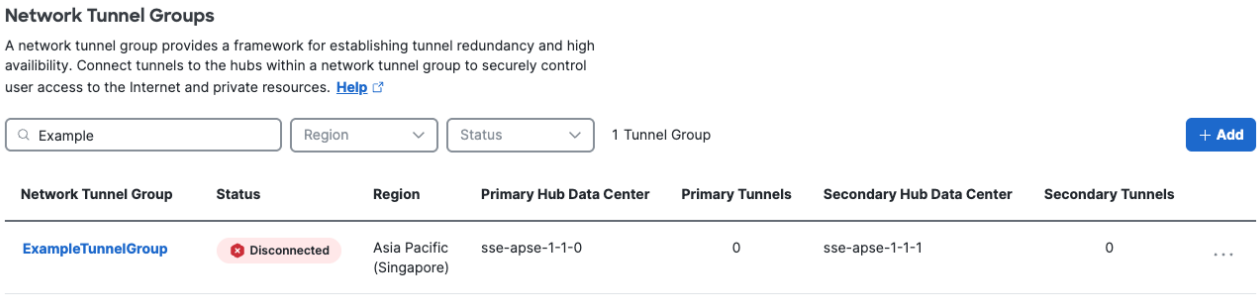
Recommendations

- Initiate a tunnel termination when a traffic failure is detected through the primary tunnel.
- If initiating a tunnel termination is not feasible, terminate the BGP session or wait for the BGP hold timer to expire.
- Configure the DPD timeout for your organization to match the Secure Access DPD timeout (156 seconds maximum). For example, 1 DPD every 30 seconds with 4 retransmits before failure: 30 seconds × 5 DPD = 150 seconds delay.

Add a Network Tunnel Group

Configure and deploy a network tunnel group in Secure Access to connect multiple IPsec tunnels from your branch network devices to primary and secondary Secure Access data center hubs for high-availability connectivity.

This task describes how to configure network tunnel groups in Cisco Secure Access to provide high availability and redundancy for IPsec tunnels connected to data center hubs.



Network tunnel groups enable high-availability connectivity by allowing multiple IPsec tunnels to share primary and secondary hub sites. Any network device capable of establishing an IPsec tunnel can join a network tunnel group using the credentials generated during deployment.

Note

Hub capacity depends on your Network Address Translation (NAT) configuration:

- **With NAT:** Supports up to 100 tunnels.
- **Without NAT:** Limited to 10 tunnels.

Regardless of your network device type, the setup process follows these three steps:

1. **Configure and deploy the tunnel group:** In Secure Access, define the tunnel group attributes and deploy the group. Upon deployment, the tunnel group status changes from Unestablished to Inactive.
2. **Configure tunnels on your network device:** Configure the primary and secondary tunnels on your network device to send traffic to Secure Access. Associate these tunnels with the deployed tunnel group using the required attributes, including the tunnel ID, tunnel passphrase, and the Secure Access data center IP address.
3. **Enable traffic flow and monitor status:** Once user devices are configured to connect through the tunnel, Secure Access logs the traffic and the tunnel status changes to Active. You can monitor the status of tunnel groups and individual tunnels, as well as view related events, on the Secure Access **Status** page, Secure Access Overview, and Activity Search.

Follow these detailed steps to add a network tunnel group in Secure Access.

Before you begin

Ensure that your account has the Full Admin role in Secure Access. For more information, refer to Manage Accounts.

If you select a region and Secure Access returns with two data centers within that region, you can only swap the primary and secondary data center of a high-availability environment if the two data centers are Cisco owned data centers. You should only switch to your backup region **if** your primary region is unavailable.

> **Note**
>
> You cannot swap the primary and secondary data center if there is at least one AWS data center configured as a region.

Procedure

Step 1 - General Settings

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. Click **Add**.
3. Enter the **General Settings** for your tunnel group:
   - **Tunnel Group Name**: Enter a meaningful name for the tunnel group.
   - **Region**: Select a Secure Access region from the dropdown list. Click "+ Backup region" to add a backup primary and secondary data center for failover purposes.

     > **Tip**
     >
     > When you select a region, Secure Access displays two data centers within that region for you to choose from with one automatically assigned as the primary data center for you. You can swap the primary status of a region by clicking the "**Make primary**" button located under the secondary region. This is applicable to both the active HA region and the backup regions.

   - **Device Type**: Choose the network device type from the dropdown list.
   - Click **Next**.

Step 2 - Tunnel ID and Passphrase–Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group. If you opted to configure a backup primary or secondary region, you must also enter the IP addresses for both data centers within that region.

4. Enter the **Tunnel ID**.
   - Tunnel ID may be an email address or a primary and secondary pair of IP addresses.
   - Tunnel ID format requirements vary based on the device type selected in **Step 1 - General Settings**:

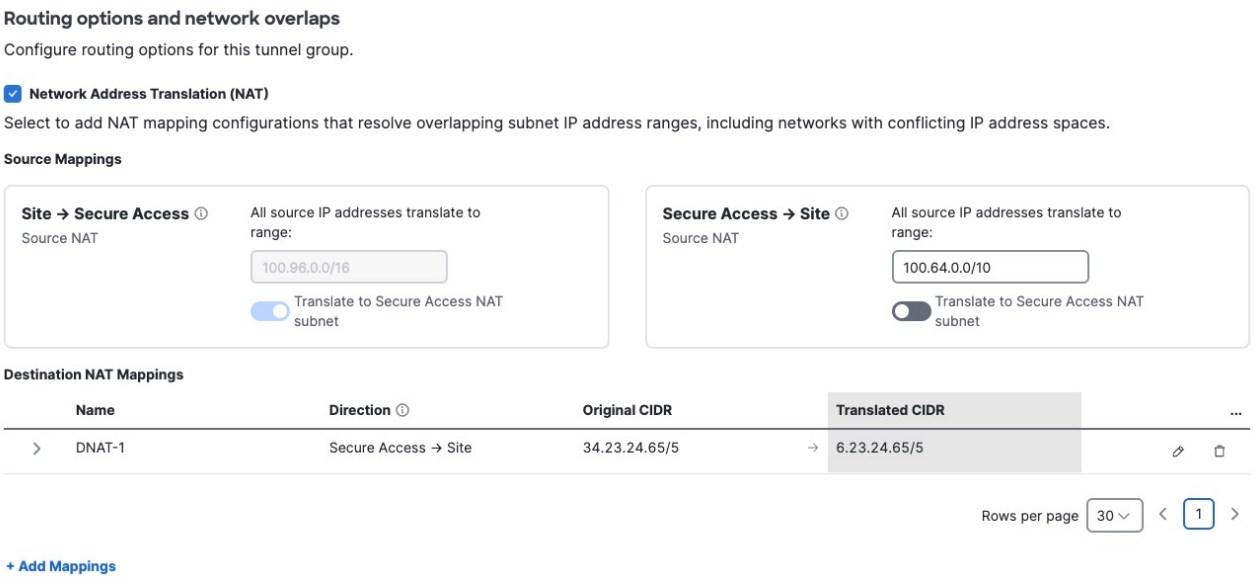
Device Type	Tunnel ID Format
Meraki MX	Email
Catalyst SDWAN	Email
ISR	Email
ASA	Email OR IP address (primary and secondary)
AWS	IP address (two each for primary and secondary)
AZURE	IP address (primary and secondary)
FTD	Email OR IP address (primary and secondary)
Other	Email OR IP address (primary and secondary)
VeloCloud	IP address (two each for primary and secondary)

- Email tunnel ID requires the format `<tunnel name>@<org><hub>.sse.cisco.com`. Use the name you assigned to the tunnel group in **Step 1 - General Settings**.
- IP address Tunnel IDs require both a primary and a secondary IP address.
- IP address Tunnel IDs support both IPv4 and IPv6.

5. Enter a tunnel **Passphrase** between 16 and 64 characters in length. The passphrase must contain at least one upper case letter, one lower case letter, and one number. The passphrase cannot include any special characters. Backup regions, if configured, use the same passphrase.
6. Reenter your passphrase to confirm.
7. Click **Next** to continue.

Step 3 - Routing – Configure routing options and network overlaps for this tunnel group.

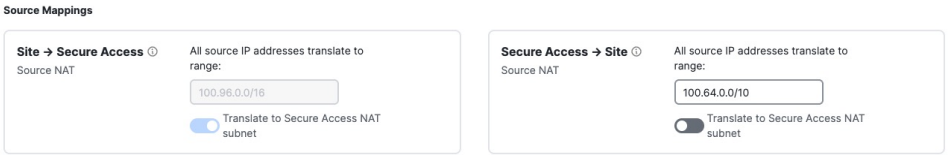
8. Select **Network Address Translation (NAT)** if the IP address space behind this tunnel group overlaps with other IP address spaces in your network. NAT mapping translates real IP prefixes to unique mapped prefixes to resolve address conflicts and enable routing between branch sites, partner networks, and cloud applications. For more information, see NAT Mapping for Network Tunnel Groups.



> **Note**
>
> ECMP is not supported by tunnels with NAT mappings. For more information, see Equal-Cost-Multi-Path (ECMP) Support.

> **Note**
>
> For clients at this site to communicate with private resources at other sites, you must route return traffic to addresses in the 100.64.0.0/10 range through Secure Access.

a) Check the box to enable NAT and reveal the **Source Mappings** and **Destination NAT Mappings** sections.
b) Review the **Source Mappings** tiles.

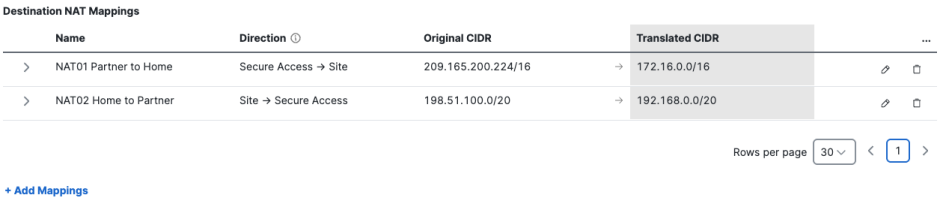


Source mapping tiles display the translation behavior for source IP addresses in each traffic direction.

- **Site → Secure Access** – Source addresses are automatically translated to the Secure Access NAT subnet. This mapping is not configurable. To request a change to the source translation pool, contact Cisco Support.
- **Secure Access → Site** – By default, source addresses are translated to the Secure Access NAT subnet. Override this default by enabling **Translate to Secure Access NAT subnet** and entering a custom IP prefix range. This mapping applies to all destination NAT mappings.

> **Note**
>
> When no destination mappings are configured, the **Secure Access → Site** source mapping has no effect. In this state, the NTG performs outbound-only NAT.

c) Configure **Destination NAT Mappings**.



Destination NAT mappings translate destination IP addresses for traffic between your network and external destinations. You can create up to 100 mappings per direction in each NTG.

Click + Add Mappings and configure the following fields:

- **Name** – Enter a name that clearly identifies the mapping.
- **Direction**:
  - **Secure Access → Site** – Translates destination IP addresses in the **Original CIDR** for inbound traffic to devices on your network. Sources send traffic to the **Translated CIDR** to reach destinations on your network.
  - **Site → Secure Access** – Translates destination IP addresses in the **Original CIDR** for outbound traffic from devices on your network. Devices send traffic to the **Translated CIDR** to reach cloud, branch, or partner destinations.
- **Original CIDR** – The untranslated IP address range.
- **Translated CIDR** – The translated IP address range.
- **Description** – (Optional) Additional context for the mapping. Limited to 200 characters.
- **Summary** – Displays a description of the translation in this format: `Traffic destined to [Original CIDR] is translated to [Translated CIDR] in a 1-1 NAT translation.`

d) Click the **checkmark** on the right side of the row to save the mapping.

Important

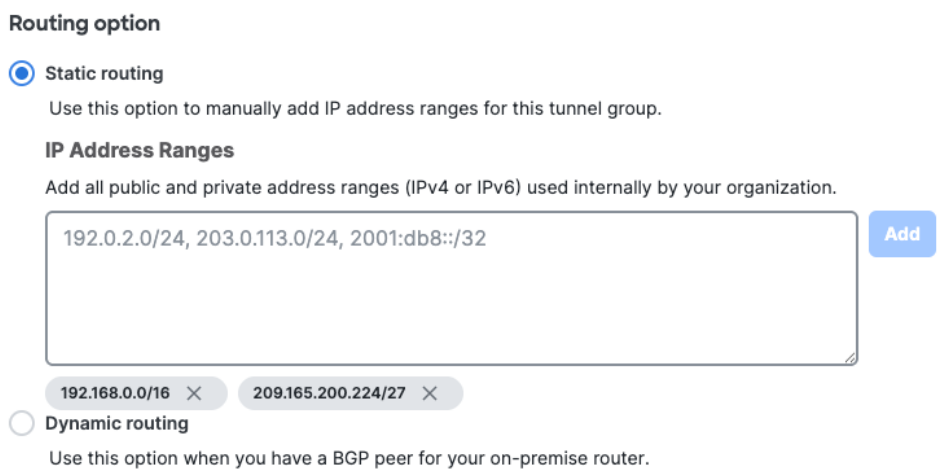
- NAT mappings in the **Site → Secure Access** direction support overlapping mapped IP addresses between NTGs.
- NAT mappings in the **Secure Access → Site** direction do not support overlapping mapped IP addresses between NTGs. Each NTG must use unique mapped IP address ranges to avoid routing errors.

> **Note**
>
> When configuring private resources and access rules for NAT-mapped destinations, use the **Translated CIDR** for **Secure Access → Site** mappings and the **Original CIDR** for **Site → Secure Access** mappings. For more information, see NAT Mapping for Network Tunnel Groups.

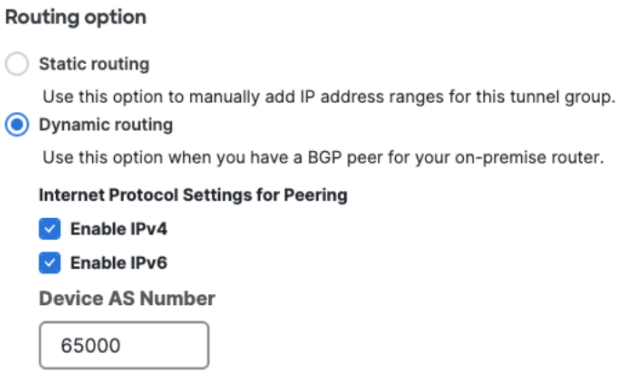
> **Note**
>
> Enabling NAT disables the static and dynamic routing options for the NTG.

9. **Internet Protocol Version Setting for Routing**: Choose whether to **Enable IPv6 Routing in addition to IPv4**.
10. Choose a **Routing option** for this network tunnel group.
    - Choose **Static routing** to manually add IPv4 and IPv6 address ranges for this tunnel group. You should add all public and private address ranges used internally by your organization. For more information, refer to Static Routing.

      > **Caution**
      >
      > Adding a default route in static routing is not supported and can lead to traffic disruptions.

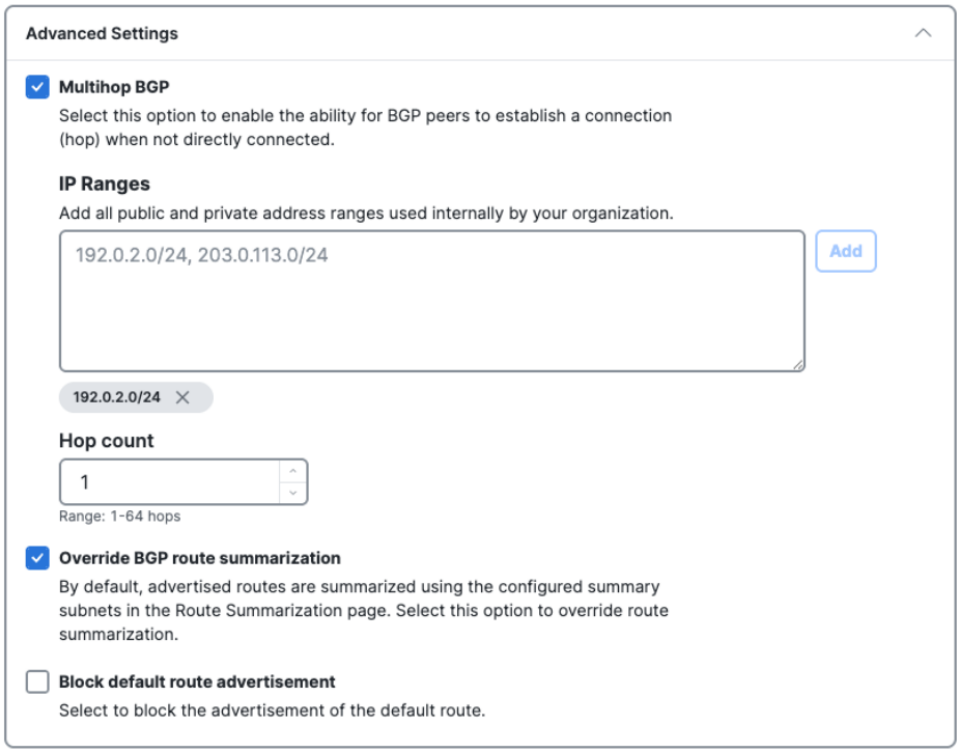
      

    - Choose **Dynamic routing** when you have a BGP peer for your on-premise router. Enter the router's autonomous system (AS) number. For more information, refer to Dynamic Routing with BGP.



- If IPv6 routing is enabled for **Internet Protocol Version Setting for Routing**, choose to enable IPv4, IPv6, or both internet protocol versions for peering. Then enter the router's AS number.

- Expand **Advanced Settings** for additional dynamic routing options.



  - **Multihop BGP** – Enables BGP peers to establish a connection when not directly connected.
    - Enter the **IP Ranges** from where BGP peering sessions will originate, then click **Add**
    - (Optional) Enter the **Hop count** to limit the number of hops over which the BGP multihop session is established. The hop count equates to the time to live (TTL) parameter. The range is 1 to 254 hops, with a default value of 1. The hop count is disabled until IP addresses are entered. For more information, refer BGP Next-Hop Configuration.
  - **Override BGP route summarization** – By default, advertised routes are summarized using the configured summary subnets on the **Route Summarization** page. Select this option to override route summarization for this NTG. For details, refer to Manage Summary Subnets.
  - **Multi-region backhaul** supports a customer backhaul network that spans multiple Secure Access regions. Enable this setting for each network tunnel group connected to your backhaul. Overlapping

prefixes advertised to multiple Secure Access regions from 1 NTG per region is supported when MRB is enabled. For more information, refer to Dynamic Routing with Multi-Region Backhaul.

> **Attention**
>
> **The Multi-Region Backhaul feature is currently controlled by a feature flag and is not available or enabled by default.** To request access to this feature, please contact Cisco Secure Access Support.

> **Note**
>
> Inter-region high availability and MRB cannot be enabled simultaneously. If you opt to utilize inter-region high availability, you cannot configure MRB. The reverse logic applies so if you enable MRB, then inter-region HA is not available.

- **Block default route advertisement** – Blocks the advertisement of the default route in dynamic routing mode. Advertising default routes via BGP is not supported and can lead to traffic disruptions.

Step 4 - Data for Tunnel Setup

11. Review and save network tunnel group information for use when setting up your network tunnel devices.

- **Primary Tunnel ID**: The ID you entered in **Step 2 - Tunnel ID and Passphrase**.
- **Primary Data Center IP Address**: The IPv4 and IPv6 addresses to which your network tunnel device will connect to establish the primary tunnel.
- **Secondary Tunnel ID**: The ID you entered in **Step 2 - Tunnel ID and Passphrase**.
- **Secondary Data Center IP Address**: The IPv4 and IPv6 addresses to which your network tunnel device will connect to establish the secondary tunnel.
- **Passphrase**: The passphrase you entered in **Step 2 - Tunnel ID and Passphrase**. This is the only time your passphrase is displayed.

> **Note**
>
> If you opted to configure backup regions, the primary and secondary data center and IP addresses in both the primary and secondary region are included in this page for review. Ensure the IPs and region designations are correct before you click **Done**.

12. Click **Download CSV** to save your tunnel setup information. You can use the information to configure and deploy a tunnel in a network device.
Once the tunnel group is deployed, the initial state of the tunnel group changes from **Unestablished** to **Inactive**.

What to do next

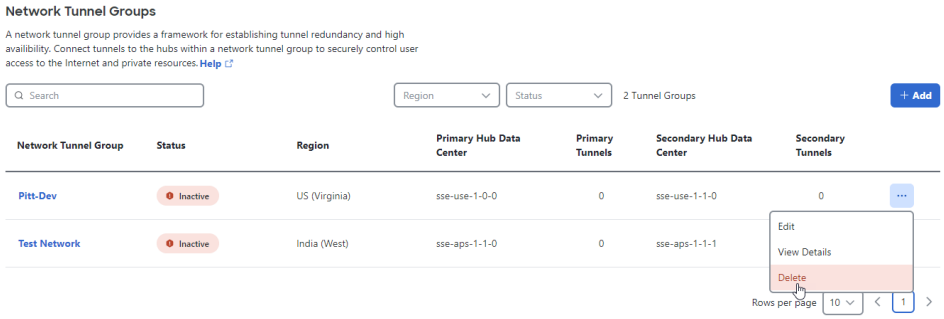
After you configure the tunnel group, perform the following tasks to ensure a robust environment:

- **Configure primary and secondary tunnels:** Configure your network devices to connect to both primary and secondary tunnels to ensure redundancy. For more information, refer to Configure Network Tunnels by Device, Tunnel throughput, capacity, and scaling, and Failover for Branch Connections in Secure Access Data Centers.
- **Enable user connectivity:** Configure user computers to connect securely through the tunnel and send traffic to Secure Access.
- **Verify tunnel status:** Once Secure Access receives traffic, the tunnel status changes to Active. Navigate to the **Overview** page to confirm the status of your configured tunnel.
- **Monitor traffic:** Use the Overview page and Activity Search Report to monitor tunnel traffic events.
- **Configure alert rules:** Set up automated alerts in the Secure Access dashboard or via email to receive notifications when tunnel groups enter a disconnected or warning state. For more information, refer to Monitor Secure Access with Alert Rules.

Delete a Network Tunnel Group

Remove a deployed network tunnel group and its associated IPsec tunnels from your Secure Access organization.

Once a network tunnel group is added to Cisco Secure Access, you can remove the deployed tunnel group from your organization.



Before you begin

Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. From the list of network tunnel groups, expand a tunnel.
3. Click the ellipsis (**...**), and then choose **Delete**.
4. After the delete is completed, verify that the tunnel group is not present in the list of network tunnel groups.

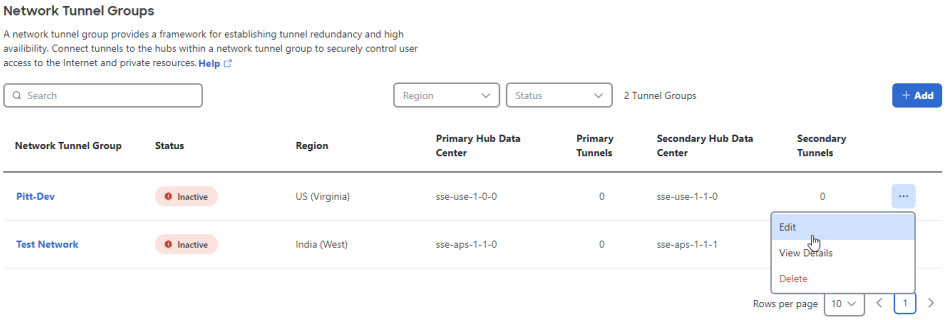
Edit a Network Tunnel Group

Provides instructions for completing the Edit a Network Tunnel Group workflow in Cisco Secure Access. Once a network tunnel group is added to Cisco Secure Access, you can edit the configuration attributes of the deployed tunnel group.

Once a network tunnel group is added to Cisco Secure Access, you can edit the configuration attributes of the deployed tunnel group.

Important

When a network tunnel group is modified, the existing tunnel group is immediately terminated and a new one is established based on the new configuration, leading to a brief interruption in traffic flow while the re-negotiation process occurs. The exact duration of the disconnect depends on the complexity of the configuration change and the network conditions.



Before you begin

Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. From the list of network tunnel groups, expand a tunnel group.
3. Click the ellipsis (**...**), and then choose **Edit**.
4. Navigate through the settings to edit **Tunnel Group Name**, **Region**, **Device Type**, **Tunnel ID**, **Passphrase**, **NAT Mapping**, or **Routing** configuration attributes. This includes the settings for the primary and secondary backup regions if you configured those for your organization. Click "+ Backup region" to add a backup region.

   Tip

   You can swap the primary and secondary data center of a region by clicking the "**Make primary**" button located under the secondary data center.

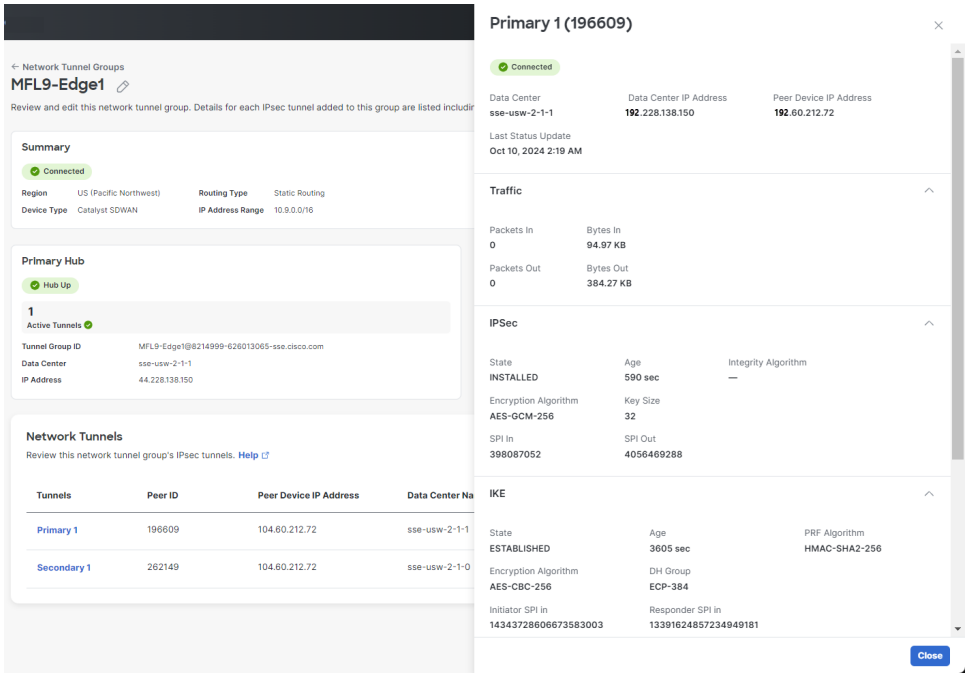
5. Click **Save**.

View Network Tunnel Group Details

Provides instructions for completing the View Network Tunnel Group Details workflow in Cisco Secure Access. Once a network tunnel group is added to Cisco Secure Access, you can view the configuration attributes of a deployed tunnel group.

Once a network tunnel group is added to Cisco Secure Access, you can view the configuration attributes of a deployed tunnel group. You can also edit the attributes of a network tunnel group and view information about the network tunnels associated with the selected tunnel group.

Secure Access also lists the status of your network tunnels and information about the attributes of the deployed tunnel groups in **Home** > **Connectivity**.



Before you begin

A minimum role of Read Only in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. From the list of network tunnel groups, expand a tunnel group.
3. Click the ellipsis (**...**), and then choose **View Details**.
4. Review the **Summary** details for the selected network tunnel group. You can also view the **Primary Hub** and **Secondary Hub** details. If you opted to configure backup regions, the primary and secondary data center IPs are included in this page for review. If you want to swap the primary and secondary regions, you must edit the network tunnel group.
5. Review the **NAT Mappings** table and edit entries in the table.

   Note

   NAT Mappings only apply to Network Tunnel Groups with **Network Address Translation (NAT)** enabled. For more information, refer to Add a Network Tunnel Group.

6. Click on a tunnel name under the **Network Tunnels** pane to view detailed information about the tunnel. You can also download a routing table for the tunnel.
7. (Optional) Click the pencil icon next to the network tunnel group name to edit the tunnel group attributes. See Edit a Network Tunnel Group

The connection status of network tunnel groups and hubs is determined by the following conditions:

- **Connected**: Once Secure Access receives and logs traffic from a network tunnel, the tunnel status will switch to **Active** and the network tunnel group status will switch to **Connected**.

- **Disconnected**: Both primary and secondary hubs are down and have no active network tunnels. This will result in a loss of connectivity for the network tunnel group.
- **Warning**: One of the hubs of the network tunnel group is down and has no active tunnels. This will result in reduced failover and redundancy capabilities, and increased load on the remaining hub.

What to do next

- Monitor tunnel traffic events in Secure Access Overview and Activity Search Report.
- Configure rules to automate alerts in the Secure Access dashboard and by email when network tunnel groups are in a disconnected or warning state. For more information, see Monitor Secure Access with Alert Rules.

Manage Summary Subnets

Configure summary subnet prefixes that Secure Access uses to aggregate BGP routes advertised to network tunnel groups (NTGs) configured for dynamic routing.

Enable, disable, and override advertised BGP route summarization for network tunnel groups (NTGs) configured for dynamic routing with BGP peers. Summary subnets and summarization overrides apply globally across your Secure Access organization.

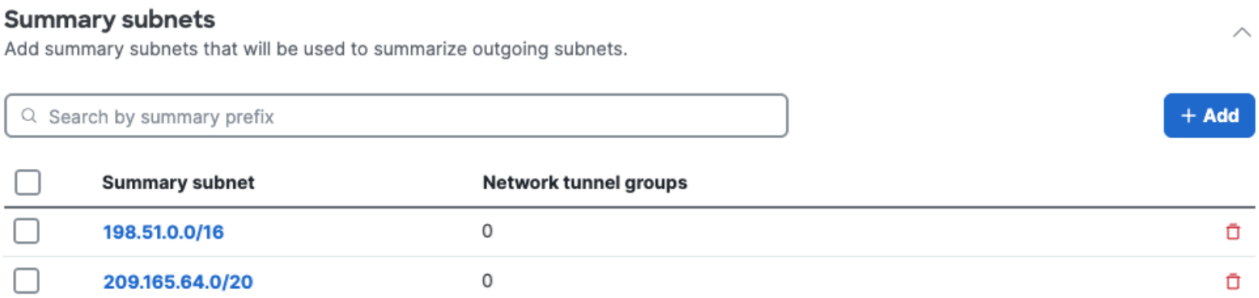
For more information, refer to Route Summarization.

Before you begin

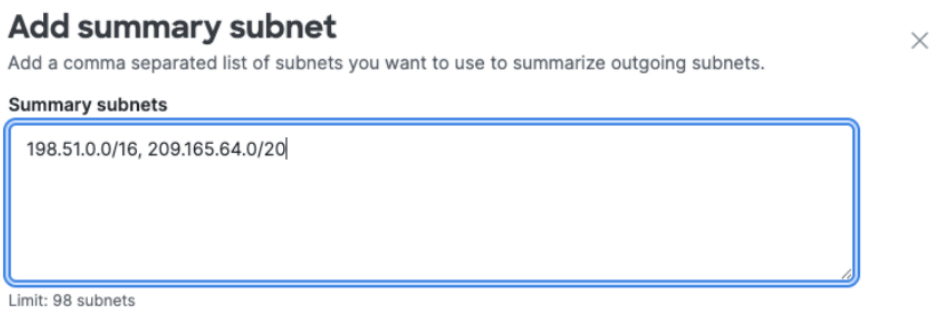
You must have a Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. Click **Route Summarization** (top right).



3. In the **Summary subnets** table, click **+ Add**.
4. Enter a comma-separated list of up to **100** subnet prefixes. Secure Access uses these prefixes to summarize advertised BGP routes.

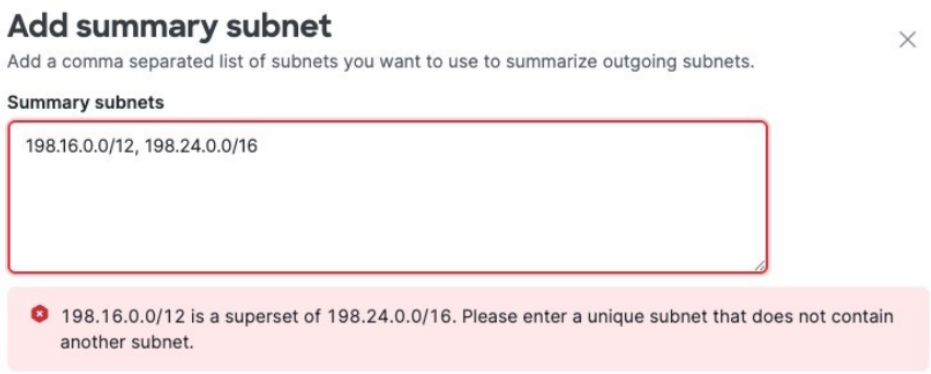


> **Note**
>
> Note: The maximum number of summary subnets allowed is 100 in total. The **Limit** counter below the text field dynamically counts down from 100, reflecting the remaining number of summary subnets available. For example:
>
> - If no summary subnets exist prior to opening the drawer, the counter displays **Limit: 100 subnets**.
> - If 20 summary subnets have already been added, the counter displays **Limit: 80 subnets**.
> - Each subnet in the **Summary subnet** field further decreases the count.

5. Click **Add** to save your changes.

The subnet prefix is added to the Summary subnet table. Secure Access automatically advertises the summary subnet in place of the more specific NTG egress routes it encompasses.

If a subnet prefix overlaps with an existing summary subnet, Secure Access displays the following error: `Please enter a unique subnet that does not contain another subnet.`



Override Route Summarization for a Network Tunnel Group

Override route summarization for specific network tunnel groups (NTGs) that need to receive individual, unsummarized routes instead of aggregated BGP prefixes.

Override route summarization for specific network tunnel groups (NTGs) that need to receive individual, unsummarized routes. This is useful when large branches or data centers require the full set of advertised routes while smaller branches benefit from summarized routes.

You can configure this override from the Route Summarization page as described below. To configure an override from the NTG settings menu, refer to Add a Network Tunnel Group.

Before you begin

- You must have a Full Admin role in Secure Access. For more information, see Manage Accounts.
- Route summarization must be enabled with at least one summary subnet configured. For more information, see Manage Summary Subnets.

Procedure

---

1. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.

2. Click **Route Summarization** (top right).
3. In the **Summarization Override** table, click **+ Add**.
4. Select up to 5 NTGs to override summarization.
5. Click **Add** to save your changes.

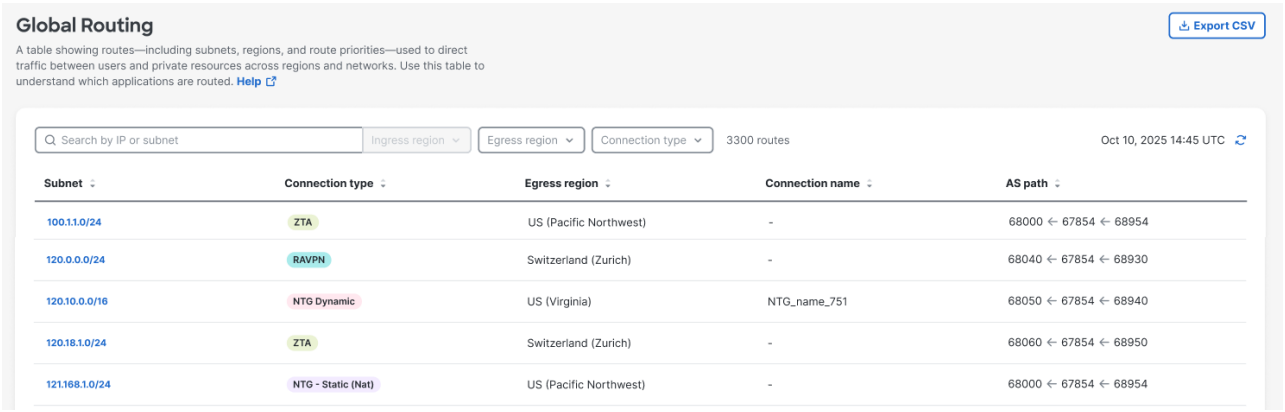
> **Note**
>
> You can add up to 5 NTGs at a time, but there is no limit to the total number of NTG overrides.

View Global Routes

The Global Routing table provides a centralized view of all routes that Secure Access uses to direct traffic between users and private resources across your organization's regions and networks. Use it to investigate overlapping routes, verify route priority, and confirm whether a route exists.

The Global Routing table provides a centralized view of all routes that Secure Access uses to direct traffic between users and private resources across your organization's regions and networks. Use it to investigate overlapping routes, verify route priority, and confirm whether a route exists.

For more information, refer to Global Routing.



Procedure

1. In Secure Access, navigate to **Connect** > **Traffic Management** > **Global Routing Table**.
2. (Optional) In the search bar, enter a destination IP address or subnet.

   All matching routes are displayed.

   If your search returns no matching routes, Secure Access displays one of the following messages:

Message	Meaning
No available routes	The IP or subnet is a non-internet-routable address.
Internet bound route	The IP or subnet routes to the internet despite having no specific route.
Cannot reach internet	The IP or subnet cannot reach the internet until you add a backhaul.

Message	Meaning
No routes	No routes exist because you have not configured VPN, ZTNA, or NTGs.
Could not load routes	A system error is preventing routes from loading. Refresh the page and try again. If the problem persists, contact support. For contact information, see Welcome to Cisco Secure Access.
No routes found	Routes will appear once you begin advertising network subnets from this ingress region.

3. (Optional) Apply filters to narrow results:
   - **Egress region**
   - **Connection type**
   - **Ingress region** (enabled only after you search for a subnet)
4. Review the results in the routing table.

   Important

   The route marked **Prioritized** (blue label with a star) is the route Secure Access selects for the destination.
5. (Optional) Click **Download CSV** to export the results.
6. (Optional) To inspect a specific route, click the route's **Subnet** to open the detail drawer.
   The information displayed in the detail drawer depends on the connection type.

   General information (all connection types)
   - **Subnet** (displayed at the top)
   - **Prioritized** label (when search and Ingress region filter are applied)
   - **Connection type**
   - **Egress region**

   Network details by connection type
   - RAVPN and ZTNA
     - **Data center** – For RAVPN, the data center is based on your Secure Access configuration. For ZTNA, this can be any Cisco data center worldwide.
   - NTG Static (NAT)
     - **Framework**: Network Tunnel Group
   - NTG Static and NTG Dynamic
     - **Framework**: Network Tunnel Group
     - **Connection name**: NTG name (links to the NTG detail page)
     - **NTG status**: Connected, Disconnected, or Warning
     - **Primary hub**: Hub up or Hub down

    - **Secondary hub**: Hub up or Hub down

- NTG Dynamic with a backup region
    - **Framework**: Network Tunnel Group
    - **Connection name**: NTG name (links to the NTG detail page)
    - **NTG status**: Connected, Disconnected, or Warning
    - **Main region** (region name)
        - **Primary hub**: Hub up or Hub down
        - **Secondary hub**: Hub up or Hub down
    - **Backup region** (region name)
        - **Primary hub**: Hub up or Hub down
        - **Secondary hub**: Hub up or Hub down

- Site-to-Site VPN tunnel with Amazon Web Services

  For configuration details, refer to Configure a Site-to-Site VPN tunnel with Amazon Web Services.
    - **Framework**: Network Tunnel Group
    - **Connection name**: NTG name (links to the NTG detail page)
    - **NTG status**: Connected, Disconnected, or Warning
    - **Primary tunnel hubs**
        - **Tunnel group 1**: Hub up or Hub down
        - **Tunnel group 2**: Hub up or Hub down
    - **Secondary tunnel hubs**
        - **Tunnel group 1**: Hub up or Hub down
        - **Tunnel group 2**: Hub up or Hub down

Routing

- **AS path**

Establish an IPsec Tunnel

Prerequisites, requirements, and reference information for establishing an IPsec IKEv2 tunnel from a supported network device to a Cisco Secure Access data center.

Prerequisites

Before you configure an IPsec tunnel to Secure Access, ensure the following items:

- Your network device supports IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels. Secure Access is compatible with any device that fully complies with the IKEv2 RFC standard.
- Your network device firmware is up to date.

- You have administrative access to the network device.
- You have generated tunnel passphrase credentials in Secure Access.
- The IP addresses of all endpoints within a network tunnel group, including the Secure Access hubs and the customer spoke endpoints, must be unique. However, if your endpoints are behind devices that apply NAT to the tunnel, you can reuse an IP address for your endpoints if you ensure that NAT translates unique source ports for each tunnel.

> **Note**
>
> Any third-party router or device that fully complies with the IKEv2 RFC standard should be able to connect to Secure Access. To confirm device compatibility, review the device documentation for IKEv2 RFC compliance.

Establish a Tunnel

You can establish an IPsec IKEv2 tunnel from a supported network device to a Secure Access data center. To configure the tunnel, use the tunnel passphrase credentials you generated in Secure Access.

For device-specific configuration steps, see Configure Network Tunnels by Device. The sample commands in those guides use the `<secure_access_dc_ip>` variable to represent the public IP address of the Secure Access data center you are connecting to.

For supported IPsec parameters, see Supported IPsec Parameters.

Maximum Transmission Unit (MTU) Size

- IPsec tunnels for Secure Access must have an MTU of **no larger than 1390 bytes** for inner packets. Where possible, configure the MTU of the peer devices VTI interface to match 1390.
  - Some devices (including Cisco FTD and Cisco Meraki) auto-calculate the VTI interface MTU by default and do not require manual configuration. Never reduce the MTU on physical interfaces (LAN or WAN).
- Packets that exceed the MTU in the underlay or overlay are dropped. Exceeding the supported values risks fragmentation and packet loss.
- If you experience fragmentation or packet loss, verify that your tunnel (inner) MTU does not exceed 1390 bytes and that TCP MSS clamping is correctly configured.

TCP MSS (Maximum Segment Size) Clamping

Cisco Secure Access automatically performs TCP MSS Clamping (1350 bytes) to ensure that TCP payloads are always small enough to be compatible with the maximum supported MTU. To avoid fragmentation and performance issues ensure that TCP MSS clamping is either disabled on the peer device, or configured to match the Secure Access supported value of 1350.

Path MTU Detection

Secure Access supports path MTU detection (PMTUD) to allow detection of the maximum packet size for other protocols (for example, UDP). Path MTU detection relies on ICMP packets; ensure ICMP Fragmentation Needed messages are allowed to cross from Secure Access to your local network.

Tunnel Throughput, Capacity, and Scaling

Each tunnel supports the following limits and allowances:

Parameter	Limit
Maximum throughput	1 Gbps per tunnel (in either direction)
Packets per second	No restriction

Parameter	Limit
Users per tunnel	No restriction

Warning

Exceeding the 1 Gbps throughput limit may result in degraded performance, including increased latency and packet loss.

To achieve throughput beyond 1 Gbps, you can establish multiple tunnels. You can initiate multiple IPsec tunnels from the same device or aggregate tunnels from different devices within the same network tunnel group. When you use multiple tunnels, divide traffic with one of the following methods:

- **ECMP (Equal-Cost Multi-Path routing)** – Load-balances traffic across tunnels. Secure Access supports up to 10 ECMP tunnels. For more information, see Equal-Cost Multi-Path (ECMP) Support.
- **Policy-based routing** – Assigns specific traffic to specific tunnels based on your routing policies.

Secure Access also supports connecting multiple high-availability (HA) routers from the same branch in either **Active - Active** or **Active - Standby** mode. In an Active/Standby configuration, traffic routes through the primary tunnel when it is up. The secondary tunnel is used only when the primary tunnel is down; client routes are populated on the secondary tunnel only during failover.

Important

To protect against loss of connectivity, set up redundant tunnels for a network tunnel group. For more information, see Manage Network Tunnel Groups.

Carrier-Grade NAT (CGNAT) Requirement

Secure Access internally uses the Carrier-Grade NAT (CGNAT) IP block for services such as **ZTNA** and **Resource Connector**. Proper handling of this IP space on your on-premises tunnel gateway is critical to prevent connectivity issues (such as the inability to access private resources, or inconsistent traffic routing), even when test connectivity results appear successful.

On your on-premises tunnel gateway, you must ensure the following:

1. Do not block traffic destined for the CGNAT IP address range (`100.64.0.0/10`).
2. Route all traffic destined for `100.64.0.0/10` through the tunnel to Secure Access.
3. Apply the same routing treatment to your customer-configured remote access VPN and system IP pool subnets. Ensure traffic destined for these subnets is routed through the tunnel to Secure Access and is not blocked.

Table 3: CGNAT routing requirements

Subnet or range	Required action
`100.64.0.0/10` (Secure Access CGNAT)	Do not block; route through the tunnel to Secure Access
Remote access VPN pool subnets (customer-configured)	Do not block; route through the tunnel to Secure Access
System IP pool subnets (customer-configured)	Do not block; route through the tunnel to Secure Access

The specific configuration steps vary depending on your device and environment.

For more information, see Add an IP Pool.

Client-Reachable Prefixes

By default, Secure Access routes all traffic destined for private RFC 1918 addresses back through the tunnel. This means Secure Access expects the source IP of outbound packets from your network to be a private RFC 1918 address.

If your network uses non-RFC 1918 source addresses, add those prefixes as client-reachable prefixes when you configure your tunnel. This overrides the default behavior so that Secure Access also routes return traffic for those prefixes through the tunnel. For information about address allocation and private networks, see RFC 1918.

Secure Access supports two options for client-reachable prefixes:

- **Static IP addresses** – Must be globally unique within your Secure Access organization. No other network tunnel group in your organization can use the same address.
- **BGP-based dynamic routing** – Enables advertisement of private network prefixes to physical network devices that support BGP (such as routers), removing the dependency on static route configuration.

Important

After you update client-reachable prefixes for an established tunnel, wait at least **five minutes**, then disconnect and shut down the tunnel for at least **ten seconds** before reconnecting.

Supported IPsec Parameters

Provides reference information about Supported IPsec Parameters in Cisco Secure Access. Cisco Secure Access uses the IPsec protocol for tunneling traffic.

Cisco Secure Access uses the IPsec protocol for tunneling traffic. IPsec has multiple components and one of the core components is Internet Key Exchange (IKE). IKE manages negotiation with peers, authentication, and certificate exchanges. IKE maintains the session by using Dead Peer Detection (DPD) as per RFC 5996. Secure Access supports IKEv2, which is faster and more secure than IKEv1.

Secure Access supports the configuration of certain IPsec parameters to deploy a network tunnel. Even if a device can establish an IPsec tunnel to Secure Access, we do not guarantee that the tunnel is compatible. For example, if the tunnel enables Perfect Forward Secrecy (PFS), you can establish a tunnel, but in the event of reconnection, the tunnel may fail to rekey and lose service. We recommend that you test the tunnel connectivity thoroughly before putting any tunnel into production.

Components	IKEv2 (Phase I) (no IKEv1 support)	ESP (Phase II)
Encryption	**AES-256-16 (GCM)**, AES-256-8 (GCM), AES-128-16 (GCM), AES-128-8 (GCM), AES-128(CBC), AES-256(CBC)	**AES-256-16(GCM)**, AES-128-16(GCM), AES-256(CBC), AES-128(CBC), NULL(GCM) - AES-256 GMAC, NULL(GCM) - AES-192 GMAC, NULL(GCM) - AES-128 GMAC NULL(CBC)
Hashing	**SHA256**, SHA1	**SHA256**, SHA1
DH Group	**20**, **19**, 15 14	**20**, **19**, 15, 14
Authentication	**Pre-Shared Key (PSK)**	N/A
Protocol	N/A	ESP in UDP (NAT-T) (Port - UDP 4500)
Total Child SAs Supported	N/A	1

Components	IKEv2 (Phase I) (no IKEv1 support)	ESP (Phase II)
Lifetime (Rekey) **Note** Lifetime (Rekey) does not support seamless IKE re-authentication.	Based on client settings (IKE default is 4 hours)	Based on client settings (Child SA default is one hour)
Perfect Forward Secrecy (PFS)	N/A	Allowed (Ciphers configured with both PFS and non-PFS.) **Note** If the remote end prefers to negotiate PFS, it has to set the child rekey timer lower than the head end and/or allow both PFS and non-PFS. Reason: CNHE prefers non-PFS. We configured both, but if the other side wants PFS, we can negotiate.
DPD Timeouts*	1 DPD every 30 seconds 5 retransmits with exponential backoff (Maximum DPD timeout = 156 seconds)	N/A
IP fragmentation	Not supported	Not supported
IKE Fragmentation (RFC 7383)	Enabled	N/A
Extended Sequence Number (ESN)	N/A	Allowed and preferred

Recommendations are in **Bold**.

Note

Secure Access routing platforms are optimized for Galois/Counter Mode (GCM) encryption. Thus, we recommend that you use GCM encryption for maximum throughput. Using cipher block chaining (CBC) may result in lower throughput. Performance is subject to hardware and configurations.

* 1. DPD is sent 30 secs after the previous one (or tunnel up)

1. 1st retransmit - after 2 secs
2. 2nd retransmit - after 4 secs
3. 3rd retransmit - after 8 secs
4. 4th retransmit - after 16 secs
5. 5th retransmit - after 32 secs

6. 64 secs later, we give up - no more retransmits

Max total DPD timeout = 30 + 2 + 4 + 8 + 16 + 32 + 64 = 156 secs

Routing Options and Guidelines for Network Tunnel Groups

Before you configure network tunnel groups in Secure Access, understand and choose the correct routing option for tunnel redundancy and high availability.

Secure Access Network Tunnel Groups provide a framework for establishing tunnel redundancy and high availability by connecting your on-premise network devices securely to Cisco Secure Access data centers. When configuring a network tunnel group, you must define routing to the host or network using either static or dynamic routing.

Routing Options:

Routing Options for Network Tunnel Groups

- **Static Routing**–Use static routing for small, simple networks where routes are predictable and manual configuration is manageable. Choose static routing if:
  - Your network uses unsupported router discovery protocols.
  - You want to avoid the overhead of dynamic routing protocols.
  - A default route is insufficient, and you need to specify explicit routes to internal networks.
  - You are using features that do not support dynamic routing.

> ⚠ **Caution**
>
> Advertising a default route using static routing is not supported and may cause traffic disruptions.

- **Dynamic Routing Using BGP**–Use dynamic routing with BGP for large, complex networks with multiple connections. BGP provides automatic route updates, optimal path selection, and supports advanced features like Multi-Region Backhaul and Equal Cost Multi-Path (ECMP) load balancing. BGP peering is typically configured over the 169.254.0.0/24 subnet with your on-premise router.
- **Asymmetric Routing**–When using SD-WAN or complex, multi-region topologies, forward and return traffic may enter Secure Access through different data centers or regions (asymmetric routing). Secure Access automatically detects and manages these asymmetric flows by forwarding both directions of the connection to a single region for stateful inspection and consistent policy enforcement. This feature works transparently alongside both static and dynamic routing configurations and helps maintain reliable connectivity and security without requiring manual route symmetry.

Additional Benefits of Network Tunnel Groups

- Each network tunnel group includes primary and secondary hubs for redundancy. Traffic normally flows through the primary tunnel, failing over to the secondary if needed.
- Multiple tunnels can be configured to increase throughput (up to 1 Gbps per tunnel). ECMP can be used to load balance traffic across tunnels.
- For high availability, Active/Standby or Active/Active CPE device configurations are supported, with BGP recommended for routing.

- AS path preservation: Secure Access dynamic routing will honor AS path lengths, allowing customers to influence routing to Secure Access within a region using Active/Active NTG deployments.
- Multi-hop support: External BGP peer sessions can be established between network devices that are not directly connected, enabling more flexible routing architectures.

More Information

For more information, refer to specific routing topics:

- Static Routing
- Dynamic Routing with BGP
- Dynamic Routing with Multi-Region Backhaul
- BGP Next-Hop Configuration
- User VPN Pool Sizing and BGP Advertisement
- Asymmetric Routes
- Equal-Cost-Multi-Path (ECMP) Support

NAT Mapping for Network Tunnel Groups

Network Address Translation (NAT) mapping for network tunnel groups translates IP address prefixes to resolve overlapping subnets and enable site-to-site and site-to-cloud communication through Secure Access.

Overview

When your network and your partners' networks use overlapping IP address ranges, NAT mapping translates real IP prefixes to unique mapped prefixes. This resolves address conflicts and enables correct routing between branch sites, subnets, and cloud applications.

Secure Access supports explicit NAT mappings for both sources (such as endpoints that initiate requests) and destinations (such as internet destinations or private applications on your WAN). This enables bidirectional communication between sites and between sites and cloud resources.

> **Note**
>
> Secure Access does not support IPv6 for NAT mapping.

For NAT mapping configuration details, refer to the **Routing option** step in Add a Network Tunnel Group.

Key Capabilities

- **Overlapping subnet resolution** – Maps real IP prefixes to unique translated prefixes, resolving address conflicts and ensuring correct routing between branch sites and cloud applications.
- **Bidirectional NAT flows** – Supports both Secure Access-to-site and site-to-Secure Access traffic flows so that applications and users can communicate in both directions with correct address translations.
- **Automatic route advertisement** – Advertises static routes for mapped prefixes automatically to maintain network reachability after translation.
- **Real-time validation** – Validates mappings in the user interface to prevent overlapping or mismatched prefix lengths and avoid configuration errors.

- **IP address conservation** – Hides internal private IP addresses by translating them to public or unique mapped IPs, which conserves public IP address space.

NAT Terminology
Table 4: Secure Access NAT Terminology

Term	Definition
Network address translation (NAT)	Translates private (inside local) IP addresses to public (inside global) IP addresses. NAT can be static (one-to-one mapping) or dynamic (many-to-many mapping that uses a pool of public IP addresses).
Prefix-to-prefix translation	Translation of one IP address prefix to another, where prefixes use CIDR notation to specify the network address and subnet mask length. This method translates entire blocks of IP addresses rather than individual addresses.
Site-to-site	Traffic flow in which branch site users access private resources at other sites. NAT translates source private IP addresses to addresses from the destination site subnet.
Site-to-Secure Access	Traffic flow in which branch site users access cloud resources. NAT translates private IP addresses to public IP addresses.
Secure Access-to-site	Return traffic flow from internet destinations to source devices at a branch site. NAT translates the cloud's public IP addresses back to the site's private IP addresses, which enables cloud services to communicate with site devices.

Static Routing

Provides reference information about Static Routing in Cisco Secure Access. You add network tunnel groups to Secure Access to enable secure network connections to the internet and private resources.

You add network tunnel groups to Secure Access to enable secure network connections to the internet and private resources. When setting up a network tunnel group, you can choose static routing or dynamic routing (when you have a BGP peer for your on-premise router).

Use static routing for small, simple networks where predictable routes are needed and manual configuration is manageable. You might want to use static routes in the following cases:

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes, such as a static route to an "inside network" when you need to explicitly direct traffic to a specific internal network segment that isn't reachable through the default gateway or via dynamic routing protocols.
- You are using a feature that does not support dynamic routing protocols.
- Note that advertising a default route using static routing is not supported and can lead to traffic disruptions.

Dynamic Routing with BGP

Provides reference information about Dynamic Routing with BGP in Cisco Secure Access. Border Gateway Protocol (BGP) automates the exchange of routing information between autonomous systems (AS) to determine optimal paths for data traffic and failover routing without the need to configure and maintain static routes.

Border Gateway Protocol (BGP) automates the exchange of routing information between autonomous systems (AS) to determine optimal paths for data traffic and failover routing without the need to configure and maintain static routes.

When setting up a network tunnel group in Secure Access, choose dynamic routing if you have a BGP peer for your on-premise router. Dynamic routing using BGP enables the advertisement of customer-specific routes, which is essential for Secure Access tunnels to properly route return traffic to your networks. Without these routes, return traffic cannot be routed correctly.

For more information about BGP, refer to Cisco Support documentation topics Select BGP Best Path Algorithm and Examine Border Gateway Protocol Case Studies

For Secure Access configuration details, refer to Add a Network Tunnel Group, View Network Tunnel Group Details, and Secure Access Regions.

Advantages of Dynamic Routing with BGP

- **Automatic Route Updates**–Route changes on the customer side are automatically communicated to Secure Access, eliminating the need for manual updates in the dashboard settings.
- **Dynamic Failover**–If a tunnel on the Secure Access side becomes unavailable, routes sent to the customer dynamically adjust, enabling seamless failover to a secondary tunnel.

BGP Peer Route Limitations

Exceeding the 10k routes per BGP peer limit resets the BGP connection and blocked further requests to use BGP on that network group tunnel. Review the following limitation for any specific environment limitations or recommendations:

- Each IPSEC/Meraki AutoVPN Network Tunnel Group is limited to a maximum of 10K routes per BGP peer.

Important

Exceeding the route limitations resets the BGP connection and blocks further requests to use BGP on that network group tunnel.

Secure Access BGP Configuration Best Practices

Tunnel Redundancy and High Availability Principles

- A single network tunnel group can support multiple IPsec tunnels to achieve redundancy and high availability.
- For optimal redundancy, maintain a 1-to-1 correspondence between primary and secondary IPsec tunnels. For example, if you configure six primary IPsec tunnels to a data center for Equal-Cost Multi-Path (ECMP), you should have six corresponding secondary IPsec tunnels to ensure full redundancy. This setup requires one BGP connection per IPsec tunnel.

BGP Peer IP Addresses

- **Secure Access (SSE) Side**–Secure Access uses IP addresses within the 169.254.0.0/24 range for BGP peering. For example, the primary data center might use 169.254.0.5 and the secondary data center 169.254.0.9.

- **Customer Side**–For ease of configuration, it is recommended to use corresponding IP addresses within the 169.254.0.0/24 range (e.g., 169.254.0.6 for 169.254.0.5, and 169.254.0.10 for 169.254.0.9). However, the customer-side IP address range is not restricted to 169.254.0.0/24 and can be different.

BGP Identifier (Router ID)

- Do not use 169.254.0.1 as the BGP identifier.
- For the customer-side BGP identifier, use the local router's gateway address (typically an RFC1918 address, e.g., 192.168.x.x). Avoid using addresses within the 169.254.0.0/24 range. Note that some devices refer to the BGP identifier as the Router ID.

Customer Autonomous System Number (ASN)–Use any private BGP ASN within the range `64512-65534`.

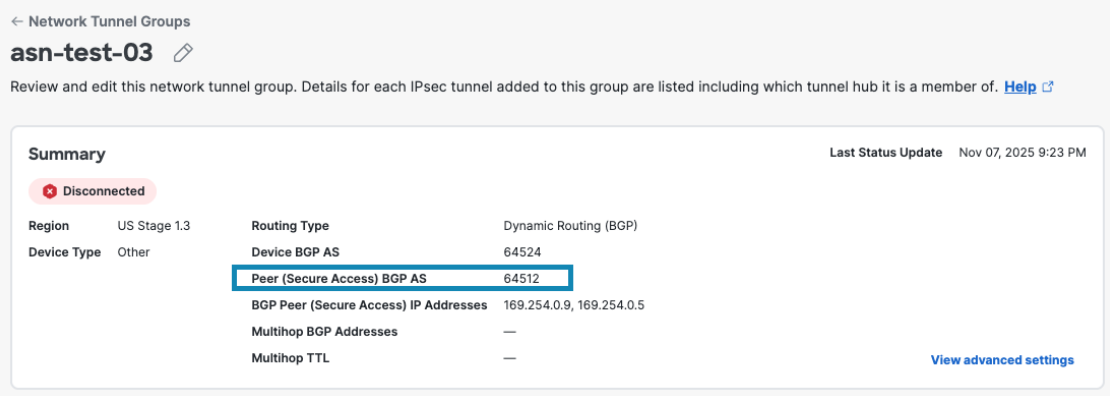
Note

eBGP peering can only happen between devices with different ASNs.

All newly created Secure Access organizations use the public ASN `32644` by default for BGP peering in network tunnel groups. Existing organizations established prior to November 2025 continue to use the private ASN `64512` that was previously reserved for Secure Access BGP peers.

If the private AS number `64512` is assigned to a device on your network, it will not be able to peer with a network tunnel group configured for **Peer (Secure Access) BGP AS**`64512`.

To identify the AS number used by your network tunnel groups, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**, click a network tunnel group by name, and check the field **Peer (Secure Access) BGP AS** to identify the ASN.



If your organization requires a different ASN, contact Cisco Secure Access support to request an update. For more details, refer Welcome to Cisco Secure Access. Note that changing the ASN is a global setting and will affect all network tunnel groups and BGP peering relationships for your Secure Access organization.

Route Advertisement by Secure Access–Secure Access advertises multiple routes for various services and components. To ensure the correct return path for traffic, separate routes are advertised for each region in use. The number of routes advertised will scale depending on the type of features deployed and the number of regions used by end users. The table below details the types of routes Secure Access advertises:

Table 5: Route Advertisement by Secure Access

Destination Address	Route Size	Purpose / Number of routes
35.95.175.78 44.240.251.165	/32	Secure Access speedtest tool
100.64.0.0/10	/32	ZTA Proxy servers (several /32 prefixes in each region utilised by ZTA users) Resource connector (one /32 prefix per connector)
100.64.0.0/10	/28	Network tunnel groups in NAT mode (several /28 prefixes, with the NAT prefix shared in common by multiple tunnels)
240.0.0.0/28	/32	Resource connector (legacy connector groups)
System IP Pool	/32	Remote Access VPN servers (two /32 prefixes or more in each configured region)
User VPN Pool	/22 or smaller	Each pool separated into a minimum of two or more smaller pools (maximum prefix of /22 per chunk) to support high availability and scaling
Other Branches	-	Routes advertised by other network tunnel branches (depends on customer configuration)

Routes advertised by Secure Access prepend the original AS path to include:

- `1` for primary tunnels
- `2` for secondary tunnels

This preserves the original AS path and allows customers to install all received routes in their Forwarding Information Base (FIB) and switch between primary and secondary routes based on their routing decisions.

Connecting Multiple High Availability (HA) Devices to Secure Access—Secure Access supports connecting multiple HA routers from the same branch, whether in Active/Active or Active/Standby mode.

- All IPsec tunnels from all HA routers must belong to the same Network Tunnel Group.
- Devices should advertise the same set of routes to Secure Access.
- Use AS path length to define device priority:
  - For Active/Active mode, use the same AS path length for all routes advertised by both devices.
  - For Active/Standby mode, advertise routes from your Active device with a shorter AS path length (e.g., length of 1 for Active, 2 for Standby).
- You can connect as many HA routers as needed, but a Network Tunnel Group is limited to a maximum of 20 IPsec tunnels overall (10 IPsec tunnels to the primary data center and 10 to the secondary).

- You can aggregate IPsec tunnels from different devices within the same network tunnel group if those devices are part of a HA pair (either Active/Active or Active/Standby mode).
- Do not aggregate multiple IPsec tunnels from different devices that are not part of an HA pair within the same network tunnel group.

Block Default Route Advertisement

Advertising default routes via BGP from the customer to Secure Access is not supported and can lead to traffic disruptions. You can block default route advertisements from Secure Access to the customer site.

1. From the Secure Access dashboard, go to **Connect** > **Network Connections** > **Network Tunnel Groups**.
2. In the Advanced Settings of the network tunnel group routing configuration, check **Block default route advertisement**.

Avoid Router ID and BGP Peer Conflicts

BGP requires a Router ID to establish BGP sessions between peers. Without a unique Router ID, BGP cannot establish peering sessions. When configuring Secure Access network tunnel groups, you can use the same BGP peer IP addresses for any or all of your network tunnel groups within the same region. However, the BGP Router ID must be unique to each BGP peer within a network. Each router in the network must have a unique Router ID.

Monitor BGP Client and Cloud Routes

To view BGP client routes received from your customer-side network:

- Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
- Click on a specific network tunnel to open its details pane on the right-hand side of the page.
- The **Client Routes** section displays the routes received from your network.
- Routes are visible on the primary tunnels. If multiple primary tunnels advertise the same route, the route will appear on each of those primary tunnels.

All other routes for your organization (those not originating from a primary tunnel) are displayed in the **Cloud routes** section of the network tunnel details pane.

Dynamic Routing with Multi-Region Backhaul

Provides reference information about Dynamic Routing with Multi-Region Backhaul in Cisco Secure Access. The Multi-Region Backhaul feature is currently controlled by a feature flag and is not available or enabled by default.

> **Attention**
>
> **The Multi-Region Backhaul feature is currently controlled by a feature flag and is not available or enabled by default.** To request access to this feature, please contact Cisco Technical Support.

Secure Access network tunnel groups can extend customer backhaul networks across multiple Secure Access regions, providing enhanced routing and failover capabilities. With **Multi-region backhaul (MRB)**, customers can connect their entire BGP fabric to Secure Access, allowing them to advertise the same routes in different Secure Access regions. With MRB, if active tunnels in a network tunnel group fail within a region and equivalent routes exist in other regions, Secure Access prioritizes routing traffic to standby tunnels in the same region before considering alternate regions.

Note

Overlapping prefixes advertised to Secure Access from multiple customer Network Tunnel Groups are supported by Secure Access BGP only when MRB is enabled on those Network Tunnel Groups. When MRB is not enabled, overlapping prefixes should not be advertised across multiple Network Tunnel Groups.

MRB requires the following conditions:

- The customer backhaul network must connect to two or more Secure Access network tunnel groups with **Multi-region backhaul** enabled.
- The customer backhaul network must use **BGP** to advertise subnet prefixes and preferences to Secure Access.

When MRB is enabled on network tunnel groups connected to the customer backhaul, Secure Access employs BGP attributes to prioritize traffic flow, particularly between primary and secondary tunnels:

- **BGP community string:** When a network tunnel group is created with MRB enabled, Secure Access advertises a BGP community string to the customer backhaul in the format `32644:X`. In this string, 32644 is the Cisco Secure Access public Autonomous System Number (ASN), and X encodes regional priority. The customer backhaul network policy can then transform this BGP community string into an internal priority (e.g., a local preference for iBGP or an EIGRP metric) to preserve routing symmetry with Secure Access.
- **Multi-Exit Discriminator (MED):** If MRB is enabled, the primary Secure Access data center advertises the prefix with a MED value of 0, while the secondary data center uses MED: 1. The lower MED value is always preferred, ensuring that the primary data center is preferred for routing whenever possible.

For more information, see the Cisco SASE Design Guide Deep Dive.

Remember

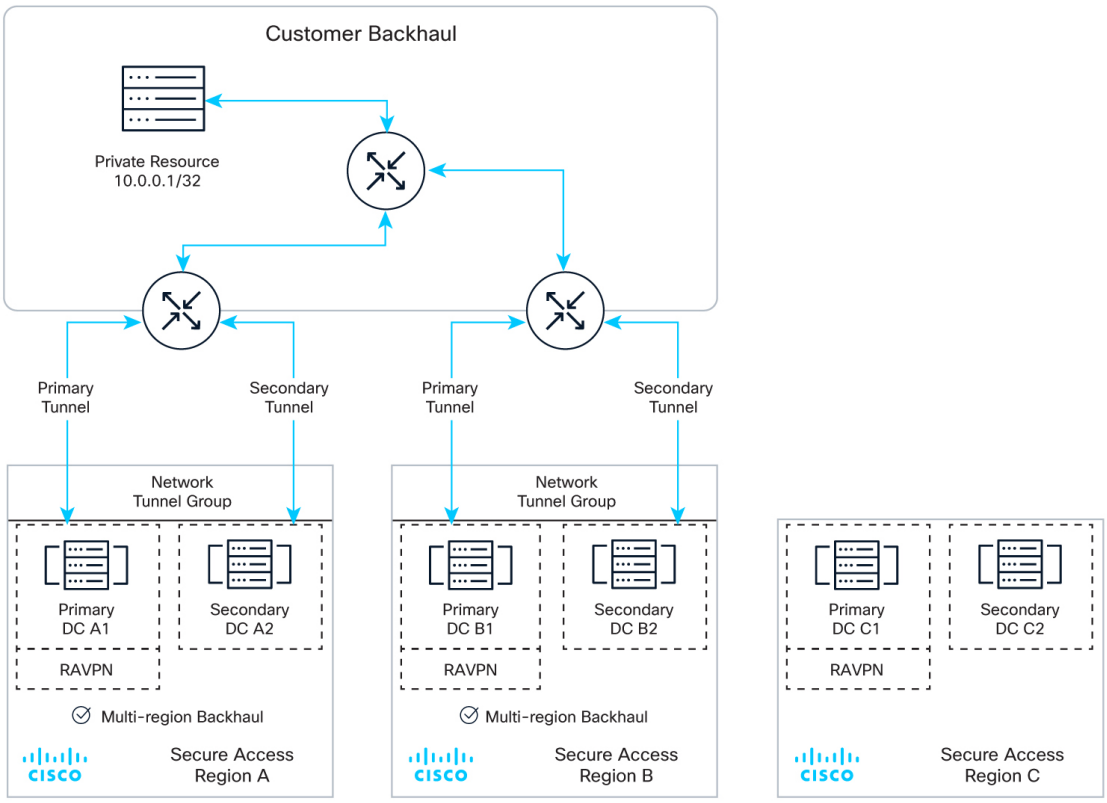
When MRB is not enabled, Secure Access typically uses the AS path length for route prioritization between primary and secondary tunnels instead of MED. BGP prefers shorter AS paths.

Multi-Region Backhaul Scenarios

Multi-region backhaul supports the following scenarios:

- **Local Tunnel Failover**–When a primary tunnel fails, the network tunnel group automatically fails over to the secondary tunnel within the same region.
- **Regional Failover**–If an entire Secure Access region fails, traffic fails over to another region connected to the customer backhaul. To enable regional failover, **Multi-region backhaul** must be enabled on all relevant network tunnel groups connected to the customer backhaul network.
- **RAVPN User Access to Remote Resources**–If an RAVPN user connects to a Secure Access region that is not directly connected to the customer backhaul where the requested private resource resides, Secure Access forwards the RAVPN user traffic to the appropriate region to complete the request.
- **Optimal RAVPN Return Traffic**–Secure Access advertises RAVPN user route prefixes and preferences to the customer backhaul. This ensures optimal routing of return traffic and helps avoid asymmetric routing by customer routers.

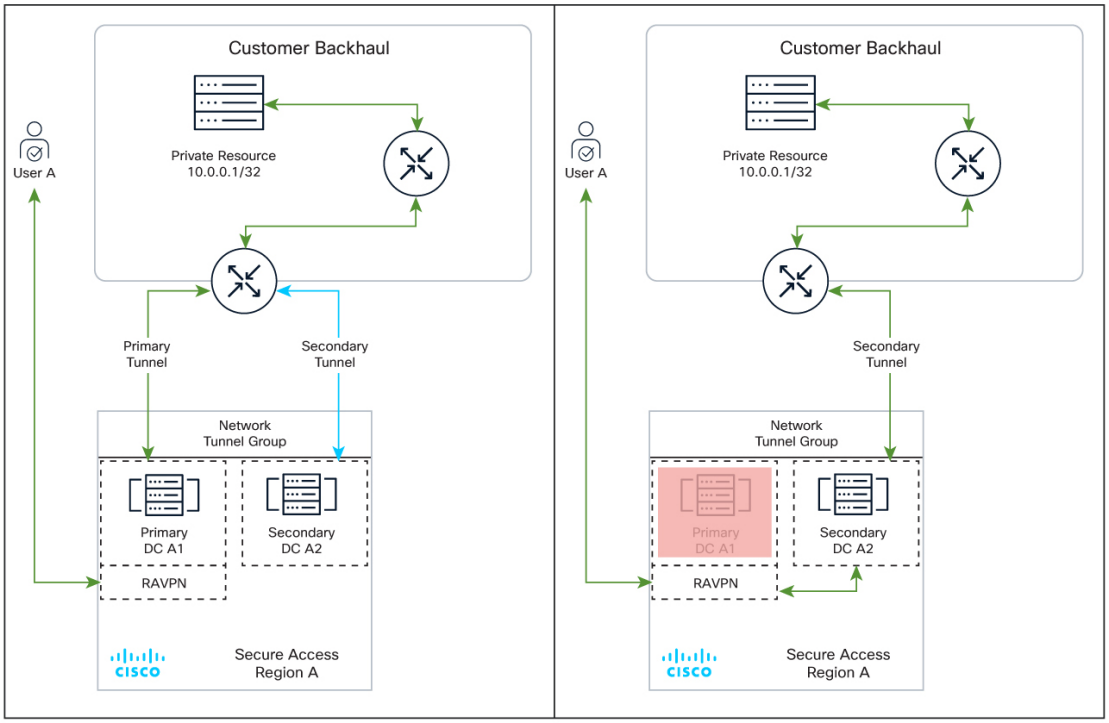
This diagram illustrates a private resource within a customer backhaul network spanning Secure Access Regions A and B. Region C is not directly connected to the backhaul. All three regions share routing information. The customer backhaul can advertise the same prefixes in all the Secure Access regions without breaking traffic symmetry. Secure Access always uses the shortest path to the backhaul.



The customer IPsec router is connected to a network tunnel group in Secure Access Region A, which is the customer's preferred route to the subnet prefix advertised by BGP (10.0.0.1/32 in this example).

Scenario A: Local Tunnel Failover

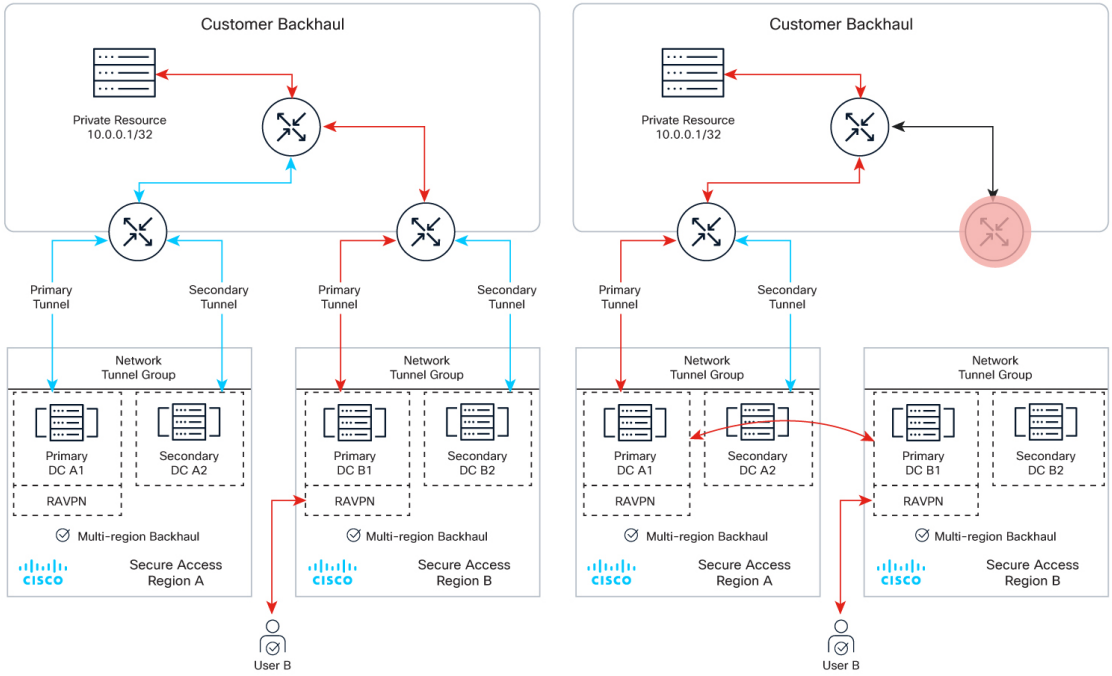
When the primary tunnel fails, the network tunnel group fails over to the secondary tunnel within the same region. Automatic failover from the primary to the secondary tunnel is the expected behavior with or without **Multi-region backhaul** enabled.



When **Multi-region backhaul** is not enabled on the network tunnel group, the subnet prefix will only be advertised for that network tunnel group, and remote users will only be able to access the private resource from Region A.

Scenario B: Regional Failover

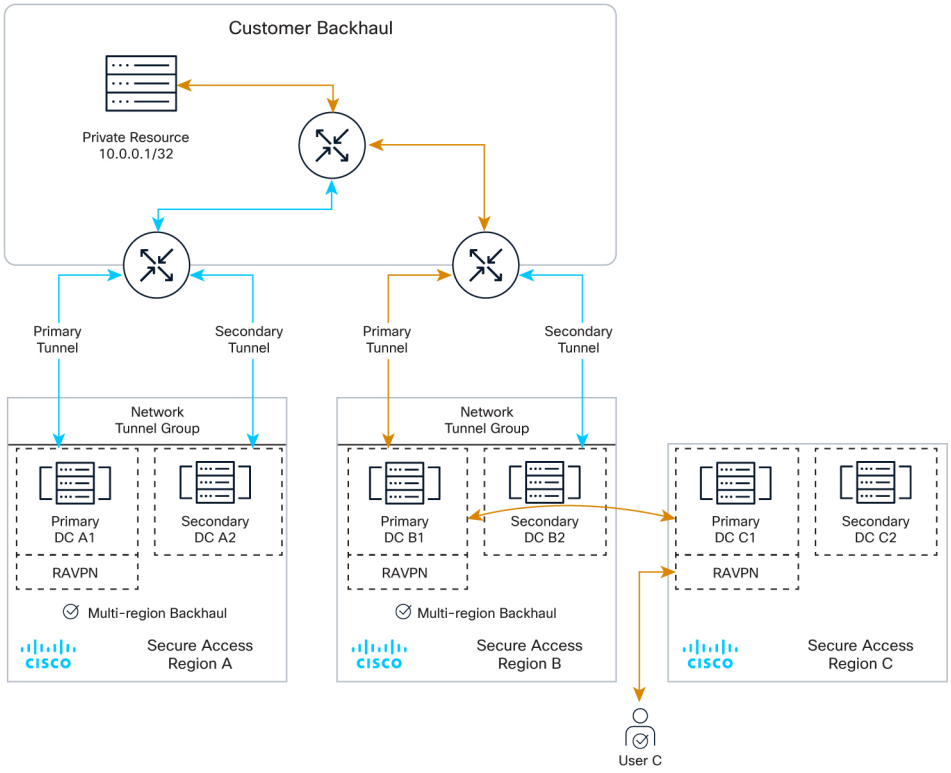
When **Multi-region backhaul** is enabled, the subnet prefix will be advertised to multiple network tunnel groups that may span Secure Access regions. Each region will prioritize local routes.



- Region B learns the prefix and routes advertised for both Region A and Region B, and prioritizes local routes.
- User B connects to RAVPN via DC B1 in Region B and accesses the private resource via the primary tunnel in Region B.

- If the network tunnel group between Region B and the customer backhaul goes down, automatic failover supports User B's access to the private resources via the primary tunnel in Region A.

Scenario C: Access from an Unconnected Region



- In this scenario, the customer has not set up a network tunnel group in Region C. Without a direct connection to the customer backhaul, Region C learns the prefix and routes advertised for both Region A and Region B.
- Region C prefers Region B because it is closer.
- As in Scenario B, if Region B goes down, automatic failover supports User C's access to the private resource via the network tunnel group in Region A.

For configuration details, refer to Add a Network Tunnel Group, View Network Tunnel Group Details, and Secure Access Regions.

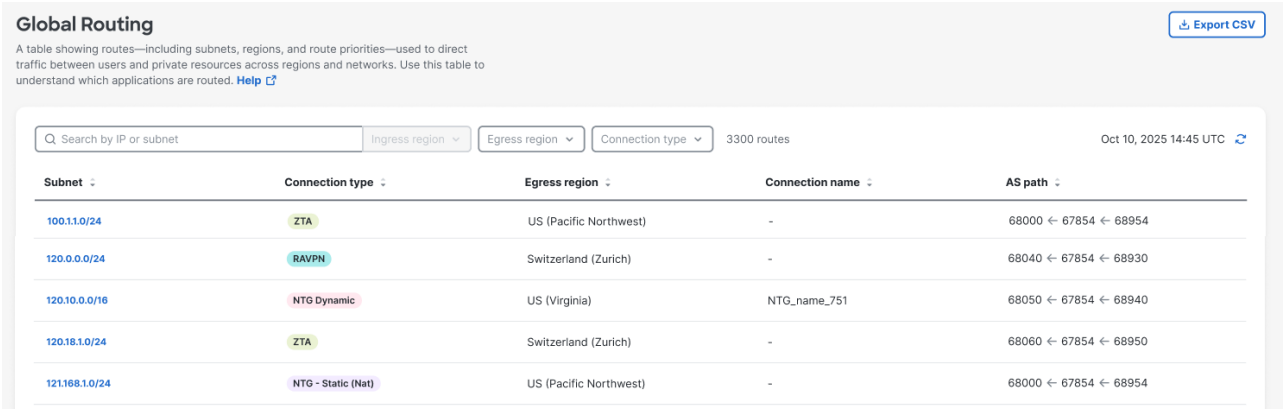
Global Routing

The Global Routing table provides a centralized view of all routes that Secure Access uses to direct traffic between users and private resources across your organization's regions and networks. Use it to investigate overlapping routes, verify route priority, and confirm whether a route exists.

The Global Routing table provides a centralized view of all routes that Secure Access uses to direct traffic between users and private resources across your organization's regions and networks. Use it to investigate overlapping routes, verify route priority, and confirm whether a route exists.

For more information, refer to View Global Routes.

Route information



The Global Routing table displays the following information for each route:

Column	Description
Subnet	The destination IP subnet.
Connection type	The connection method: NTG Dynamic (BGP), NTG Static, NTG Static (NAT), RAVPN, or ZTNA.
Egress region	The region where traffic exits Secure Access.
Connection name	The name of the network tunnel group (NTG).
AS path	The BGP AS path. A shorter path indicates a more optimal route.

> **Note**
>
> The AS path appears only for subnets advertised from NTG configured for dynamic routing with BGP. For more information, refer to Dynamic Routing with BGP.

Route prioritization

When you enter a subnet in the search field and apply an Ingress region filter, Secure Access identifies the **prioritized route** – the route that Secure Access selects before any others for that destination. A blue **Prioritized** label with a star icon appears next to the subnet in both the table and the route details drawer.

Secure Access determines route prioritization based on:

- AS path length
- Preference for the ingress region
- The route traverses a tunnel connected to the currently active NTG hub

> **Tip**
>
> In general, a shorter AS path indicates a more optimal route.

In its default state (no search or ingress region filter applied), no prioritized label appears. The absence of a label does not mean the route is unused; it means that the route selection process has not yet been triggered by a search.

Important

Multiple prioritized routes can appear when NTGs, RAVPN, or ZTNA pools advertise the same prefixes to multiple Secure Access regions. Unless the routes are associated with an NTG configured for Multi-Region Backhaul (MRB), treat this condition as a misconfiguration and review the affected connections.

For more information, refer to Dynamic Routing with BGP and Dynamic Routing with Multi-Region Backhaul.

BGP Next-Hop Configuration

This topic describes how BGP next-hop addresses are configured for customer route advertisements based on the BGP session type and neighbor addresses.

This topic describes how BGP next-hop addresses are configured for customer route advertisements based on the BGP session type and neighbor addresses. For more information, see Dynamic Routing with BGP and Add a Network Tunnel Group.

Session Types and Next-Hop Behavior

1. **Dual-Stack BGP Sessions (IPv4 and IPv6)**–Each address family uses its corresponding BGP neighbor address as the next-hop.
   - IPv4 routes: Next-hop matches the IPv4 BGP neighbor address.
   - IPv6 routes: Next-hop matches the IPv6 BGP neighbor address.
2. **IPv4-Only BGP Session**–Can advertise both IPv4 and IPv6 prefixes.
   - IPv4 routes: Next-hop matches the IPv4 BGP neighbor address.
   - IPv6 routes: Next-hop is derived by mapping the IPv4 neighbor's suffix to the IPv6 prefix.
3. **IPv6-Only BGP Session**–Can advertise both IPv4 and IPv6 prefixes.
   - IPv4 routes: Next-hop is derived by mapping the IPv6 neighbor's suffix to the IPv4 prefix.
   - IPv6 routes: Next-hop matches the IPv6 BGP neighbor address.

Example BGP Next-Hop Configuration

This example shows how to configure route advertisements given these prefix ranges:

- IPv4: `169.254.0.0/24`
- IPv6: `2a04:e4c4:b:c723::b67:0000/120`

Scenario 1: IPv6 BGP session–If your BGP peer address is `2a04:e4c4:b:c723::b67:0009`, Secure Access dynamically sets the next-hop addresses based on the peer:

- IPv4 next-hop will include the mapped suffix 0x9: `169.254.0.9`
- IPv6 next-hop will match the peer address: `2a04:e4c4:b:c723::b67:0009`

Scenario 2: Dual-stack IPv4/IPv6 BGP session–If your BGP peer addresses are `169.254.0.5` and `2a04:e4c4:b:c723::b67:0009`, Secure Access sets the next-hop addresses to match the peer:

- IPv4: `169.254.0.5`
- IPv6: `2a04:e4c4:b:c723::b67:0009`

Next-hop addresses always match the BGP neighbor address for the corresponding address family when both IPv4 and IPv6 sessions are established.

User VPN Pool Sizing and BGP Advertisement

Provides reference information about User VPN Pool Sizing and BGP Advertisement in Cisco Secure Access. Secure Access BGP will not advertise a prefix larger than /22.

Secure Access BGP will not advertise a prefix larger than /22. When you configure a user VPN pool for remote access VPN (RAVPN) in Secure Access, the platform processes the network as follows.

Prefix larger than /22

If the provided network is larger than /22 (e.g., /20), the platform automatically splits the network internally into multiple /22 chunks.

Example:

- You provide a /20 pool.
- Secure Access splits this into 4 × /22 subnets internally.
- Each /22 is leased by a data center in the region on demand.
- When a data center leases a /22, it advertises only that /22 (or smaller) over BGP – not the full /20.

Prefix equal to /22 or smaller

If the provided network is /22 or smaller (e.g., /24), the platform splits the network into at least two smaller subnets to support high availability across a minimum of two data centers in the region.

Example:

- You provide a /24 pool.
- Secure Access splits this into 2 × /25 subnets.
- Each /25 is assigned to a different datacenter in the region.
- Each data center advertises its respective /25 over BGP.

VPN pool subnet advertisement scaling on demand

VPN pool subnets are not all advertised simultaneously. Instead, they are allocated and advertised on demand as the number of RAVPN client connections increases: Initially, only the first subnet (e.g., the first /22 of a /20) is leased and advertised via BGP. As demand grows, additional subnets are leased by data centers and subsequently advertised. This is consistent with how cloud resources are dynamically scaled.

Example:

- You configure 4 × /22 pools to cover a /20 range.
- At low connection volume, BGP advertises only the first /22.
- As RAVPN connections increase, the remaining /22 pools are activated and advertised incrementally.

Important

If you observe that only one of your configured pools is being advertised, this is expected behavior. Additional pools will be advertised as scaling demands require.

Table 6: Summary

Provided pool size	Internal split	BGP advertisement	Reason
Larger than /22 (e.g., /20)	Split into multiple /22s (e.g., 4 × /22)	Each /22 or smaller, on demand	Max advertised prefix is /22; on-demand scaling

Provided pool size	Internal split	BGP advertisement	Reason
/22	Split into 2 or more smaller subnets	Each smaller subnet, on demand	High availability across ≥2 data centers
Smaller than /22 (e.g., /24)	Split into at least 2 subnets (e.g., 2 × /25)	Each subnet, on demand	High availability across ≥2 data centers

Key takeaways

- **Maximum BGP advertised prefix:** /22 – Secure Access never advertises a network larger than /22 over BGP.
- **Automatic splitting** – Networks are split internally for high availability (minimum 2 data centers per region) and scalability.
- **On-demand advertisement** – Subnets are advertised via BGP only when they are actively leased by a data center to serve connections. Not all pools appear in BGP at once.
- **Scaling is dynamic** – Additional pool subnets are activated as RAVPN client connection counts increase, following cloud-native resource scaling principles.

Asymmetric Routes

This concept explains how Secure Access identifies asymmetric routes and ensures that both directions of network traffic are forwarded to a single region. This approach enables unified security inspection, consistent policy enforcement, and continuous connectivity across multi-region or SD-WAN environments.

Asymmetric routes occur when the forward and return flows of your connection pass through different Secure Access regions or data centers. This happens in modern SD-WAN or multi-region architectures. Dynamic routing may send traffic along different paths for each direction.

The Secure Access platform provides automatic handling of asymmetric routing. If it detects that a connection's directions traverse different regions, Secure Access forwards both flows to one region for inspection and policy enforcement. Flow pinning ensures consistent application of security policies and uninterrupted connectivity, even when asymmetric paths exist.

Key Concepts

- **Automatic Flow Pinning**: Secure Access automatically reroutes asymmetric flows so both directions are inspected in the same region.
- **Consistent Security Enforcement**: Security policies and stateful firewall checks always occur in one region, regardless of the SD-WAN routing choice or the network routing choices.
- **Operational Simplicity**: You do not need to manually enforce route symmetry, even in complex environments.
- **Session Reliability**: You avoid connection drops and maintain secure, reliable access to applications.

Supported Workflows

- Remote Access VPN (RAVPN) users connect to SD-WAN.
- Users from non-SD-WAN branches connect to SD-WAN.
- Users from Network Address Translation (NAT) branches to SD-WAN.

> **Note**
>
> You will rarely encounter asymmetric routing between non-SD-WAN branches because these branches are usually not multi-homed.

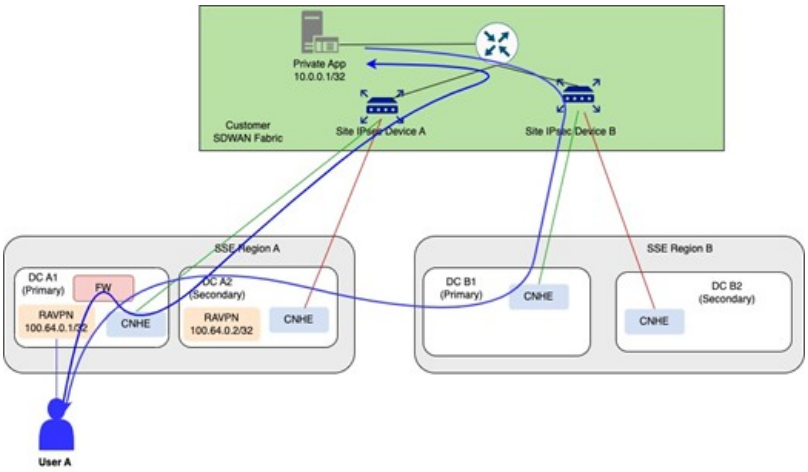
Scenarios

1. **Scenario 1: RAVPN User with Asymmetric Path**

   A RAVPN user initiates a connection to a private application.

   - The forward flow enters Secure Access through the US West region.
   - Due to SD-WAN routing, the return network traffic from the application is routed through the US East region.

     Secure Access Handling: Secure Access detects the asymmetry and forwards the return traffic to the US West region, where it inspects both flows and enforces security policies.



2. **Scenario 2: Branch User with Asymmetric Routing**

   A branch user connects to a private resource.

   - The forward flow is established through a branch router connected to the EU Central region.
   - SD-WAN routing can send the return flow through a different branch router connected to the EU North region.

     Secure Access Handling: Secure Access processes both the forward and reverse flows in the EU Central region to maintain session integrity and consistent security enforcement.

3. **Scenario 3: NAT Branch with Multi-Region SD-WAN**

   If your branch uses NAT, it initiates a session with Secure Access.

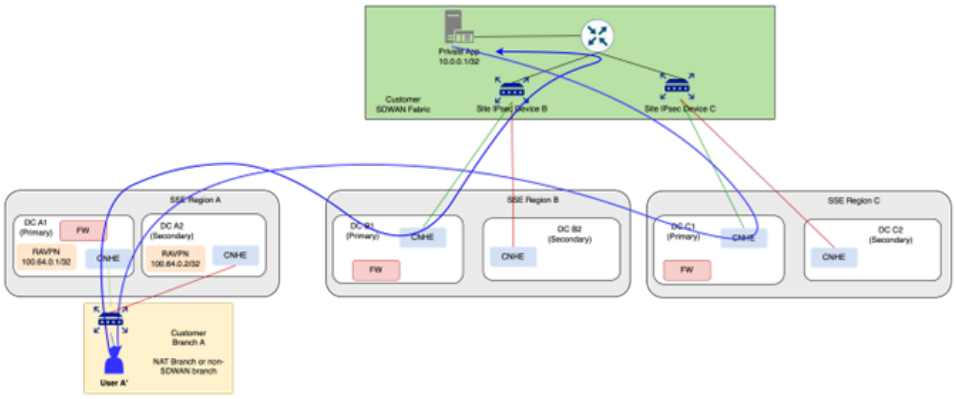
   - The forward traffic enters through the APAC South region.
   - SD-WAN routing causes the return traffic to pass through the APAC North region.

     Secure Access Handling: Secure Access processes both flows in APAC South to provide stateful inspection and uninterrupted security.

     Benefits

     - **Reliability:** Prevents session drops caused by asymmetric routing across regions.
     - **Consistent Security:** Ensures that all connections are inspected and policies enforced in a single location.

- **Operational Efficiency:** Simplifies network design and reduces administrative overhead in multi-region and SD-WAN deployments.



Note

Secure Access supports asymmetric routing only for flows that involve SD-WAN connections. It does not support multi-homing or asymmetric routing between Remote Access VPN (RAVPN), Network Address Translation (NAT), or non-Software Defined Wide Area Network (SD-WAN) branches. For example, asymmetric routing between RAVPN and a branch or between two non-SDWAN branches is not supported.

Equal-Cost-Multi-Path (ECMP) Support

Cisco Secure Access supports ECMP across primary IPsec tunnels within the same network tunnel group.

Equal-Cost-Multi-Path (ECMP) is a routing strategy that distributes next-hop packet forwarding across multiple tunnels with equal routing cost. In Cisco Secure Access, ECMP load-balances traffic across primary IPsec tunnels within a Network Tunnel Group (NTG), improving bandwidth utilization and providing redundancy. If primary tunnels become unavailable, traffic failover to secondary tunnels is automatic and ECMP will continue to route traffic across equal cost paths.

Key capabilities

Feature	Specification
Maximum tunnels to Primary DC	10
Maximum tunnels to Secondary DC	10
Maximum throughput per NTG	Up to 10x1 Gbps
Tunnel naming convention	Base name + prefix (+1, +2, +3, etc.)

ECMP behavior

Understanding how ECMP handles traffic flows is critical for proper deployment. When a network tunnel group has multiple IPsec tunnels to the same data center, Secure Access automatically applies ECMP in the following conditions:

- **Static routing** – ECMP occurs automatically across all IPsec tunnels in the NTG. For more information, refer to Static Routing.
- **Dynamic routing** – ECMP occurs automatically across all IPsec tunnels where the same prefix is advertised on BGP connections. For more information, see Dynamic Routing with BGP.

ECMP is supported on tunnels within a single NTG but is not supported on tunnels between NTGs. If multiple prefixes need to be advertised over different NTGs in different regions, consider enabling **Multi-Region Backhaul** on the NTGs. For information about how Multi-Region Backhaul works in Secure Access, refer to Dynamic Routing with Multi-Region Backhaul. For information about configuring Multi-Region Backhaul, refer to Add a Network Tunnel Group.

Default behavior: stateless ECMP

By default, ECMP operates in stateless mode:

- A hash of packet fields ensures all packets from a single flow follow the same path.
- Flow stickiness is not enforced, meaning forward and return paths may differ: A flow may traverse Tunnel 1, while return traffic comes back through Tunnel 2.

Example: A user initiates a connection that is routed through Tunnel 1. The response from the destination may return through Tunnel 2 if both tunnels are part of the same ECMP group.

> **Note**
>
> Secure Access ECMP hashing uses source IP, destination IP, protocol, and IPv6 flowlabel, deliberately excluding ports. This design ensures that IP fragments or related flows without port information follow the same ECMP path, leveraging the IPv6 flowlabel to maintain flow consistency in IPv6 environments. By contrast, default ECMP hashing uses the 5-tuple: source IP, destination IP, source port, destination port, and protocol.

Stateful ECMP with NAT for Secure Internet Access (SIA)

When an NTG is configured to use **outbound NAT** for an SIA tunnel use case, ECMP behavior is stateful: Outbound NAT enforces flow stickiness, so both forward and return traffic use the same tunnel.

Use case: Enable NAT when internet destinations require symmetric routing or when firewalls/security devices need to see both directions of a flow on the same path.

> **Note**
>
> - Unless stateful ECMP is required for a specific use case, it is not best practice to use ECMP with an NTG that is configured to use NAT. NAT may reduce routing performance and reliability.
> - NTGs configured to use NAT do not support ECMP for a Secure Private Access (SPA) tunnel use case.

For more information, see **Network Address Translation (NAT)** on Add a Network Tunnel Group.

Configuring ECMP

To enable ECMP, each tunnel must be uniquely identifiable using one of these methods:

- **Different public IP addresses**, OR
- **Unique tunnel name prefixes** (+1, +2, +3, etc.)

Additional ECMP requirement: For ECMP to distribute traffic across multiple tunnels to the same remote peer, each tunnel must use a unique combination of **source IP address** and **UDP source port**. ECMP commonly hashes on the outer packet headers. If multiple tunnels use the same effective source IP address and UDP source port, they can hash to the same path, reducing or eliminating the benefit of load balancing.

You can meet this requirement in either of these ways:

- Use a **different public source IP address** for each tunnel.

- Use a **different local source address** for each tunnel, such as a **dedicated loopback interface** per tunnel. If all tunnels share the same public WAN IP address, use NAT/PAT to assign a **unique translated UDP source port** to each tunnel.

A common approach is to use one loopback interface per tunnel:

1. Create a separate loopback interface for each tunnel and assign each loopback a unique IP address.
2. Configure each tunnel or IKE/IPsec peer to use its assigned loopback as the local source address.
3. If all tunnels egress through a single public WAN IP address, configure NAT/PAT so that each loopback-sourced tunnel is translated to the same public IP address with a unique UDP source port.
4. Verify that each tunnel presents a unique source IP address and UDP source port combination on the WAN.

Note

When NAT is used, uniqueness is determined by the translated outer source IP address and UDP source port seen on the WAN, not by the internal loopback address alone.

Note

The requirement applies to the **source** IP address and **source** UDP port used on egress. The destination UDP ports used for IKE or NAT remain unchanged.

Caution

Do not configure multiple tunnels with the same effective source IP address and UDP source port. If you do, those tunnels can follow the same ECMP path, which can prevent traffic from being balanced across available paths.

Tunnel naming convention

When creating multiple tunnels to the same hub within an NTG, use the following naming convention:

Tunnel hub	Tunnel name format
Tunnel 1	HUB 1 SDWANCSS@8195126-656604351-sse.cisco.com
Tunnel 2	HUB 1 SDWANCSS+1@8195126-656604351-sse.cisco.com
Tunnel 3	HUB 1 SDWANCSS+2@8195126-656604351-sse.cisco.com
Tunnel N	HUB 1 SDWANCSS+{N-1}@8195126-656604351-sse.cisco.com

Note

- The prefix values (+1, +2, etc.) must be sequential. Maximum of 10 tunnels per hub.
- Although you add prefixes (+1, +2, etc.) to differentiate tunnels, Secure Access strips these identifiers during authentication to keep the tunnels grouped under the same NTG.

Step-by-step: Enabling ECMP

1. Plan your tunnel architecture. Determine the number of tunnels needed based on throughput requirements. Plan an equal number of tunnels for Primary and Secondary DCs for failover parity.
2. Configure tunnel names with prefixes. For each additional tunnel to the same hub:
   a. Use the base tunnel name for the first tunnel, for example SDWANCSS@<domain>.
   b. For each additional tunnel to the same hub, append a numeric suffix:
      1. Second tunnel: +1
      2. Third tunnel: +2
      3. Continue up to +9 (for a maximum of 10 tunnels)
3. Ensure that each tunnel is differentiated for ECMP. Each tunnel must present a unique combination of source IP address and UDP source port on egress. You can achieve this by using one or both of the following:
   a. A unique public source IP address for each tunnel
   b. A unique UDP source port for each tunnel, configured manually or through NAT/PAT on egress
4. Configure NAT based on the deployment design.
   a. If the NTG performs source NAT for tunnel-bound traffic, enable **Outbound NAT** on the NTG.
   b. If the attached device is a firewall, do not enable **Outbound NAT** on the NTG.
5. Enable ECMP on the device that forwards traffic across the tunnels.
   a. If the attached device is a firewall, enable ECMP on the firewall.
   b. Configure the device to preserve flow symmetry so that return traffic uses the same tunnel as forward traffic.
6. Validate the configuration.
   a. Verify that each tunnel uses a unique effective source IP address and UDP source port on the WAN.
   b. Verify that traffic is distributed across the expected ECMP paths.
   c. If stateful inspection is used, verify that return traffic follows the same tunnel as the forward traffic.

Best practices

Recommendation	Rationale
Configure equal primary and secondary tunnels	Ensures equivalent throughput during failover
Use sequential prefix numbering	Maintains organizational clarity and avoids conflicts
Avoid configuring NTGs to use NAT	NTGs configured for static or dynamic routing will support stateless ECMP for both SIA and SPA tunnels
Monitor tunnel health regularly	Ensures ECMP distributes traffic only across healthy paths
Document your tunnel naming scheme	Simplifies troubleshooting and future modifications

Recommendation	Rationale
Distribute load based on Layer 4 criteria rather than round robin.	When configuring the ECMP distribution algorithm on the IPsec peer device, we recommend selecting a Layer 4-based algorithm (protocol/port) to ensure optimal performance and application reliability.

Route Summarization

Understand how route summarization reduces the number of BGP routes advertised between customer sites through Secure Access by combining specific subnets into aggregate network prefixes.

Route Summarization combines specific subnets into a single aggregate network prefix before advertising them to your network. This reduces the number of routes your branch routers need to store and process. Enable route summarization in Secure Access for network tunnel groups (NTGs) configured for dynamic routing with your BGP peers.

Route summarization applies only to egress routes advertised between customer NTGs and Secure Access.

For configuration details, refer to Manage Summary Subnets and Override Route Summarization for a Network Tunnel Group.

Why use route summarization

Route summarization is most useful in Secure Access NTG deployments with many branches or ZTNA host routes, where routing table size can become a scaling concern.

When many branches are connected to Secure Access with each advertising its own prefixes, the total number of routes advertised to every branch can grow significantly. Small branch routers and SD-WAN devices may struggle to handle large routing tables. Route summarization (also known as route aggregation) addresses this by:

- **Reducing routing table size** – Aggregated prefixes replace large numbers of individual routes, lowering memory and CPU usage on branch routers.
- **Improving network performance** – Summary routes hide individual subnet changes, reducing route churn and BGP routing reconvergence events.
- **Simplifying network management** – Fewer advertised routes make monitoring and troubleshooting easier.

How route summarization works in Secure Access

1. **Define global summarization profiles** – In the Secure Access dashboard, configure a list of prefixes that you want to use as summary addresses. Configure up to 100 summary prefixes. Both IPv4 and IPv6 prefixes are supported. Summary prefixes cannot overlap with one another.
2. **Override summarization for specific NTGs** – Route summarization applies globally to all NTGs and BGP peers by default. You can override it for specific NTGs when large branches or data centers need to receive the full set of individual routes while smaller branches benefit from summarized routes.
3. **Secure Access advertises summary prefixes** – When your configured summary prefixes encompass your branch egress routes, Secure Access advertises only the summary prefix to your other branches instead of every individual sub-prefix.

   For example, if you configure a summary prefix of `10.0.0.0/16`, Secure Access advertises the summary route in place of any NTG routes whose subnets are encompassed by `10.0.0.0/16` (such as `10.0.1.0/24` or `10.0.128.0/17`). No additional configuration is required.

   Routes whose subnets extend beyond the summary prefix (such as `10.0.0.0/8` or `192.168.1.0/24`) are not summarized and continue to be advertised individually.

> **Note**
>
> Route summarization is configured for NTGs, but if a configured summary prefix also includes addresses from remote access VPN IP pools or the Carrier-Grade NAT (CGNAT) IP block, those routes will also be summarized. For more information about IP pools, refer to Add an IP Pool. For more information about CGNAT, refer to Establish an IPsec Tunnel.

Route summarization does not apply to the following cases:

- Routes that do not match a configured summary prefix are advertised individually.
- Routes with a shorter prefix length than the summary prefix are not summarized to prevent over-aggregation.
- NTGs configured for static routing or NAT.

Multi-Region Backhaul (MRB) exclusion:

- NTGs configured for multi-region backhaul (MRB) are automatically excluded from summarization and always receive individual routes.
- Route summarization and MRB cannot be enabled simultaneously on the same NTG. MRB requires the full set of individual route prefixes and their associated regional priority attributes to function correctly.

Important

For MRB-enabled tunnels, you must configure traffic steering policies (route maps) on your network device based on the individual, unsummarized routes. For more information, refer to Dynamic Routing with Multi-Region Backhaul.

Key considerations

- **Visibility** – In the NTG details in the Secure Access dashboard, you can see which routes are being advertised as summarized and which are being passed through individually. You can also view the detailed component routes that make up a summarized prefix.
- **Flexible control** – Turn summarization on or off for all NTGs with a single setting. Override summarization for specific NTGs.
- **IPv4 and IPv6** – Route summarization is supported for both IPv4 and IPv6 address families.
- **Limits** – Up to 100 summary subnet prefixes can be configured.

BGP route filtering per network tunnel group

Explains how Cisco Secure Access route filtering controls routes accepted from or advertised to BGP-enabled network tunnel groups. It describes the benefits, use cases, filtering directions and modes, default behavior, and supported prefix types and features.

BGP route filtering per network tunnel group (NTG) is a Cisco Secure Access feature that enables administrators to control, from the cloud and client, which routes are accepted from or advertised to each BGP-enabled NTG. This allows for granular security, compliance, and optimization without editing filters on individual branch devices.

By default, Cisco Secure Access advertises all known routes to all BGP-enabled NTGs and accepts all prefixes from branch peers. This can lead to excessive routing table entries, security risks, and operational complexity. Route filtering per NTG solves these problems by allowing centralized, per-peer control over which IP prefixes are accepted or advertised, using simple cloud-based configuration.

Benefits

- Centralizes control with a single interface for route filtering across multiple NTGs.
- Reduces operational overhead by eliminating per-device BGP filter management.

- Improves security and compliance by isolating sensitive or rogue routes.
- Optimizes routing behavior and network performance by selective advertisement.

Sample use cases

Some of the use cases for the route filtering feature include:

- Selective advertisement: Only advertise necessary routes to certain branches.
- Partner route protection: Prevent overlap or rogue routes from external partners.
- Region-based segmentation: Restrict route propagation to NTGs in a specific geography.
- Compliance assurance: Ensure sensitive subnets are never advertised to unauthorized branches.

Types of route filtering

Filtering can be applied in two directions:

- Client or Ingress filtering: controls which routes received from branches are accepted into Secure Access.
- Cloud or Egress filtering: controls which routes Secure Access advertises to branch devices.

Filter modes

- Equal to: Filters only the specified prefix match. For example, 10.10.5.0/24.
- Less than: Filters the specified prefix and any sub-prefixes under it.

  For example, /24 rule applies also to /25, and /26 within that /24 subnet.

BGP route filter parameters and limits

Lists the parameters, options, and organizational limits for BGP route filters used with network tunnel groups in Cisco Secure Access.

This section lists the parameters, match options, limits, and supported values for BGP route filters per network tunnel group in Cisco Secure Access.

Table 7: Route filter parameters

Parameter	Description	Allowed Values	Default
Direction	Filter direction: ingress (client) or egress (cloud)	ingress, egress	-
Prefix/Subnet	IP prefix in CIDR notation to filter	IPv4 or IPv6 prefix For example, 10.10.5.0/24	-
Match Mode	How the prefix is matched	Equal to Less than	Equal to
Action	Permit (allow) or deny (block)	Allow, Deny	Depends on the direction
Target NTGs	One or more NTGs by name where the filter needs to be applied	Multi-select	-

Table 8: Route filter limits

Limit	Value
Maximum filters per organization	1000
Bulk action limit	Up to 5 per operation
Supported tunnel types	BGP-enabled NTGs only
Propagation Delay	1 – 2 minutes This is the time for a new filter to take effect.

Restrictions for BGP route filtering per NTG

Outlines restrictions on configuring BGP route filtering for NTGs, specifying that this feature is not supported on static NTGs or NTGs with MRB enabled.

You cannot configure the BGP route filtering feature on static NTGs, and on NTGs with multi-region backhaul (MRB) enabled.

Key considerations

Lists key considerations for BGP route filtering per NTG, including how filtering interacts with route summarization, which overlapping filters are allowed, and guidelines on filter modifications.

- Filtering and summarization: Plan the interaction between filters and route summarization. Filtering is always evaluated before summarization and may prevent a summary from being advertised if all child prefixes are filters out or denied.
- Allowed overlapping filters:
  - Overlapping filters that have different prefix length, say less than /24 and /23, where the more specific prefix takes priority.
  - Overlapping filters that have the same prefix length, say /24 and /24, only if there are no overlapping NTGs
- Filter modification: You can modify the filter action while editing the rule. You cannot change the filter from client filter to cloud filter or the other way around by editing.
- Review the impact of filter changes using the per-NTG and global route tables before and after deployment.

Configure BGP route filters per NTG

Guides you through configuring BGP route filters per NTG in Cisco Secure Access, including client and cloud filters, filter actions, target groups, bulk actions, and applying filters during NTG creation to control route acceptance and advertisement.

Use this procedure to configure BGP route filters per NTG to control which routes are accepted from or advertised to BGP peers.

Before you begin

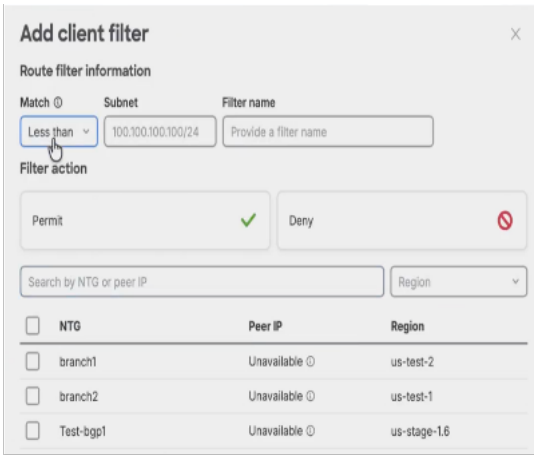
- Ensure you have at least one BGP-enabled NTG in Cisco Secure Access.
- Verify that you have sufficient privileges to modify Traffic Management and route filters.
- Decide which prefixes, and match modes you want to allow or deny.

Procedure

1. Navigate to **Connect** > **Traffic Management** > **Route Filters** in the Secure Access UI.
2. Choose the filter type:
   - Choose Client filters for ingress filters that control which routes are accepted from the branch. They support both allow and deny filter actions.
   - Choose Cloud filters for egress filters that control which routes are advertised to the branch. They support only deny filter action.
3. Click **Add Filter**.

   A side panel **Add client filter** or **Add cloud filter** opens.

   Figure 1: Add client filter panel



   a) Enter a filter name.
   b) Specify the Subnet/Prefix.

      Enter the prefix in CIDR notation. For example, `10.10.5.0/24`.

   c) Select a match mode: **Less than** or **Equal to**.
   d) Set the **Action** as **Allow** or **Deny**.
      - **Allow**: Permits only the specified NTGs. By default, it denies all other NTGs in this case.
      - **Deny**: Blocks only the specified NTGs. By default, it allows all other NTGs in this case.

   e) Select the target NTGs by name.

      You can select multiple NTGs.

   f) Review your settings.
4. Click **Save**.
5. (Optional) Apply a bulk action.

   You can select up to five filters and choose **Change Action** or **Delete**.

6. (Optional) Apart from the steps listed above, you can also apply route filters while creating a new NTG.
   a) Navigate to **Secure Access** > **Connections** > **Network Connections** > **Network Tunnel Groups** > **Add a Network Tunnel Group** to create a new NTG.
   b) In the Route Filters section, select the subnets to be filtered.
   c) Select the filter actions to be applied.

d) Click **Save**.

Verify BGP route filtering configuration

Outlines procedure for verifying BGP route filter status, actions, route counts, and route table results across network tunnel groups. Also includes use of Secure Access Route Filters, NTG routing views, and audit logs to confirm filter propagation and identify denied routes.

Procedure

1. Navigate to **Connect** > **Traffic Management** > **Route Filters** > **Client Filters** > **or** > **Cloud Filters** to check the filter status after adding a new filter.

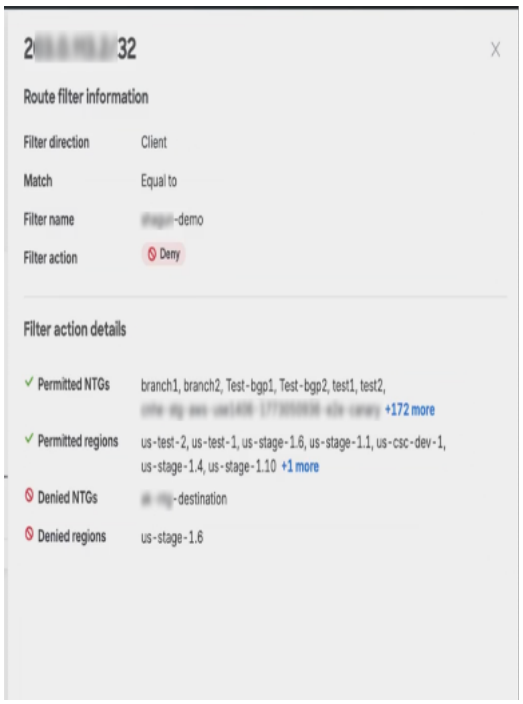
   The table lists the newly created filter. Hover over the respective subnet entry for the filter to view the status. The initial status shows as `In Progress, Filter is being created`.

   At this stage, you cannot edit the filter. You can either delete the filter or view the details. Click on the ellipses (...) on the right corner of the filter table to perform these actions, if required.

   After a few minutes, the filter status finally changes to `Active` when all the NTGs have the rule configured.

2. Click on the respective filter subnet listed in the Route Filters table to view the route filter information and filter action details.

   Figure 2: Route filter details



3. View Network Tunnel Group Details to check the pre- and post-filter route count for client or cloud routes.
4. Navigate to **Secure Access** > **Connections** > **Network Tunnel Groups** > **<NTG-name>** > **Routing** > **Client Routes** > **or** > **Cloud Routes** to verify if the intended prefixes are shown as allowed or denied in the route table per NTG.
5. Verify that the denied routes do not appear in the client or cloud route tables accordingly.

6. Use the audit and log features to verify filter propagation, especially after bulk changes or when route counts are unexpectedly low.

---

10 Network Tunnels by Device

Topics:

- Best Practices for Configuring Network Tunnels by Device
- Configure Tunnels with Cisco Catalyst SD-WAN
- Configure Automatic Tunnels with Catalyst SD-WAN
- Configure Tunnels with Cisco ISR
- Configure Tunnels with Cisco Adaptive Security Appliance
- Configure Tunnels with AWS Virtual Private Clouds and Elastic Compute instances
- Configure Tunnels with VeloCloud SD-WAN
- Configure Tunnels with Cisco Secure Firewall
- Configure Tunnels with Meraki MX
- Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels
- Configure Tunnels with NEC IX2000 Series Router
- Site-to-Site VPN tunnels with Microsoft Azure
- Configure a Site-to-Site VPN tunnel with Amazon Web Services

Provides an overview of Network Tunnels by Device in Cisco Secure Access, including Best Practices for Configuring Network Tunnels by Device, Configure Tunnels with Cisco Catalyst SD-WAN, and Configure Automatic Tunnels with Catalyst SD-WAN. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Best Practices for Configuring Network Tunnels by Device

Describes Best Practices for Configuring Network Tunnels by Device in Cisco Secure Access. You can establish an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel from a network device deployed in your environment to Cisco Secure Access.

You can establish an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel from a network device deployed in your environment to Cisco Secure Access. IPsec tunnels created for Secure Access accept traffic on all ports and protocols with a throughput of 1 Gbps per tunnel.

High availability

You must deploy both a primary and a backup tunnel to ensure high availability. If you configure only a primary tunnel, you will experience interruption of service during regular maintenance windows or unplanned outages.

Higher throughput

If you require more than 1 Gbps of throughput, you can set up multiple tunnels in a network tunnel group and join them with Equal-Cost Multi-Path (ECMP) routing.

Configure Tunnels with Cisco Catalyst SD-WAN

Explains the prerequisites and procedures for configuring network tunnels with Cisco Catalyst SD-WAN.

Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels. Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access. A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources.

Follow these steps to connect a Cisco IOS XE Catalyst SD-WAN device through an IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnel to Cisco Secure Access.

For more information about Cisco Catalyst SD-WAN devices and related topics, see Cisco's SD-WAN product documentation.

Before you begin

The following prerequisites must be met for the tunnel to work successfully.

- You must enable NAT in the interface feature template that faces the internet.
- You can access the Cisco Catalyst SD-WAN (Manager) console with a web browser. By default, the HTTPS port is 8443, but this may vary based on how your Cisco Catalyst SD-WAN (Manager) is configured.

  Note

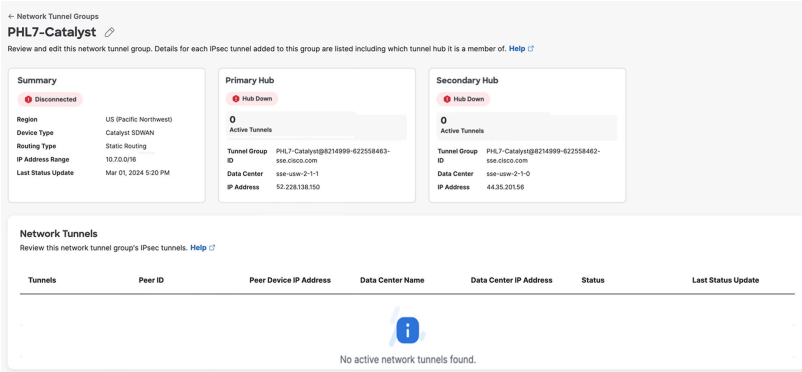
  If you get a "Not Secure" warning when accessing the link, you can ignore it. When the Cisco Catalyst SD-WAN (Manager) login screen appears, enter your credentials.

- An HSEC license is required to get high-throughput internet bandwidth for SLVPN tunnel setup. For more information, see Managing HSEC Licenses in Cisco Catalyst SD-WAN.

Procedure

1. Follow the steps in Add a Network Tunnel Group. Select **Static routing** under routing options. Only static routing is supported.
2. Make note of the **Tunnel ID** and **Passphrase** you enter when configuring the network tunnel group. These values are needed when you configure your Catalyst SD-WAN tunnel.

   The new network tunnel group appears in the Secure Access dashboard as **Disconnected**, and with the **Primary Hub** and **Secondary Hub** status showing as **Hub Down**. The network tunnel group status is updated once it is fully configured and connected with Catalyst SD-WAN.



3. Configure a Catalyst SD-WAN tunnel to connect a Catalyst SD-WAN device to Cisco Secure Access.

   In Cisco Catalyst SD-WAN Manager, all the features are configured through templates. Once the Cisco Catalyst SD-WAN devices are registered with Cisco Catalyst SD-WAN Manager, you cannot configure anything through the CLI.

   You can use the Cisco Catalyst SD-WAN Manager **Device** and **Feature** templates to establish a tunnel from the device. First define the device template and then the feature template.

   In SD-WAN Manager version 20.9, the SIG template is divided into several sections:

   a. Device Type, Template Name, Description, and SIG Provider (Umbrella, Zscaler, or Generic).

   > **Note**
   >
   > In version 20.4/17.4, the only two tunnel types that are offered are Umbrella and Third Party. You can configure Secure Access manual tunnels (IPSec or GRE) using the Third Party option. Starting in 20.5/17.5, the three tunnel types that are offered are Umbrella, Zscaler, and Generic. **To configure IPSec or GRE Secure Access tunnels, choose the Generic option.** You can configure Secure Access manual and automatic tunnels (IPSec or GRE) using the Generic option. Secure Access recommends you use automatic tunnels if available.

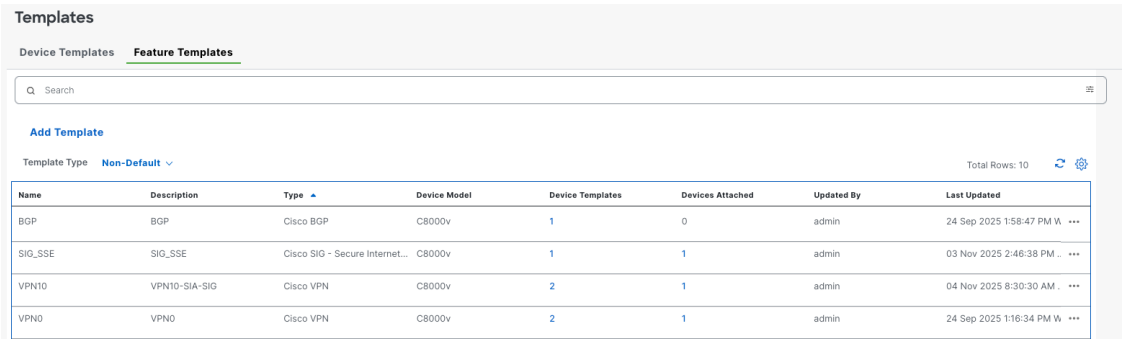
   b. Tracker: Allows you to configure custom L7 health check tracker information.

   c. Configuration: Allows you to specify different tunnel type (IPSec or GRE) and other tunnel characteristics, such as tunnel name, tracker name, tunnel source, whether the tunnel is attached to a primary or secondary data center (which is specified or discovered later) and advanced options, like IP MTU and other tunnel settings.

   d. High Availability: Allows you to choose up to 4 active tunnels or 4 active/standby tunnel pairs by choosing the tunnels defined in the Configuration section under the Active or Backup column. You can also modify traffic ratios for the tunnels.

4. Log into the Cisco Catalyst SD-WAN Manager console and navigate to **Configuration** > **Templates**.

5. Confirm that the **Feature Templates** tab is selected, then click **Add Template**.



6. Choose the device for which you are creating the template.
7. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
8. Under **SIG Provider** select **Device Types**, click the **Generic** radio button.



Trackers and Tunnel Health Monitoring

Trackers are a critical part of monitoring and maintaining overlay and SSE/SIG tunnel health on Cisco Catalyst SD-WAN. A tracker sends periodic probe packets (such as HTTP, ICMP, or DNS) towards a specified endpoint to determine reachability. When a tracker detects that its endpoint is unreachable, the SD-WAN control plan can withdraw routes or triggers failover actions to maintain service continuity. Trackers are used for interface reachability, static route tracking, service/SSE health, and SLA-based tunnel decisions.

Configuring Custom L7 Tracker URLs

Customers who require more granular SLA tracking (for example, monitoring a specific endpoint or cloud service) can define custom endpoint trackers specifying an L7 HTTP/HTTPS URL:

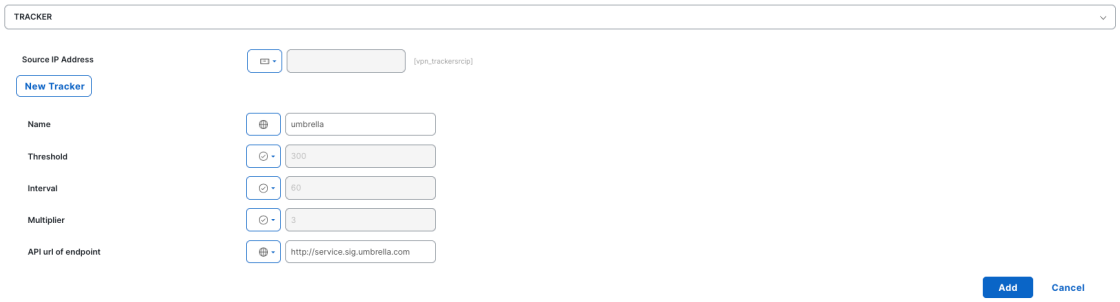
a. In Catalyst SD-WAN Manager, navigate to **Configuration** > **Feature Template** > **Secure Internet Gateway (SIG)**.

b. Click **New Tracker**.

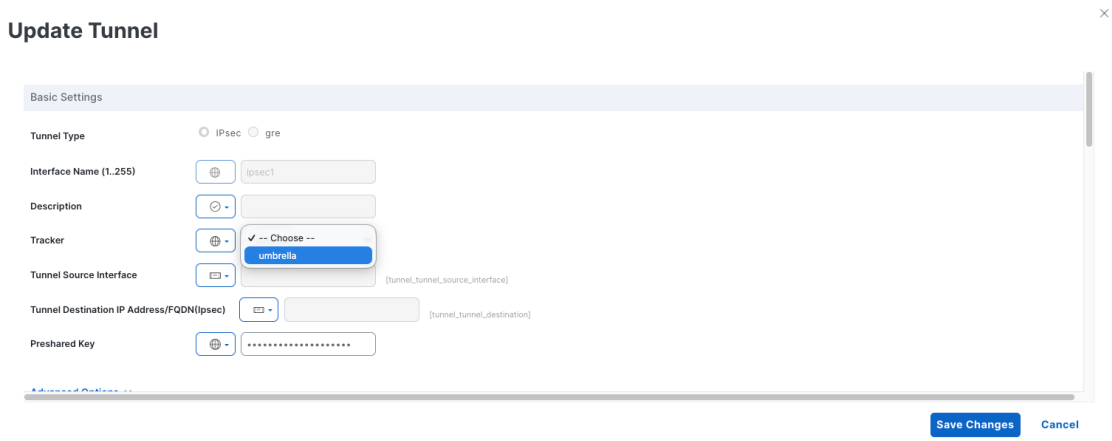
c. Enter a **Tracker Name**.

d. Adjust the **Threshold**, **Interval**, and **Multiplier** values as needed. Default values are selected by default.

e. In the API URL endpoint, enter the **API URL** for the SIG endpoint of the tunnel.



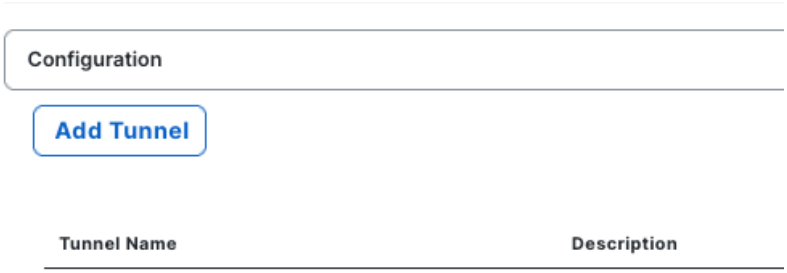
f. Choose **Tracker** from the drop-down list and enter the tracker configuration details.



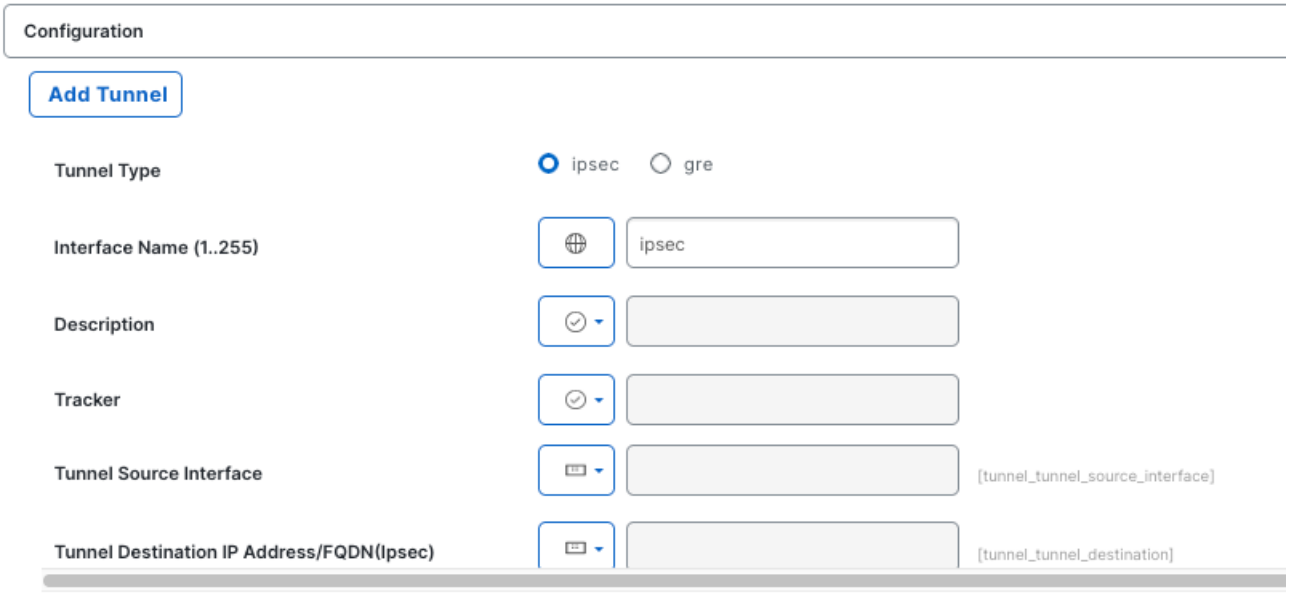
g. Click **Save Changes**.

For more information on how Catalyst SD-WAN tracker work and their use cases, see Understand Catalyst SD-WAN Tracker Usability and Use Cases.

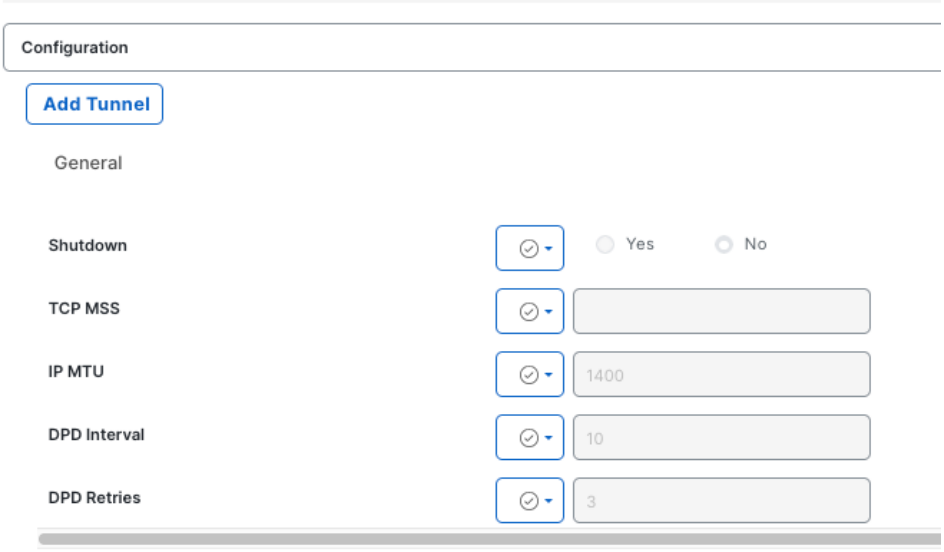
9. Under Configuration, click **Add Tunnel** .



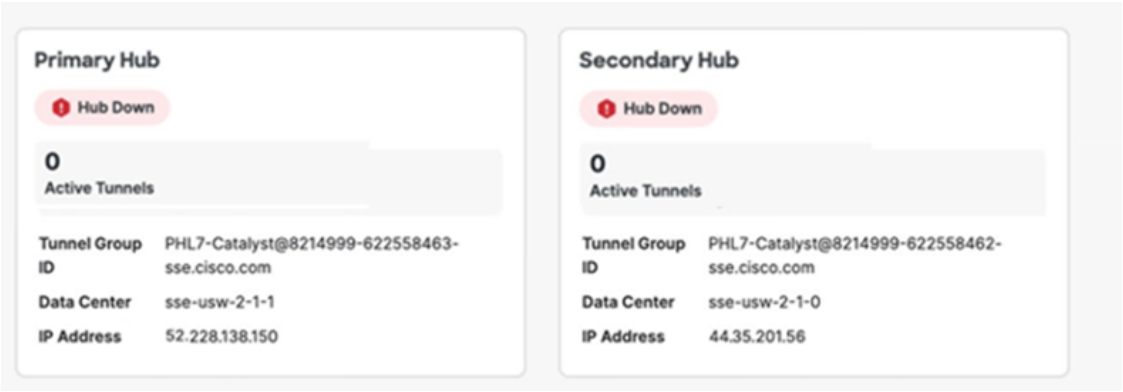
a) Choose the **Tunnel Type** radio button for the tunnel.
b) Enter the **Interface Name** from 1 to 255. For example: `ipsec1`.
c) Optionally, choose a **Tunnel Description** for the Tunnel interface.
d) Optionally, select the **Tracker** for the tunnel interface.
e) Set the **Tunnel Source Interface**. This must be the WAN interface in VPN 0, which has the internet connectivity.
f) Set the **SIG Tunnels Destination** to the closest data center.
g) Enter the **Preshared Key** from SSE.



10. Under General configuration, the **Shutdown** option is set to the **NO** radio button by default.

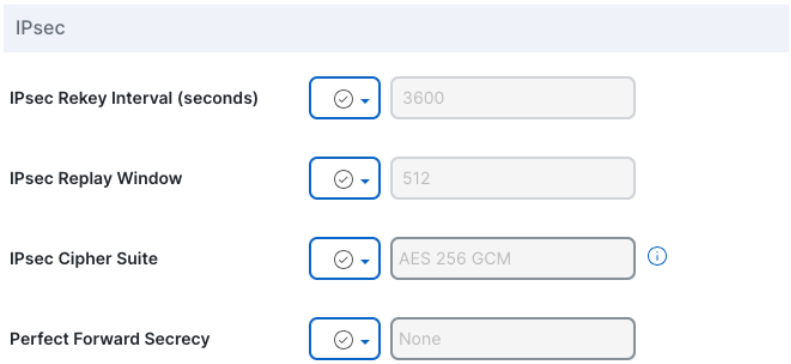


11. Choose the **Global Attribute** to change IKE defaults:
    a) **IKE Rekey Interval**: Set to `28800`.
    b) **Cipher Suite**: Leave default option unchanged, `AES-256-CBC-SHA1`.
    c) **IKE DH Group**: Set to `14 2048-bit Modulus`.
    d) **IKE ID for Remote End point**: IP address of Secure Access Data Center that is `52.228.XX.XXX`, `44.35.XXX.XX`
    e) **IKE ID for local End point**: Tunnel Group ID on SSE page.

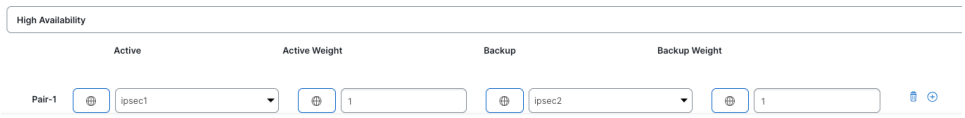


12. Choose the **Global Attribute** to change IPsec defaults:
    a) **IPsec Rekey Interval & Replay Window**: Leave defaults unchanged.
    b) **Cipher Suite**: Leave default option unchanged, `AES 256 GCM`.
    c) **Perfect Forward Secrecy**: Set to `NONE`.

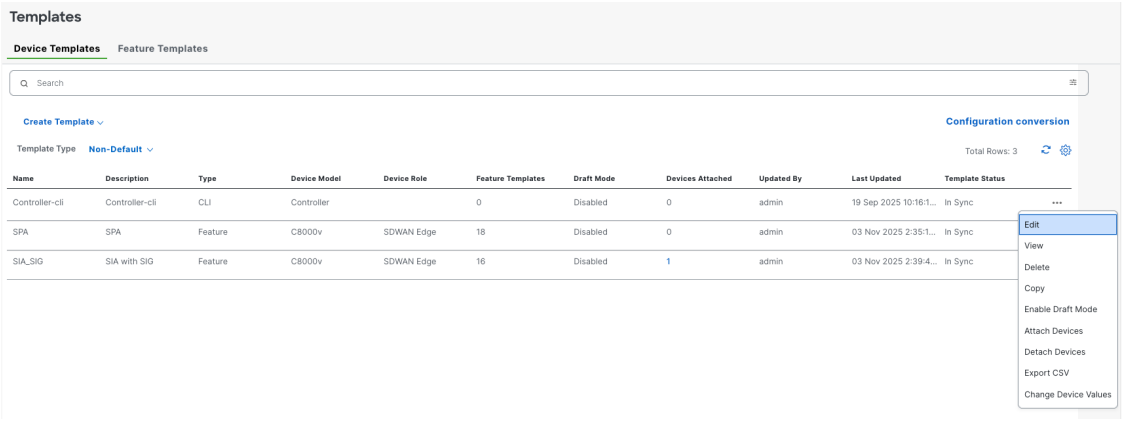
> **Tip**
>
> **Cipher Suite Encryption**
>
> If performance is an issue with the default cipher, both `AES 256 CBC SHA1` and `Null SHA1` are also supported. You can test these to determine whether one offers better performance for a particular platform. Note that `Null SHA1` isn't necessarily faster than the default `AES 256 GCM` because of the cost of the SHA1 hashing. In addition, `Null SHA1` is not recommended due to security concerns of unencrypted transport.



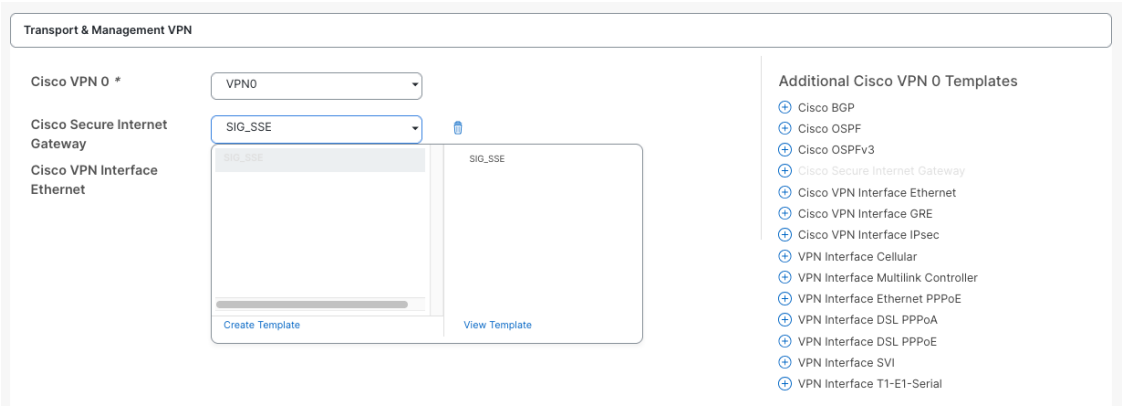
13. Under High Availability, select **Active** and **Backup** tunnel interface from the drop-down list.



14. Click **Save** to configure the template.
15. Add the **Cisco SIG** template: Navigate to **Configuration** > **Templates** > **Device**, then choose the device template for the CDFW tunnel.
16. Select **Edit** from the rightmost dropdown menu.

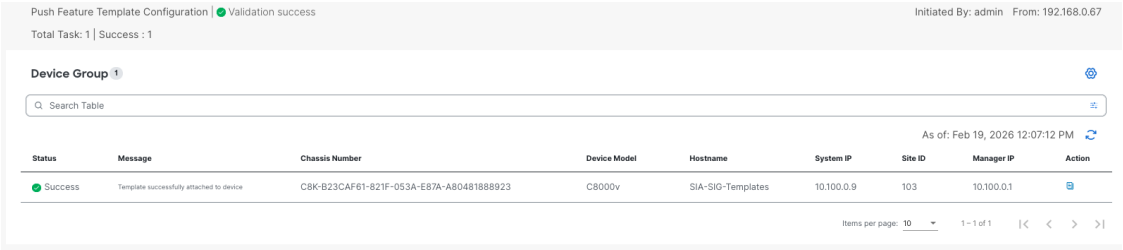


17. Add the **Cisco SIG** template in the **VPN 0 Transport & Management VPN** section. Choose the **VPN Interface IPSec** that you added as part of the feature template.

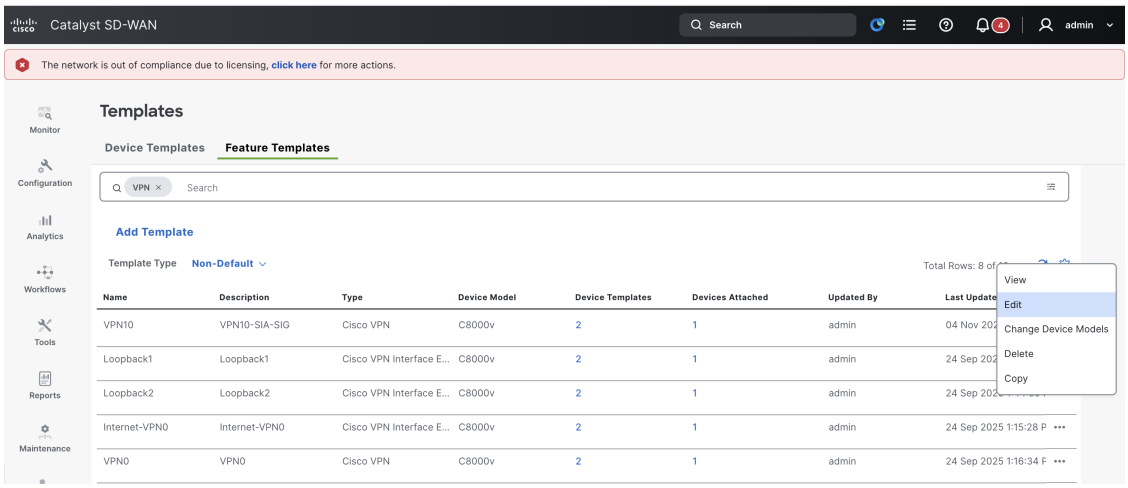


18. Click **Update**.

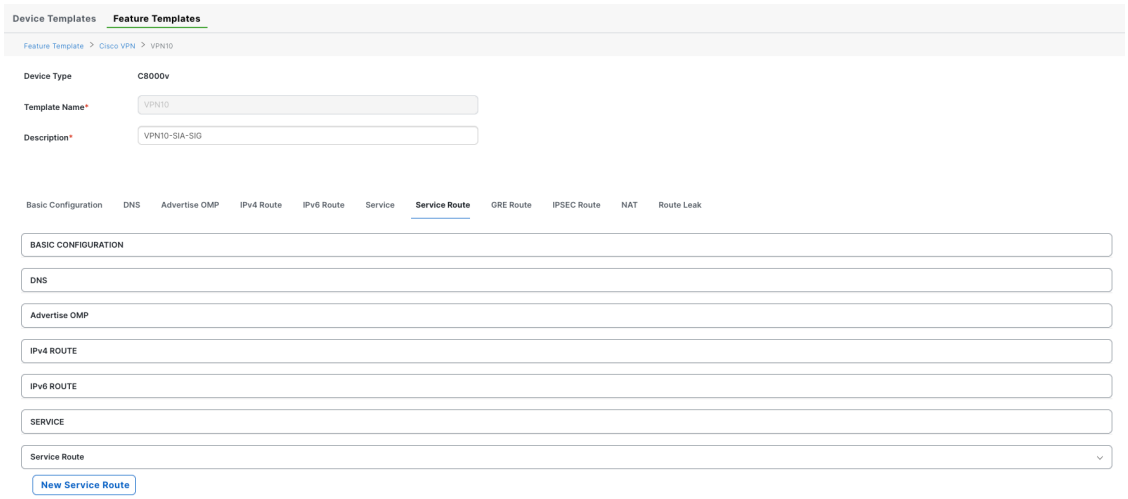
    A success message appears.



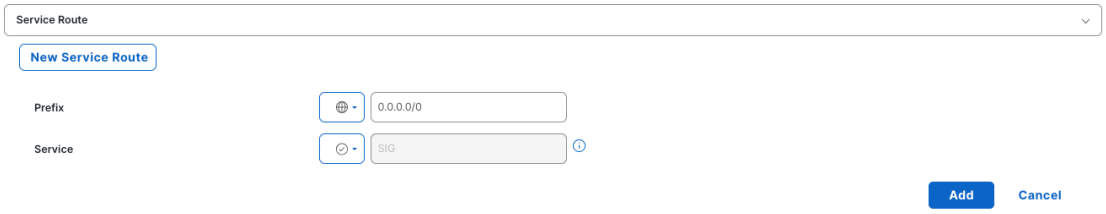
19. **Add static routes** from the service VPN to redirect the traffic through the IPSec tunnel to CDFW headend: Navigate to **Configuration** > **Templates** > **Feature Templates**.
20. Right-click the right most column of the Service VPN template, and **Edit** the template to add **SIG service route**.



21. Click **New Service Route**.



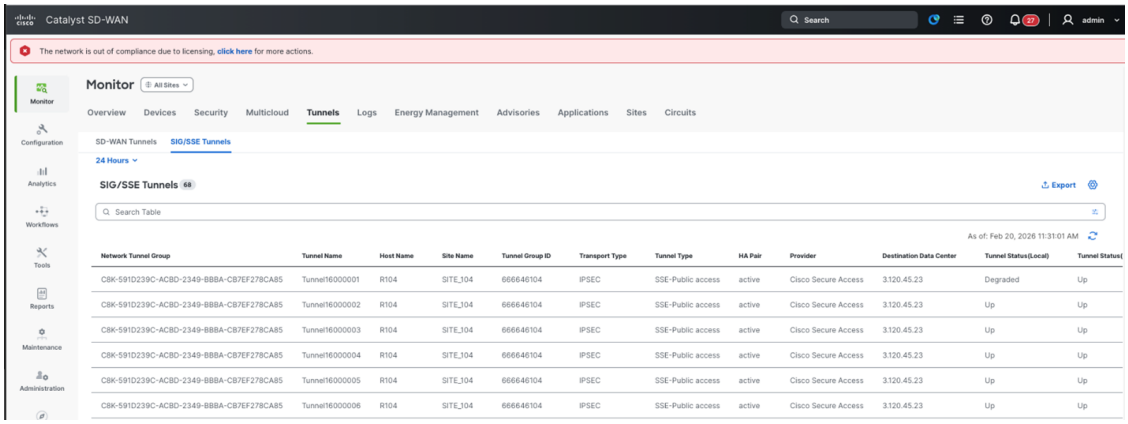
In this example, the default route is set to the **SIG** tunnel interface.



22. Verify the Tunnel Status in the Cisco Catalyst SD-WAN Manager Console.

a) Log in to the Cisco Catalyst SD-WAN Manager console.
b) Navigate to **Monitor** > **Tunnels**.
c) Click the **SIG/SSE Tunnels** tab.

You can view the tunnel status.



Configure Automatic Tunnels with Catalyst SD-WAN

Understand how to use Cisco Catalyst SD-WAN automation to integrate with Cisco Secure Access for branch-to-internet secure direct internet access (SIA).

Cisco Catalyst SD-WAN integrates with Cisco Secure Access for a branch-to-internet Secure Direct Internet Access (DIA) scenario, using Cisco Catalyst SD-WAN Manager automation. Cisco Secure Access compiles the IPsec configuration, including the tunnel destination for the device, based on the device's public IP address in the public interface of the SD-WAN router. This IP address is periodically communicated by the device to the Cisco Catalyst SD-WAN Manager.

Note that the device does not make API calls directly to Secure SD-WAN Edge (SSE). It communicates with Cisco Catalyst SD-WAN Manager.

Supported Features

- Supported only in SD-WAN (Software-Defined Wide Area Network) mode UX2.0.
- Compatible with device versions 20.13.1/17.13.1a

For more information about Cisco SD-WAN devices and related topics, see Cisco's SD-WAN product documentation.

For an additional example that includes ECMP configuration, see *Configure Secure Access with SD-WAN Automated Tunnels for Secure Internet Access*, https://www.cisco.com/c/en/us/support/docs/security/secure-access/225416-configure-secure-access-with-sd-wan.html.

Configure Cisco Catalyst SD-WAN Manager Templates

In Cisco Catalyst SD-WAN Manager, all the features are configured through templates or configuration groups. After the cEdge devices are registered with Cisco Catalyst SD-WAN Manager, you cannot configure anything through the CLI.

Enable DNS resolution

Provides instructions for completing the Enable DNS resolution workflow in Cisco Secure Access. Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.

To enable DNS resolution in the Edge device, use the IP Domain Lookup setting command. Perform this configuration in the **Global Parcel** section of the configuration group.

Before you begin

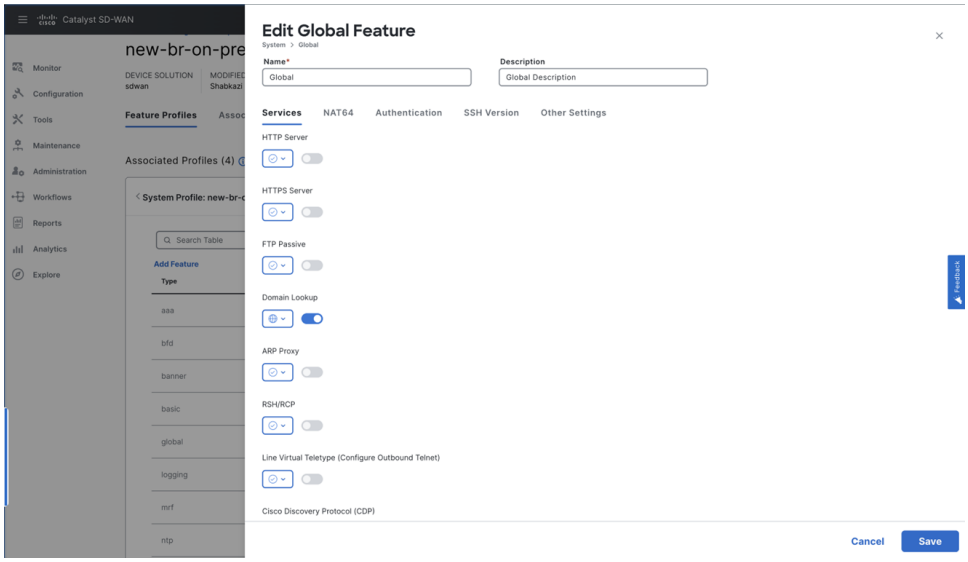
- Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.

- Confirm that DNS is configured in VPN0 for both the device and Cisco Catalyst SD-WAN Manager to enable internet access.
- Enable ip-domain-lookup in the device. This feature is disabled by default.
- Make sure that NAT is enabled in the device's internet facing interface.
- Verify that the SSE Network Tunnel Group (NTG) is enabled with NAT functionality.
- Confirm that API credentials have write access to perform the necessary operations.

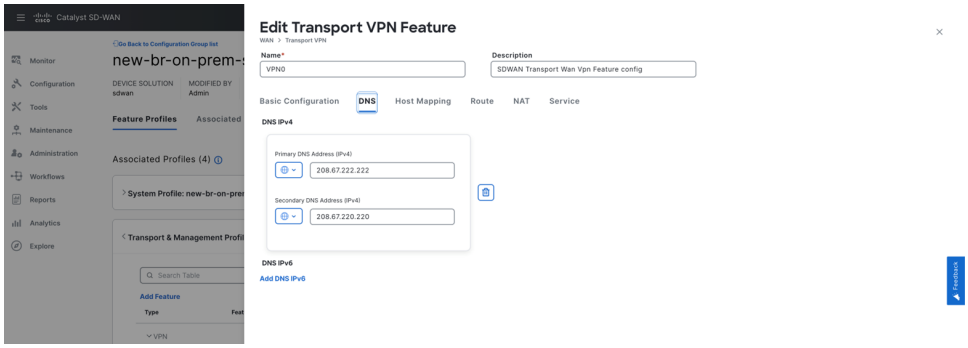
> **Note**
>
> Perform all the configuration changes through Cisco Manager. Configuration synchronization from SSE to Cisco Manager is not supported.

Procedure

1. Navigate to **Configuration Group** > **System** > **Global**.
2. Click **Edit** to open the **Edit Global Feature** dialog box.
3. Click the **Services** tab.
4. Enable the **Domain Lookup** option.
5. Click **Save**.



6. Under **Transport & Management Profile** > **Transport VPN**, enter the Primary and Secondary DNS addresses in the **DNS** section.



Configure API credentials in SD-WAN Manager

Provides instructions for completing the Configure API credentials in SD-WAN Manager workflow in Cisco Secure Access. Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.

Before you begin

- Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.
- Confirm that DNS is configured in VPN0 for both the device and Cisco Catalyst SD-WAN Manager to enable internet access.
- Enable ip-domain-lookup in the device. This feature is disabled by default.
- Make sure that NAT is enabled in the device's internet facing interface.
- Verify that the SSE Network Tunnel Group (NTG) is enabled with NAT functionality.
- Confirm that API credentials have write access to perform the necessary operations.
- Create the required Cisco Secure Access credentials from the Secure Access portal. For detailed steps on creating a Cisco Secure Access account, see Add Secure Access API Keys.

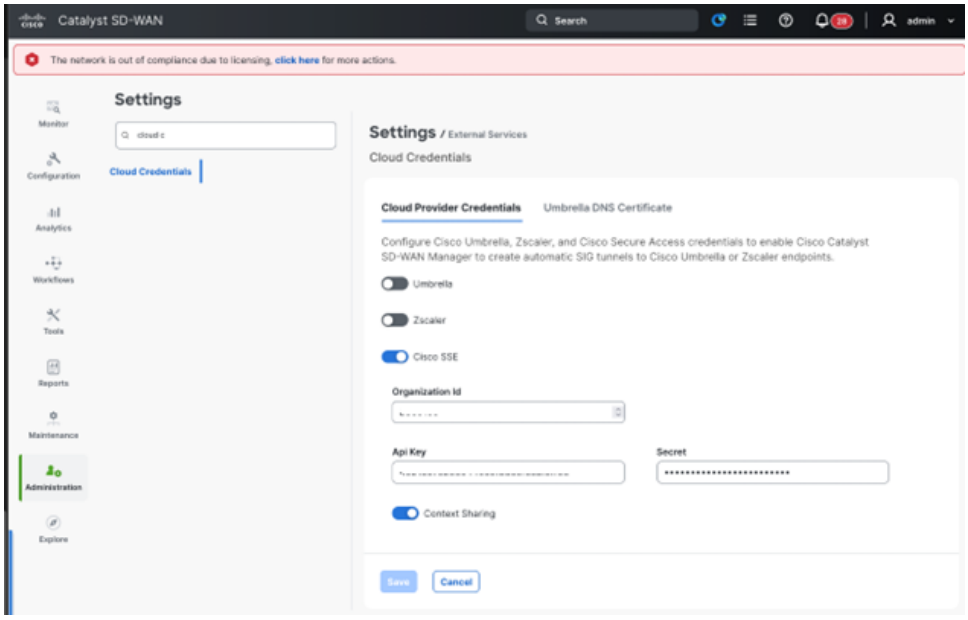
Note

Perform all the configuration changes through Cisco Manager. Configuration synchronization from SSE to Cisco Manager is not supported.

Procedure

1. Log in to **Cisco Catalyst SD-WAN** Manager.
2. Navigate to **Administration** > **Settings**.

   The **Cloud Provider Credentials** tab is selected by default.
3. Enable the **Cisco SSE** toggle button.
4. Enter your Secure Access **Organization Id**, **Api key**, and **Secret**.
5. Enable the **Context Sharing** toggle button to exchange information with SSE.
6. Click **Save**.



Create the Cisco Secure Access policy to be configured in the SD-WAN branches

Provides instructions for completing the Create the Cisco Secure Access policy to be configured in the SD-WAN branches workflow in Cisco Secure Access. Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.

> **Note**
>
> Cisco Secure Access is available only for devices configured using configuration groups. This is a new method for provisioning devices.

Policy groups enable you to configure and deploy policies to SD-WAN branches using a workflow-based process. Perform this procedure to create a new policy group and configure Cisco Secure Access.

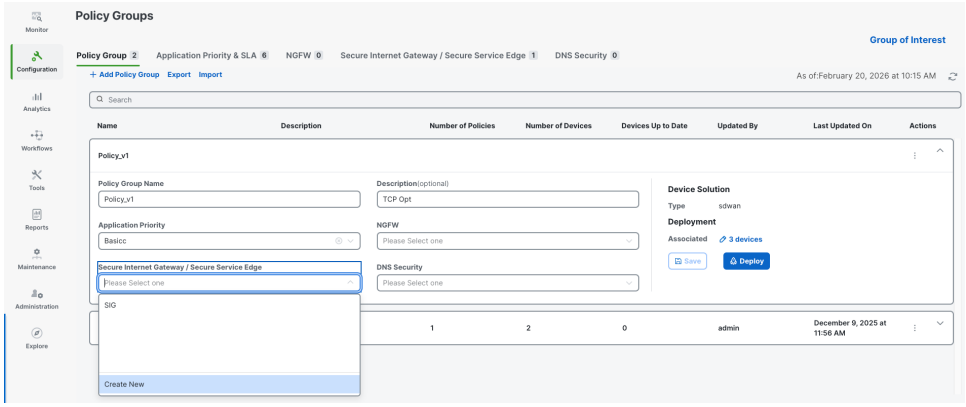
Before you begin

- Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.
- Confirm that DNS is configured in VPN0 for both the device and Cisco Catalyst SD-WAN Manager to enable internet access.
- Enable ip-domain-lookup in the device. This feature is disabled by default.
- Make sure that NAT is enabled in the device's Transport Locator interfaces.
- Verify that the Secure Service Edge (SSE) organization is enabled with NAT functionality.
- Confirm that API credentials have write access to perform the necessary operations.

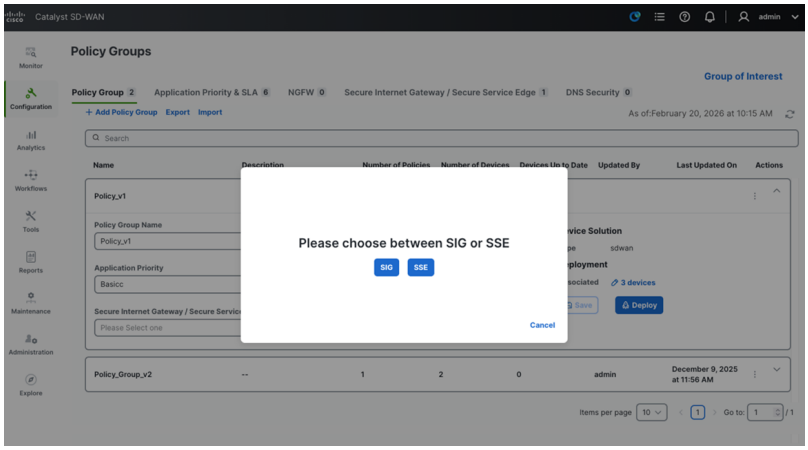
> **Note**
>
> Perform all the configuration changes through Cisco Manager. Configuration synchronization from SSE to Cisco Manager is not supported.

Procedure

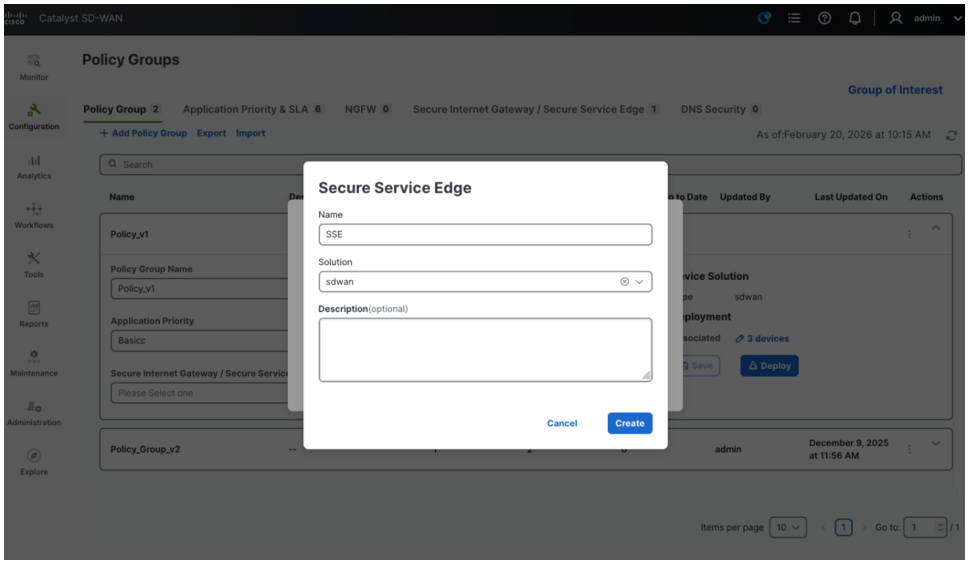
1. From the Cisco Catalyst SD-WAN Manager dashboard, navigate to **Configuration** > **Policy Group**.
2. Under the **Policy Group** tab, click **Add Policy Group**.
3. Enter a **Policy Group Name** and optionally, provide a description.
   - **Policy Group Name**: Specify the name of the policy group. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or other characters.
   - **Description**: (Optional) Provide a description for the policy group. It can contain up to 2048 characters, including spaces.
4. From the **Secure Internet Gateway / Secure Service Edge** drop-down menu, choose **Create New**.



5. In the window that appears, click **SSE**.

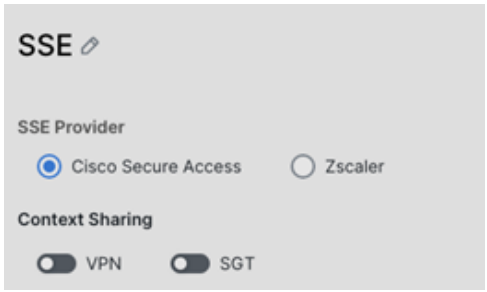


The Secure Service Edge window appears.



a) Enter a policy **Name**.
b) From the **Solution** drop-down list, choose **SD-WAN**.
c) Click **Create**.

6. Optionally, enable the **VPN** toggle button or the **SGT** toggle button for context sharing.



7. Configure trackers to monitor tunnel health.
   a. Enter the **Source IP address** for the probe packets.
   b. Click **Add Tracker**.



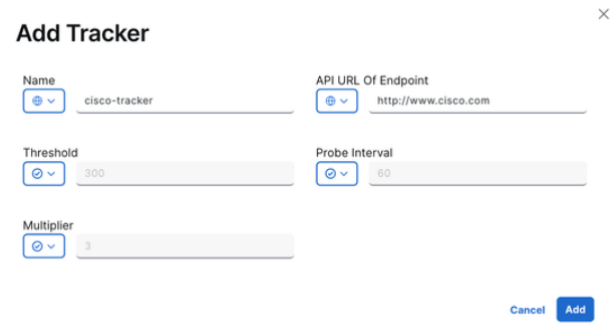
   c. Configure the SSE tracker URL parameters and do the following:

      For SSE and SIG tunnel use cases, Catalyst SD-WAN uses a default endpoint tracker when SSE is enabled:

      - **Tracker Name**: Default Tracker
      - **Default Endpoint URL**: http://service.sig.umbrella.com
      - **Endpoint Type**: API_URL
      - **Threshold (latency)**: 300 ms
      - **Interval and Multiplier**: 60s and 3 retries

      For more information, see Tracker Parameters.

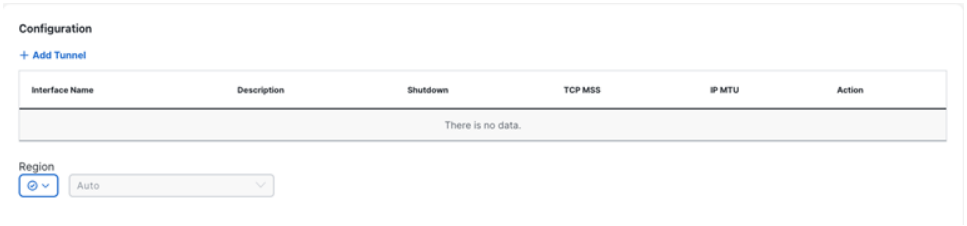
> **Note**
>
> The default tracker only checks connectivity to the Secure Service Edge (SSE). You can configure a custom tracker to test specific services or web pages.



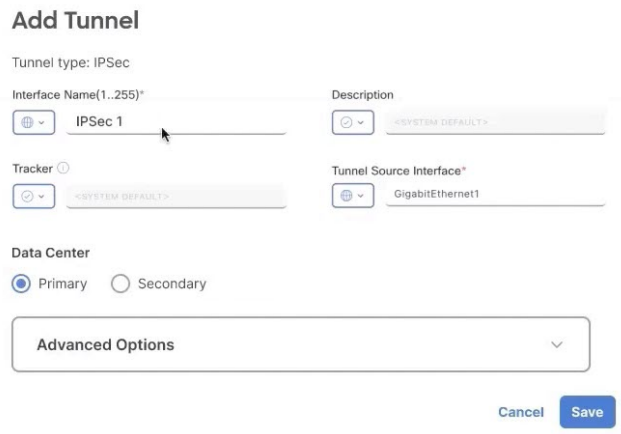
d. Click **Add**.

8. Configure tunnels.

a. Click **Add Tunnel**.



b. In the **Add Tunnel** dialog box, configure the **Basic Settings**. See Configure Secure Service Edge .



> **Note**
>
> The system supports 16 tunnels in total. This capacity includes eight active tunnels and eight backup tunnels.

> **Note**
>
> When you select the Auto option, the system uses the nearest SSE region to build tunnels.

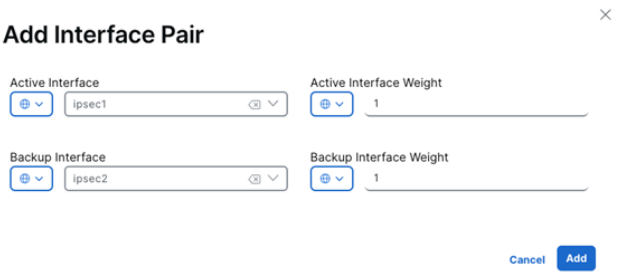
c. Click **Save**.

9. Configure High Availability.

a. Click **Add Interface Pair**.



b. Select **Active** and **Backup** Interface.



c. Click **Add** to save your changes.

Deploy the Cisco SSE policy to be configured in SD-WAN branches

Provides instructions for completing the Deploy the Cisco SSE policy to be configured in SD-WAN branches workflow in Cisco Secure Access. Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.

After the tunnels and policy-group configuration are set up, deploy the policy.

Before you begin

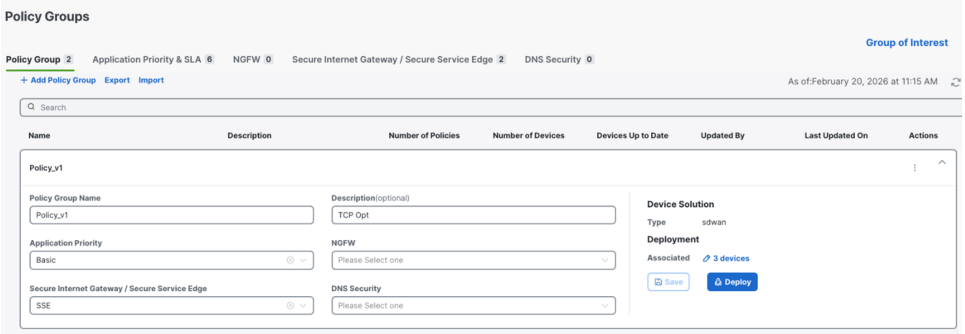
- Ensure that internet access for Cisco Catalyst SD-WAN Manager (controller-based automation) supports both proxy and nonproxy modes.
- Confirm that DNS is configured in VPN0 for both the device and Cisco Catalyst SD-WAN Manager to enable internet access.
- Enable ip-domain-lookup in the device. This feature is disabled by default.
- Make sure that NAT is enabled in the device's Transport Locator interfaces.

- Verify that the SSE organization is enabled with NAT functionality.
- Confirm that API credentials have write access to perform the necessary operations.

> **Note**
>
> Perform all the configuration changes through Cisco Manager. Configuration synchronization from SSE to Cisco Manager is not supported.

Procedure

1. Click **Deploy** to select sites and deploy the policy group.



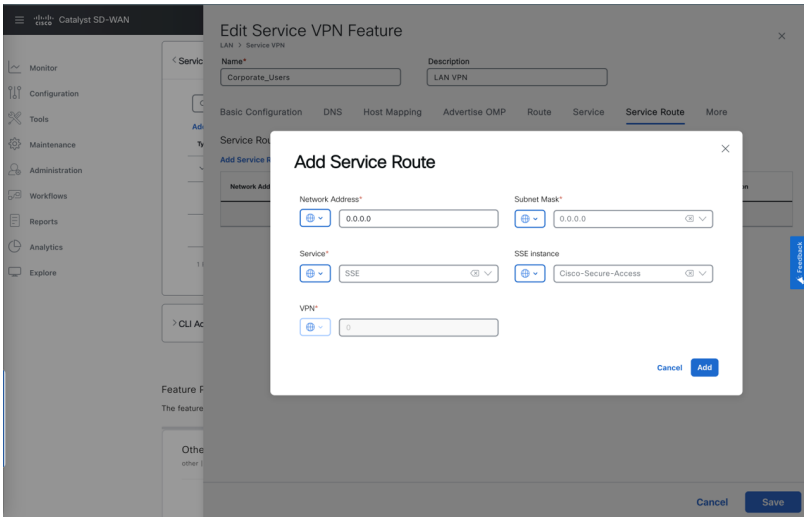
2. Add a service route for traffic redirection. The traffic is routed via the tunnels in two ways :
   - Route-Based Redirection (Using Service Routes in a VPN)
   - Policy-Based Redirection (Using Application Priority & SLA Policy)
   - Command Line Interface (CLI) Commands

Route-Based Redirection (Using Service Routes in a VPN)

Provides instructions for completing the Route-Based Redirection (Using Service Routes in a VPN) workflow in Cisco Secure Access. Navigate to the Configuration Group settings to access the specific Service VPN feature you wish to modify (example: "Corporate_Users").

Procedure

1. Navigate to the **Configuration Group** settings to access the specific **Service VPN** feature you wish to modify (example: "Corporate_Users").
2. Click the **Service Route** tab.
3. Click **Add Service Route** to open the configuration dialog for adding a new service route.
4. Enter the details in **Add Service Route**:
   a) Enter the **Network Address** and **Subnet Mask** for the traffic you want to redirect.
   b) From the **Service** drop-down list, choose SSE.
   c) From the **SSE instance** drop-down list, choose **Cisco-Secure-Access**.
   d) Enter the **VPN ID** associated with this service route.
   e) Click **Add** to add this configured route and click **Save**.



Deploy the configuration group with the new changes.

Policy-Based Redirection (Using Application Priority and SLA Policy)

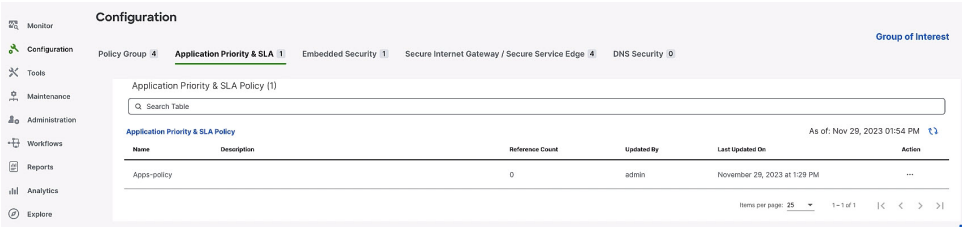
Provides instructions for completing the Policy-Based Redirection (Using Application Priority and SLA Policy) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

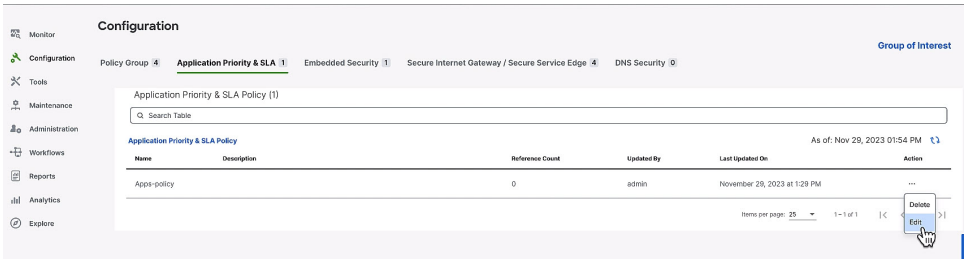
Procedure

---

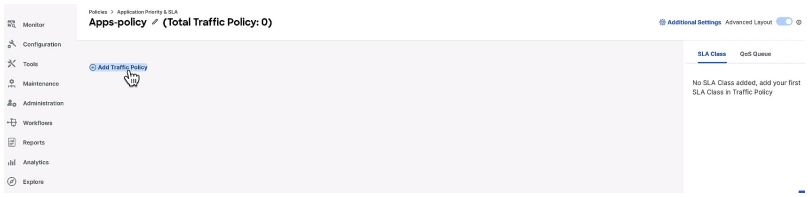
1. Choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.



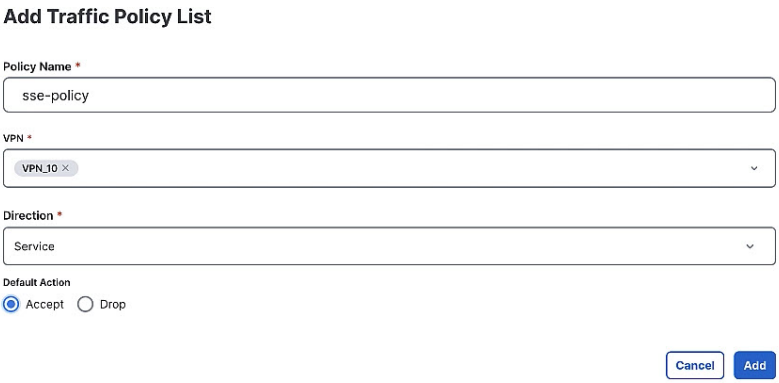
2. If you are using an existing policy, click the ellipsis (**...**), in the **Action** column for the policy and then select **Edit**.



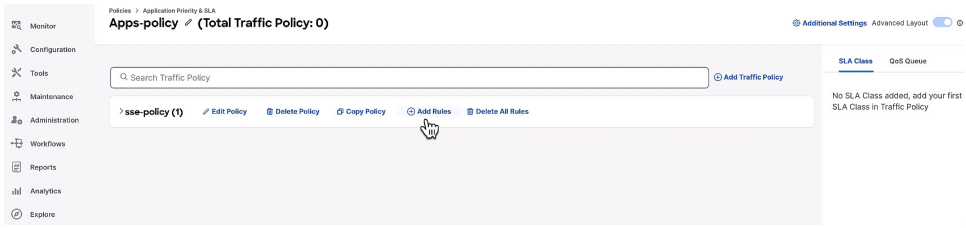
3. Click **Add Traffic Policy**.



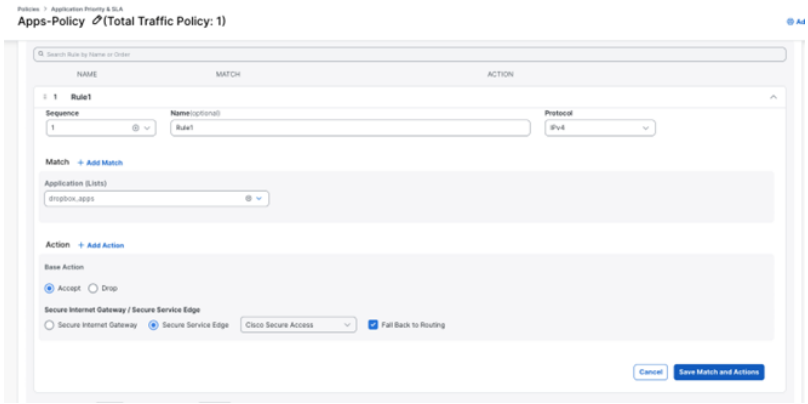
4. In the **Add Traffic Policy List** dialog box, enter the **Policy Name**, **VPN**, **Direction** and **Default Action**.



5. Click **Add** to create the traffic policy.
6. Click **Add Rule**.



7. Configure **Sequence** and provide a **Name** for the rule.
8. Specify the **Protocol** and define the **Match criteria**.
   a) Match criteria specify the traffic you want to redirect.
   b) Select **Accept**.
   c) Select **Secure Service Edge**, under **Add Action**.
   d) (Optional) Check the **Fail Back to Routing** check box to direct traffic to follow the regular routing table when the tunnel is not available.
   e) Click **Save Match and Actions**.



Deploy the configuration group with the new changes.

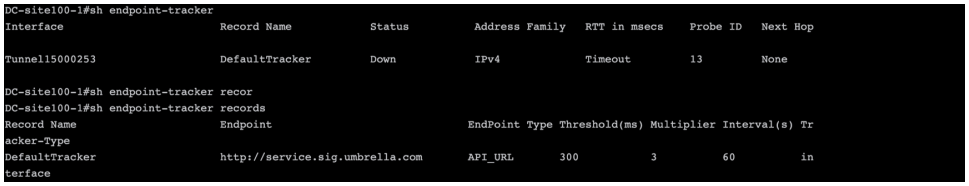
Tunnel Status Verification Using CLI Commands

This concept explains how you use the following command to verify tunnel status through the Command Line Interface, enabling you to confirm tunnel state, tracker health, and overall connectivity in an SD-WAN environment.

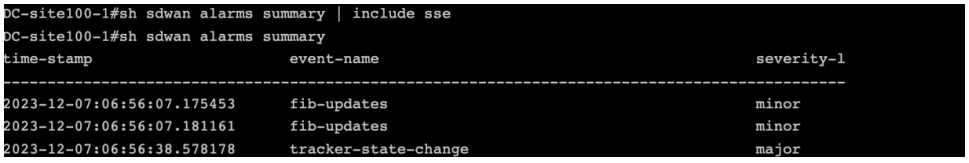
Use the `show sse all` CLI command to display Secure Service Edge (SSE) tunnel information. This command provides tunnel details, status, and service route mappings in a single view.

```
Hub2-SIG#show sse all
**************************************
SSE Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel16000001
Site id: 2
Tunnel id: 655184839
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 44.217.195.188
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

Use the `show endpoint-tracker` command to verify the health of endpoint tracking probes. These probes monitor Layer seven reachability to a defined endpoint and directly influence tunnel health for Secure Service Edge connections.



Use the `show sdwan alarms summary` command to view a consolidated list of active and historical SD-WAN system alarms. These alarms indicate control planes, data planes, or service-level events that affect device operation, including Secure Service Edge.



Use the `show sdwan alarms detail` command to view **detailed information for a specific SD-WAN alarm**.

```
show sdwan alarms detail
alarms 2023-12-05:01:42:11.576526
 event-name     sse-tunnel-params-absent
 severity-level major
 host-name      vm5
 kv-pair        [ system-ip=172.16.255.15 if-name=TunnelSSE
wan-if-ip=128.107.253.181 ]
```

Use the `show ip http client all` to verify and audit **outbound HTTP and HTTPS requests initiated by the device itself**.

This command does not display user traffic. It displays control-plane and management-plane HTTP client activity generated by the router.

```
show ip http client all
 HTTP client history:
 GET 18:24:00 UTC Fri Dec 1 2023  myipv4.p1.opendns.com/get_my_ip
```

Use the `show crypto session` command to verify the IPsec and IKEv2 state of the SSE tunnel.

```
Show crypto session
Interface: Tunnel15000010
Profile: if-ipsec10-ikev2-profile
Session status: UP-ACTIVE
Peer: 3.76.88.203 port 4500
  Session ID: 7
  IKEv2 SA: local 10.1.15.15/4500 remote 3.76.88.203/4500 Active
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Use the `show ip interface brief` command to verify the operational state of interfaces.

```
show ip interface brief
Tunnel15000010         10.1.15.15      YES TFTP   up    up
```

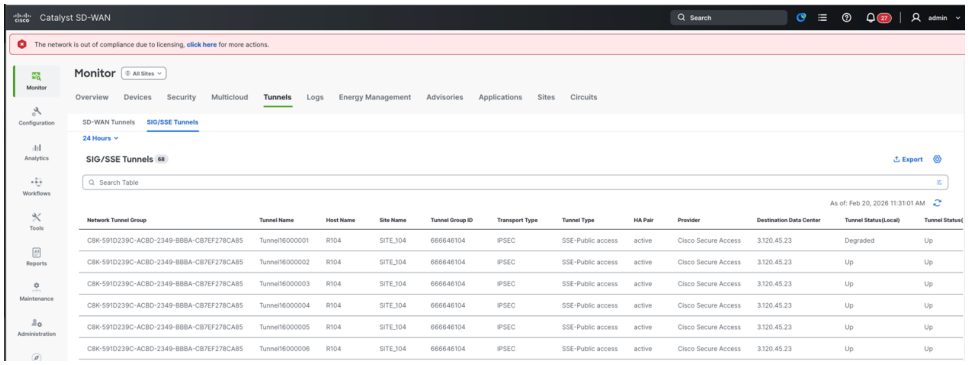
Verify the Tunnel Status in the SD-WAN Manager Console

Provides instructions for completing the Verify the Tunnel Status in the SD-WAN Manager Console workflow in Cisco Secure Access. Log in to the Cisco Catalyst SD-WAN Manager console.

Procedure

1. Log in to the Cisco Catalyst SD-WAN Manager console.
2. Navigate to **Monitor** > **Tunnels**.
3. Click the **SSG/SSE Tunnels** tab.

   You can view the tunnel status.

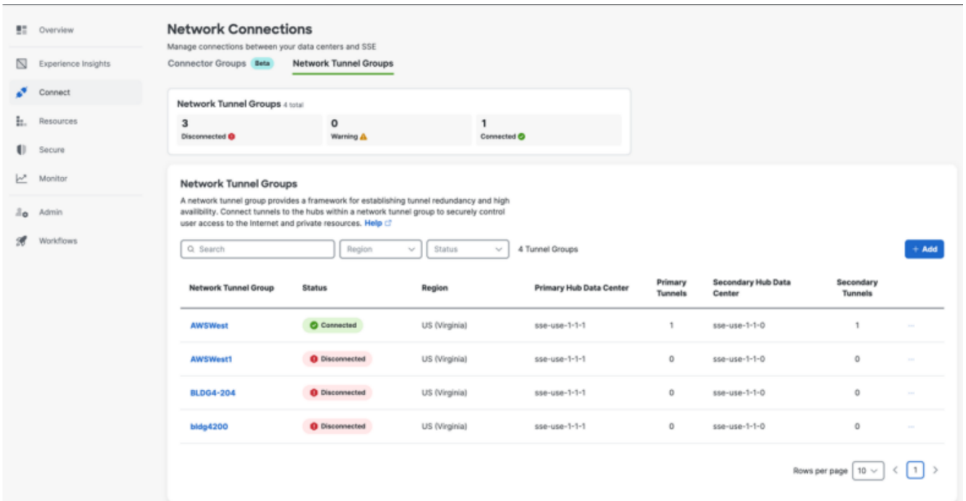


Verify the Tunnel Status in Secure Access Dashboard

Provides instructions for completing the Verify the Tunnel Status in Secure Access Dashboard workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to the Secure Access dashboard.
2. Select the **Connect** menu and click **Network Tunnel Groups** tab.
3. View the **Network Tunnel Groups** summary section. This section displays:
   - The number of tunnel groups that are disconnected.
   - The number of tunnel groups with a warning.
   - The number of tunnel groups that are connected.
4. Scroll down to the detailed **Network Tunnel Groups** table.
5. Locate each tunnel group listed by name.
6. Check the **Status** column. It displays if the tunnel group is connected or disconnected.
7. Check the **Primary Tunnels** and **Secondary Tunnels** columns to see the number of active tunnels for each group.For example, you see that the **AWSWest** tunnel group status is **Connected** and has one primary tunnel and one secondary tunnel. Three other tunnel groups show as "Disconnected" with zero primary and zero secondary tunnels.



You can use this dashboard to monitor tunnel connectivity and redundancy across your organization.

Configure Tunnels with Cisco ISR

Understand how to connect a Cisco ISR-G2, ISR4K, or CSR router through both primary and secondary IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels to Cisco Secure Access.

Follow the steps in this guide to connect a Cisco ISR-G2, ISR4K, or CSR router through both primary and secondary IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels to Cisco Secure Access.

Before you begin

The following prerequisites must be met for the tunnels to work successfully.

- A valid Cisco Secure Access account.
- A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.

- A router (ISR-G2, ISR4K, or CSR) with a security K9 license to establish an IPsec tunnel.

> **Note**
>
> An HSEC license is required to get high-throughput internet bandwidth for SLVPN tunnel setup.

- A Secure Access data center IP address to use when creating the IPsec tunnel. In the sample commands, `<sse_dc_ip>` refers to this IP address. We recommend choosing the IP address based on the data center located closest to your device.
- Open UDP ports 500 and 4500 before connecting to the tunnel.

> **Note**
>
> Cisco router (ISR-G2, ISR4K, or CSR) devices do not require public static IPv4 addresses configured on the interface that connects to the public internet and Secure Access. You can deploy these devices behind a NAT device. This is because we can specify a text as its IKE ID. This ID in combination with the PSK is used to successfully authenticate the Cisco router (ISR-G2, ISR4K, or CSR) devices with Secure Access.
>
> Text as an IKE ID also allows multiple tunnels to be established from the same Cisco router device with a single IP address. This provides an opportunity to increase bandwidth by increasing the number of tunnels.

Procedure

1. Follow the steps in Add Network Tunnel Group.

   The new tunnel appears in the Secure Access dashboard with a status of *UnEstablished*. The tunnel status is updated once it is fully configured and connected with the Cisco ISR.

Follow these steps to connect the Cisco ISR (G2, 4K) or CSR router to Secure Access.

2. Configure the IKEv2 proposal.

   ISR routers support a default proposal and policy for IKEv2, with a predefined encryption, integrity, and DH group. These values change across different software versions. You can either use the default proposal or you can create your own proposal. Your proposal needs to be attached to the policy with matching parameters. Create an IKEv2 keyring profile and configure the peer address and pre-shared key, associate the keyring profile to the IKEv2 profile, set the local identity as email and configure the IKE ID (email) which you get from the Tunnel Configuration dashboard.

   For example, the default IKE proposal of an ISR running 16.11.01a:

```
ISR-4221#sh ver
Cisco IOS XE Software, Version 16.11.01a

ISR-4221#show crypto ikev2 proposal sse-prop
 IKEv2 proposal: sse-prop
     Encryption : AES-GCM-256
     Integrity  : none
     PRF        : SHA256
     DH Group   : DH_GROUP_256_ECP/Group 19 DH_GROUP_384_ECP/Group 20
```

3. Define the IKEv2 Keyring and IKEv2 profile.

Create your IKEv2 keyring and IKEv2 profile with the [sse_dc_ip] of the Secure Access data center closest to your location. Then associate the IKEv2 keyring to the IKEv2 profile.

Replace [Portal_Tunnel_ID] and [Portal_Tunnel_Passphrase] with the Tunnel ID and Passphrase you configured in section Add Network Tunnel Group.

```
crypto ikev2 keyring sse-kr
  peer sse
  address \[sse_dc1_ip\]
  pre-shared-key \[sse-tunnel-psk\]
!
  peer sse-2
  address \[sse_dc2_ip\]
  pre-shared-key \[sse-tunnel-psk\]
!
crypto ikev2 profile sse-ikev2-profile-tunnel-1
  match identity remote address \[enter the specific DC IP from the tunnel
group in Secure Access\]
  identity local email \[sse-email\]
  authentication remote pre-share
  authentication local pre-share
  keyring local sse-kr
  dpd 10 3 periodic
!
crypto ikev2 profile sse-ikev2-profile-tunnel-2
  match identity remote address \[enter the specific DC IP from the tunnel
group in Secure Access\]
  identity local email \[sse-email\]
  authentication remote pre-share
  authentication local pre-share
  keyring local sse-kr
  dpd 10 3 periodic
```

4. Define the IPSec transform-set, profile, and policy.

   Create the transform-set and IPsec profile. Then associate the transform-set and IKEv2 Profile with the IPSec profile. Refer to Supported IPsec Parameters for the recommended algorithms.

```
crypto ipsec transform-set sse-ts esp-gcm 256
mode tunnel

crypto ipsec profile sse-ipsec-profile-tunnel-1
 set transform-set sse-ts
 set ikev2-profile sse-ikev2-profile-tunnel-1

crypto ipsec profile sse-ipsec-profile-tunnel-2
 set transform-set sse-ts
 set ikev2-profile sse-ikev2-profile-tunnel-2

crypto ikev2 policy sse
 match address local \[Router_WAN_IP\]
 proposal sse-proposal
```

5. Create the tunnel interface.

   Define the static tunnel interface with the peer IP as the Secure Access VPN headend IP and associate the IPsec profile under the tunnel. Make sure the tunnel interface does not contain NAT related commands; traffic sent to Secure Access should not have NAT applied.

```
interface Tunnel1
 ip unnumbered \[interface-name\]
 ip tcp adjust-mss 1350
```

```
 tunnel source \[interface-name\]
 tunnel mode ipsec ipv4
 tunnel destination \[sse_dc1_ip\]
 tunnel protection ipsec profile sse-ipsec-profile-tunnel-1

interface Tunnel2
 ip unnumbered \[interface-name\]
 ip tcp adjust-mss 1350
 tunnel source \[interface-name\]
 tunnel mode ipsec ipv4
 tunnel destination \[sse_dc2_ip\]
 tunnel protection ipsec profile sse-ipsec-profile-tunnel-2
```

6. Configure routing rules.

   Define the traffic which needs to be tunneled to the CDFW. Based on the requirements, these ACL rules can be modified.

   The route-map needs to be associated with the LAN interface of the router where the device receives the traffic.

   In the following examples, `192.168.20.0/24` is the LAN subnet, and `GigabitEthernet` is the LAN interface.

```
ip access-list extended traffic-to-sse
  permit ip \[lan-ip\] any
!
route-map sse-route-map permit 10
  match ip address traffic-to-sse
  set interface Tunnel1
!
interface GigabitEthernet \[lan-interface-name\]
 ip policy route-map sse-route-map
```

7. Check the tunnel status.

   Use the following command to verify the tunnel status on your ISR.

   `show crypto session detail` and the output must show the tunnel status as **UP-ACTIVE**.

   Substitute the IP address of the Secure Access data center nearest your location for `\[sse_dc_ip\]`.

```
ISR#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update

Interface: Tunnel1
Profile: sse
Uptime: 14:53:47
Session status: UP-ACTIVE
Peer: \[sse_dc_ip\] port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: \[sse_dc_ip\]
      Desc: (none)
  Session ID: 1
  IKEv2 SA: local 10.10.10.201/4500 remote \[sse_dc_ip\]/4500 Active
          Capabilities:DFNXU connid:4 lifetime:09:06:13
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/2499
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/2499
```

8. Manually trigger the tunnel.

Should the tunnel not come up immediately, or should it need to be manually triggered for any reason, select the tunnel interface, and issue the `shutdown` and `no shutdown` commands.

```
ISR(config)#int T1
ISR(config-if)#shutdown
ISR(config-if)#no shutdown
```

9. Verify the tunnel status.

   Verify the tunnel status with `show crypto session remote <Headend IP> detail`. See the example output.

```
ISR#show crypto session remote 146.112.66.2 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel1
Profile: sse
Uptime: 00:39:11
Session status: UP-ACTIVE
Peer: 192.0.2.0 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.0.2.0
      Desc: (none)
  Session ID: 1
  IKEv2 SA: local 192.0.2.0/4500 remote 146.112.66.2/4500 Active
          Capabilities:DN connid:3 lifetime:23:20:49
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4607996/1248
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4607997/1248
```

Configure Tunnels with Cisco Adaptive Security Appliance

Understand how to connect a Cisco Adaptive Security Appliance (ASA) firewall to Cisco Secure Access using one or two IKEv2 IPsec tunnels via Virtual Tunnel Interfaces (VTI).

This guide walks you through connecting a Cisco Adaptive Security Appliance (ASA) firewall to Cisco Secure Access using one or two IKEv2 IPsec tunnels via Virtual Tunnel Interfaces (VTI).

Before you begin

Table 9: Cisco Secure Access requirements

Requirement	Details
Cisco Secure Access account	A valid, active account
Organization ID	Refer to Find Your Organization ID
Network Tunnel Group	Must be pre-configured in Secure Access. Refer to Add a Network Tunnel Group

Tip

When adding a network tunnel group, select the data center closest to your ASA's geographic location to minimize latency.

Table 10: Cisco ASA requirements

Requirement	Details
Hardware	Cisco ASA firewall
Licensing	Security K9 license and ASA Base or Security Plus license
Software	ASA 9.x with IKEv2 support (refer to **ASA version and NAT and IKEv2 identity** below)

Table 11: Network requirements

Requirement	Details
UDP port 500	Open outbound (IKE negotiation)
UDP port 4500	Open outbound (NAT Traversal)
Outbound connectivity	No firewall blocks to Cisco Secure Access data center IPs

Your ASA software version determines how IKEv2 identity is handled and whether the ASA can operate behind NAT.

Table 12: ASA version and NAT and IKEv2 identity

	ASA 9.16 and Earlier	ASA 9.17 and Later
NAT support	Not supported – ASA must not be behind NAT	Supported – ASA can be behind NAT
IKEv2 identity	Automatically uses the interface IPv4 address	Supports per-tunnel identity and FQDN identity
External interface IP	Must be a static, publicly routable IPv4 address configured directly on the ASA interface	No restriction
Secure Access tunnel type	Standard configuration	Set **Tunnel Type** to `Other` and **Authentication** to `FQDN`
Additional ASA config	None	Add to IPsec profile: `set ikev2 local-identity email-id <tunnel-identity>@<org-id>.sse.com`

On ASA 9.16 and earlier, the ASA automatically uses its external interface IPv4 address as the IKEv2 identity. This identity, combined with the pre-shared key (PSK), authenticates the tunnel. If NAT translates this address, the IKEv2 identity will not match what Secure Access expects, and authentication will fail.

ASA 9.17 introduced the ability to explicitly set a per-tunnel FQDN identity, decoupling the IKEv2 identity from the interface address. This resolves the NAT identity mismatch.

Important

If your ASA is on version 9.16 or earlier and is behind NAT, the tunnel will not establish. Either assign a static public IP directly on the ASA's external interface, or upgrade to ASA 9.17 or later.

Note

The `<tunnel-identity>` and `<org-id>` values in the `set ikev2 local-identity` command are generated when you configure the network tunnel group in Secure Access. Refer to Add a Network Tunnel Group for details.

Procedure

1. Gather the following from the Cisco Secure Access dashboard after you create your Network Tunnel Group. Refer to Add a Network Tunnel Group for instructions.

Value	Description	Used in
Primary data center IP	IP address of the primary Secure Access data center	Steps 3, 5
Secondary data center IP	IP address of the secondary Secure Access data center	Step 6
Primary tunnel ID	Tunnel identity for the primary tunnel	Steps 3, 5
Secondary tunnel ID	Tunnel identity for the secondary tunnel	Step 6
Passphrase	Pre-shared key configured for the tunnel group	Step 3

2. **Configure the IKEv2 policy**
   a) Define the IKEv2 policy settings according to the Supported IPsec Parameters.
   b) Choose the policy number based on your ASA's existing policies. In the following example, the policy number is `10`.
   c) Replace `outside` with the name of the public-facing interface your ASA uses for VPN connectivity, if different.

```
crypto ikev2 policy 10
  encryption aes-gcm-256
  integrity null
  group 19
  lifetime seconds 86400
crypto ikev2 enable outside
```

3. **Configure the Group Policy and Tunnel Group**
   a) Configure the group policy and tunnel group for the primary data center connection.
   b) Replace the following placeholders. Refer to Add a Network Tunnel Group.

Placeholder	Replace With
`<Primary data center IP address>`	IP address of the primary Secure Access data center

Placeholder	Replace With
`<Portal_Tunnel_Passphrase>`	The passphrase you configured for the network tunnel group

```
group-policy sse-policy internal
group-policy sse-policy attributes
   vpn-tunnel-protocol ikev2

tunnel-group <Primary data center IP address> type ipsec-l2l
tunnel-group <Primary data center IP address> general-attributes
  default-group-policy sse-policy
tunnel-group <Primary data center IP address> ipsec-attributes
  ikev2 remote-authentication pre-shared-key 0 \[Portal_Tunnel_Passphrase\]

  ikev2 local-authentication pre-shared-key 0 \[Portal_Tunnel_Passphrase\]
```

Tip

Validate that the `crypto isakmp identity` command is set to the default value `auto`. This ensures the correct ID method is used for ISAKMP peers.

4. **Configure the IPsec Proposal and Profile (Primary tunnel)**
   a) Define the IPsec proposal and profile according to the Supported IPsec Parameters.
   b) Replace `<Primary tunnel ID>` with the tunnel identity for your primary tunnel from the Secure Access dashboard.

```
crypto ipsec ikev2 ipsec-proposal Secure-Access-Ipsec-Proposal
  protocol esp encryption aes-gcm-256
  protocol esp integrity sha-1

crypto ipsec profile Secure-Access-Primary
  set ikev2 ipsec-proposal Secure-Access-Ipsec-Proposal
  !
  !Note: below command applies for v9.17+ only
  set ikev2 local-identity email-id <Primary tunnel ID>
```

Note

The `set ikev2 local-identity` command applies to ASA 9.17 and later only. Omit this line for ASA 9.16 and earlier.

5. **Create the Virtual Tunnel Interface (Primary tunnel)**
   a) Create a VTI for the primary tunnel.
   b) Replace the following placeholders:

Placeholder	Replace With
`<Primary data center IP address>`	IP address of the primary Secure Access data center

Placeholder	Replace With
`<VTI IP address> <subnet mask>`	An unused IP address and subnet not assigned to any existing VLAN, subnet, or interface in your network (for example, 169.254.1.1 255.255.255.252)

```
interface Tunnel1
   nameif vti
   ip address <VTI IP address> <subnet mask>
   tunnel source interface outside
   tunnel destination <Primary data center IP address>
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile Secure-Access-Primary
```

6. Configure the Secondary tunnel

To add a secondary tunnel for redundancy, repeat Steps 3 through 5 with the following changes:

Parameter	Primary tunnel	Secondary tunnel
Data center IP	Primary data center IP	Secondary data center IP
Tunnel ID	Primary tunnel ID	Secondary tunnel ID
IPsec profile name	`Secure-Access-Primary`	`Secure-Access-Secondary`
VTI interface name	`Tunnel1 / vti-primary`	`Tunnel2 / vti-secondary`
VTI IP address	From one unused subnet	From a different unused subnet

Note

The group policy (`sse-policy`) and IPsec proposal (`Secure-Access-Ipsec-Proposal`) created in Steps 2 and 3 can be reused. You must create a separate IPsec profile and VTI for the secondary tunnel.

7. Configure policy-based routing (PBR)

a) Configure PBR to direct internal traffic through the tunnel interface to Secure Access.
b) In the following example:

- LAN subnet: `192.168.20.0/24`
- LAN interface: `GigabitEthernet1/2`
- Next-hop IP: An IP address in the same subnet assigned to the primary VTI

```
access-list ACL-sse line 1 extended permit ip 192.168.20.0 255.255.255.0 any4


route-map sse-PBR permit 10
  match ip address ACL-sse
  set ip next-hop x.x.x.2

interface GigabitEthernet1/2
  policy-route route-map sse-PBR
```

8. Verify the tunnel

a) Check IKEv2 and IPsec status: Run the following commands from the ASA CLI.

```
show crypto ikev2 sa detail
show crypto ipsec sa detail
```

b) Simulate traffic with packet tracer: Use the `packet-tracer` command to confirm that traffic from the inside interface routes through the tunnel.

```
packet-tracer input inside tcp <source IP> <source port> <destination IP>
 <destination port> detailed
```

Example:

```
packet-tracer input inside tcp 192.168.20.13 3520 72.163.4.161 443 detailed
```

In a successful configuration, the output includes the following key phases:

Phase	Type	Expected result	What it confirms
1	ACCESS-LIST	ALLOW	Traffic is permitted on the inside interface
2	PBR-LOOKUP	ALLOW	Policy-based routing matches the route map and identifies the VTI as the egress interface
5	VPN (encrypt)	ALLOW	Traffic is selected for encryption on the VTI
6	VPN (ipsec-tunnel-flow)	ALLOW	IPsec tunnel flow is established
9	FLOW-CREATION	ALLOW	A new traffic flow is created and dispatched

The final `Result` section should show:

```
output-interface: vti
Action: allow
```

Note

If any phase shows `DROP` or if the output interface is not `vti`, review your PBR configuration, tunnel group settings, and IPsec profile.

After completing this guide, your ASA will:

- Establish two authenticated IKEv2 IPsec tunnels to Secure Access
- Route designated internal traffic through the tunnel via policy-based routing
- Authenticate using a pre-shared key combined with IKEv2 identity
- Connect to the nearest Cisco Secure Access data center(s)

Configure Tunnels with AWS Virtual Private Clouds and Elastic Compute instances

Understand how to connect AWS Virtual Private Clouds (VPCs) and Elastic Compute Instances (ECs) to Cisco Secure Access.

Before you begin

Follow the steps in this guide to connect Amazon Web Services (AWS), Virtual Private Clouds (VPCs) and Elastic Compute instances (ECs) to Cisco Secure Access.

Limitations

When integrating AWS Transit Gateway with Cisco Secure Access, consider the following limitations. These factors impact the functionality and reliability of the connection:

- Equal-cost multi-path routing (ECMP) is not supported because AWS requires specific IP:IP tunnel identifiers. Additional tunnels must source from new IP addresses.
- You cannot configure multiple AWS Site-to-Site VPNs for overlapping subnets. However, you can add connectivity to new VPC subnets. Using two active AWS Site-to-Site VPNs as a backup causes asymmetrical routing to Cisco Secure Access.
- Redundant connectivity from multiple AWS Transit Gateways or AWS Site-to-Site VPNs is not supported. This is due to the absence of Border Gateway Protocol (BGP) preference settings in AWS Site-to-Site VPN configurations or the Cisco Secure Access dashboard.
- Disaster recovery (DR) testing is limited. Disabling individual tunnels quickly is not possible. Reconfiguring an active tunnel in AWS may take up to two minutes to restore traffic flow.

> **Note**
>
> Failover initiated by Cisco Secure Access using BGP completes within seconds. However, dead peer detection (DPD) may take up to two minutes in certain DR scenarios, such as when external factors (e.g., ISP blocking traffic) are involved.
>
> For other disconnection events where both sides can still communicate, an Internet Protocol Security (IPsec) “DELETE” event is sent. This results in failover to the secondary IPSEC tunnel within seconds.

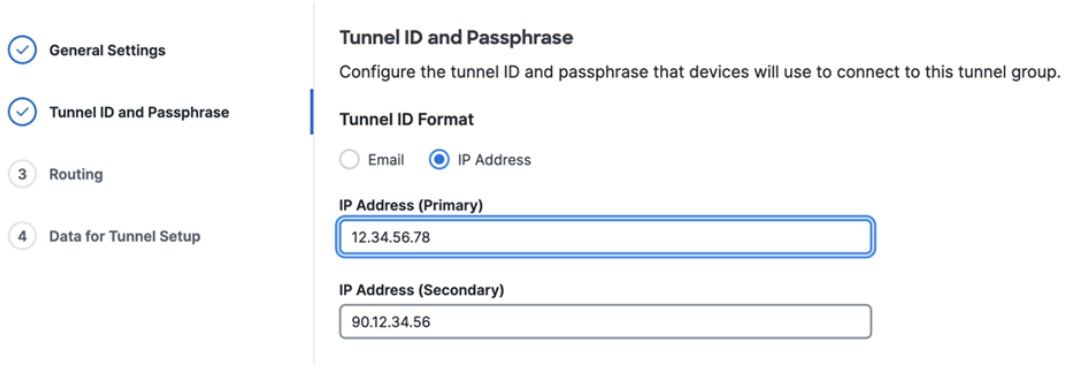
To ensure the tunnel works successfully with AWS Transit Gateway for Site-to-Site Virtual Private Networks (VPNs), you must meet the following prerequisites. These prerequisites ensure seamless interoperability between AWS Transit Gateway and Cisco Secure Access.

- You must have a thorough understanding of AWS Virtual Private Clouds (VPCs), routing, and the AWS console pages.
- Border Gateway Protocol (BGP) is mandatory. Static routing is not supported for Internet Protocol Security (IPsec) tunnels between AWS Site-to-Site VPN and Cisco Secure Access.
- BGP peering is used to learn routes and to determine if the tunnel is passing traffic. When the peer connection is lost, the tunnel is removed from the route table in both AWS and Cisco Secure Access.
- Set up two AWS Site-to-Site VPN configurations for each AWS Transit Gateway. Each configuration must connect to one Cisco Secure Access Tunnel Group.

  A single AWS configuration with two tunnels does not work.

Procedure

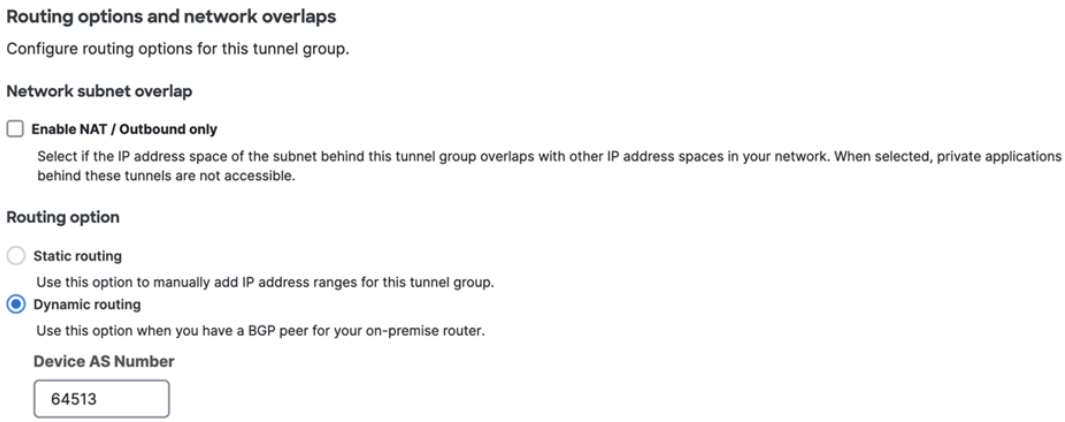
1. Add a **Network Tunnel Group** to Secure Access. For complete procedure, see Add Network Tunnel Group.
2. Select **Tunnel ID Format** as an IP address and enter the two IP addresses provided by Amazon Web Services (AWS), if available.
3. Use Placeholder IP Addresses if AWS IPs are unavailable.
   - Use valid placeholder IP addresses for the primary and secondary AWS head ends.
   - Replace the placeholders with actual IP addresses when AWS allocates them.
   - The actual IP addresses become available during the configuration of the AWS Site-to-Site Virtual Private Network (VPN).For example, use placeholder IP addresses such as 12.34.56.78 and 90.12.34.56.



4. Configure **Border Gateway Protocol (BGP)** for the tunnel group.

   For example, you can use Autonomous System (AS) number 64513.

> **Note**
>
> BGP is mandatory for Cisco Secure Access to work with AWS Site-to-Site VPN (IPsec tunnels). Any valid AS number except 64512 is acceptable.



After completion, the new tunnel group appears in the Cisco Secure Access dashboard with a status "Disconnected". The status updates once the AWS Transit Gateway Site-to-Site configuration becomes active.

Deploy a New AWS Transit Gateway

Describes Deploy a New AWS Transit Gateway in Cisco Secure Access. Transit gateways provide a convenient method for enabling communication between AWS Virtual Private Clouds (VPCs) without overlapping subnets.

Transit gateways provide a convenient method for enabling communication between AWS Virtual Private Clouds (VPCs) without overlapping subnets. They also allow these VPCs to connect to the Internet.

You must create and deploy a new AWS Transit Gateway specifically for Cisco Secure Access tunnels. While you can use an existing AWS Transit Gateway, exercise caution as advertising a default route may cause unexpected issues with existing VPC attachments.

Follow the steps in Get started with using Amazon VPC Transit Gateways to create a new AWS Transit Gateway.

Configure Two VPN Site-to-Site Connections to the New Transit Gateway

Provides instructions for completing the Configure Two VPN Site-to-Site Connections to the New Transit Gateway workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Configure the First VPN Site-to-Site Connection
2. Select the external IP address to use.
3. Set the **Target gateway** to **Transit Gateway** and choose the ID of your new transit gateway.
4. Enter the **Customer Gateway Address**.

   Enter the IP address from the Cisco Secure Access tunnel group. For example, in the United States (Virginia), use `35.171.214.188`.

5. Confirm this address in the Cisco Secure Access console because it may vary by region.
6. Record AWS Tunnel one's IP Address to update the Cisco Secure Access tunnel group.

   > **Note**
   >
   > Do not configure Tunnel 2 in this VPN connection. The Cisco Secure Access secondary tunnel will be set up in a separate VPN configuration.

7. Set the Inside IPv4 CIDR.

   Enter `169.254.0.13/30` as the "Inside IPv4 CIDR" range. AWS presents the IPv4 CIDR as the BGP peer to Cisco Secure Access.

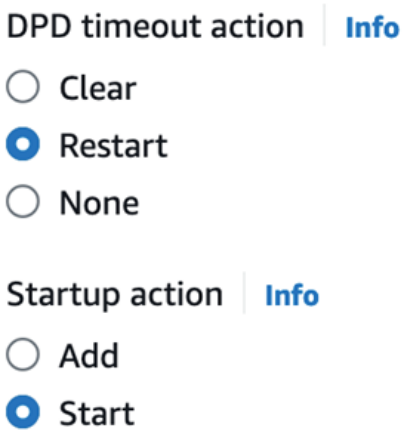
8. Enter the passphrase set during the Cisco Secure Access tunnel group configuration.
9. Configure the tunnel parameters.

   Follow the tunnel parameters in Supported IPsec Parameters. Remove unused parameters and use only the options provided in this table. Retain the remaining values and fields as their default settings.

Components	Parameters
Phase 1 encryption algorithms	AES256-GCM-16
Phase 2 encryption algorithms	AES256-GCM-16
Phase 1 integrity algorithms	SHA2-256
Phase 2 integrity algorithms	SHA2-256

Components	Parameters
Phase 1 DH group numbers	19,20
Phase 2 DH group numbers	19,20
IKE version	Ikev2

10. Check the **Restart** and **Start** boxes to configure **DPD timeout action** and **Startup action**.



> **Note**
>
> Do not configure the second tunnel. Save the settings.

Configure the Second VPN Site-to-Site Connection

Provides instructions for completing the Configure the Second VPN Site-to-Site Connection workflow in Cisco Secure Access. Repeat step 1 through step 3 from the first VPN Site-to-Site connection.

Procedure

---

1. Repeat step 1 through step 3 from the first VPN Site-to-Site connection.
2. Record the new IP address for the second VPN configuration.

> **Note**
>
> Do not configure Tunnel 2 in this new VPN configuration.

3. Obtain the customer gateway IP address for the secondary hub.

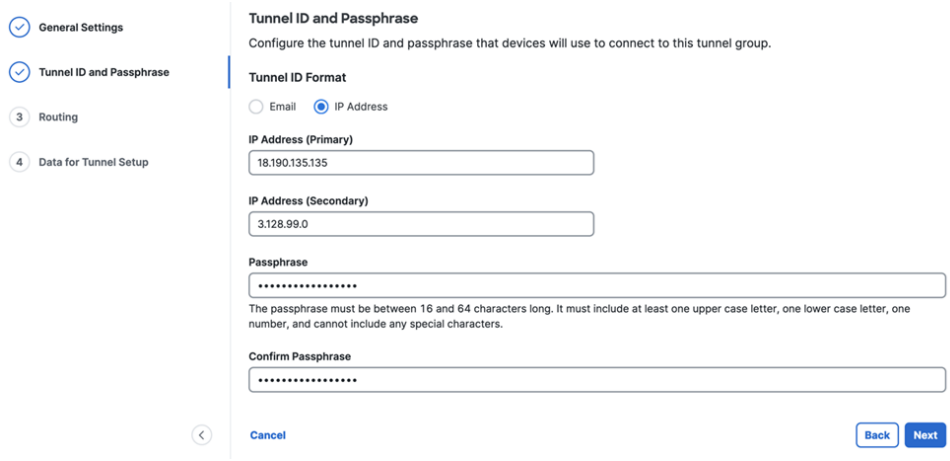
   For example, the document uses 44.217.195.188. However, your actual IP address from the Cisco Secure Access tunnel group may vary.

4. Set the Inside IPv4 CIDR to 169.254.0.16/30 for the new connection.

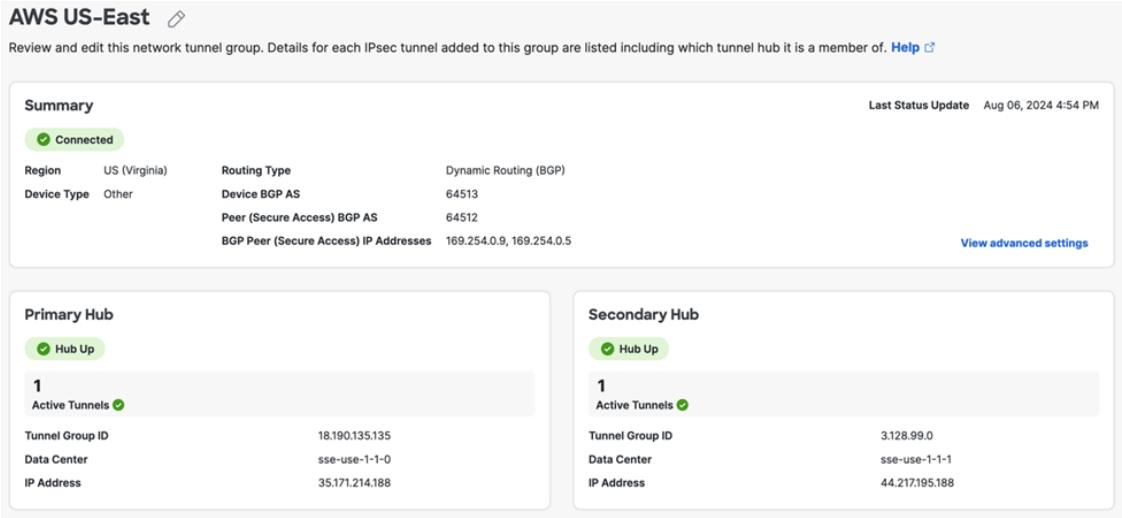
> **Note**
>
> AWS requires a /30 subnet. Cisco Secure Access IPSEC tunnels accept any IP in 169.254.0.0/24, except 169.254.0.5 and 169.254.0.9, which are reserved.

5. Update the Cisco Secure Access dashboard with the AWS IP addresses for both VPN configurations.

   For example: Use Primary IP: 18.190.135.135 and Secondary IP: 3.128.99.0



6. Allow a few minutes for the tunnels to initialize. Once active, the Cisco Secure Access status page displays the updated status.



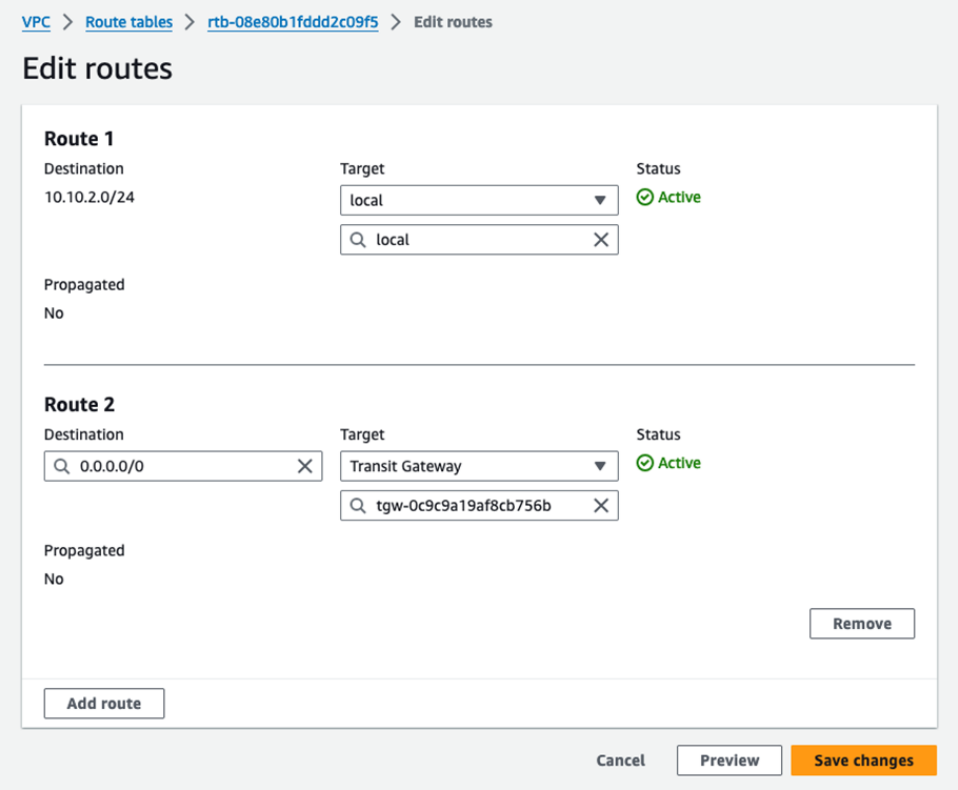
Configure the VPC Route Table to use the AWS Transit Gateway

Provides instructions for completing the Configure the VPC Route Table to use the AWS Transit Gateway workflow in Cisco Secure Access. Configure the VPC route table to target the Transit Gateway.For example: VPC Subnet: 10.10.2.0/24, Transit Gateway ID: tgw-0c9c9a19af8cb756b.

> **Note**
>
> Attaching a VPC to the Transit Gateway is insufficient.

Procedure

1. Configure the VPC route table to target the Transit Gateway.For example: VPC Subnet: 10.10.2.0/24, Transit Gateway ID: tgw-0c9c9a19af8cb756b.
2. Edit the route for 0.0.0.0/0 to target the Transit Gateway ID.



3. Click **Save the changes**.

> **Note**
>
> All connected subnets to the Transit Gateway are advertised to Cisco Secure Access using BGP.

Configure Tunnels with VeloCloud SD-WAN

Understand how to connect VeloCloud SD-WAN to Cisco Secure Access with singular or failover network tunnel groups.

VeloCloud is a cloud network service solution that you can integrate into Secure Access by adding it as a device type within a network tunnel group. You can create singular or failover network tunnel groups to address connectivity issues

for larger deployments. You can use VeloCloud as a third party SD-WAN device to enhance general security and connectivity. When used in network tunnel groups, this allows secure IPsec tunnels to redirect branch traffic to Secure Access.

Previously, failover to a secondary tunnel was not supported and environments experienced warnings, delays in migration, or excessive amounts of network tunnel groups to address the lack of support. We strongly recommend creating secondary tunnels for large deployments and organizations to create a seamless, scalable, and supported tunnel redundancy for VeloCloud SD-WAN devices. This option reduces operational risk, validates secondary tunnel configuration, and supports Zscaler and other SSE solutions.

If you intend to initiate failover or configure a primary and secondary SD-WAN hub, both hubs **must** share the same authentication ID; this is configurable in the VeloCloud dashboard. Configuring a different authentication ID does not allow the hubs to sync. Share the authID within a network tunnel group and this ensures that when if the primary hub experiences an issue, the secondary hub immediately switches to the primary role without requiring authentication from an admin.

Use this procedure to create and configure a network tunnel group using a VeloCloud SD-WAN device:

Before you begin

The following prerequisites must be met for the tunnel to work successfully.

- You ust be an admin.
- You must already have your Velocloud SD-WAN environment configured. For more information see Secure Access SD-WAN Integration with Arista VeloCloud.
- Your data center hubs must already be created and configured. If you have a secondary hub for a failover environment, both hubs **must** share the same authentication ID; this is configurable in the VeloCloud dashboard.

Procedure

1. Follow the steps in Add a Network Tunnel Group. Select **VeloCloud** as the device type.
2. Make note of the **Tunnel ID** and **Passphrase** you enter when configuring the network tunnel group. These values are needed to configure the SD-WAN tunnel.
3. Configure the network tunnel group with a secondary tunnel to support failover. Note that the secondary tunnel uses the same passphrase as the primary tunnel. Failover prevents dropped traffic during select downtime such as maintenance periods.
4. Continue with the remaining steps in Add a Network Tunnel Group. Upon completion, review and confirm the VeloCloud configuration; if you have configured a secondary network tunnel group, the details page displays details for both the primary and secondary hub as well as the corresponding network tunnel groups.

Configure Tunnels with Cisco Secure Firewall

Understand how to configure network tunnels with Cisco Secure Firewall to support site-to-site VPN between Firewall Threat Defense devices and Secure Access through Cisco Secure Firewall Management Center.

Cisco Secure Firewall is a family of threat-focused next-generation firewalls. It can be managed centrally through Cisco Secure Firewall Management Center or through the on-box manager Secure Firewall Device Manager (FDM). This guide covers the steps to configure site-to-site VPN between FTD devices and Secure Access through Cisco Secure Firewall Management Center.

Until version 6.7, FTD only supports policy-based VPN (Crypto-map). Version 6.7+ supports Virtual tunnel interface (VTI), version 7.1+ supports IKE identity and policy-based routing (PBR) through graphic interface.

The Secure Firewall configuration process consists of the following steps.

1. Add Network Object
2. Add Traffic Selector ACL
3. Configure Site-to-Site VPN
4. Configure NAT Policy
5. Configure Access Policy

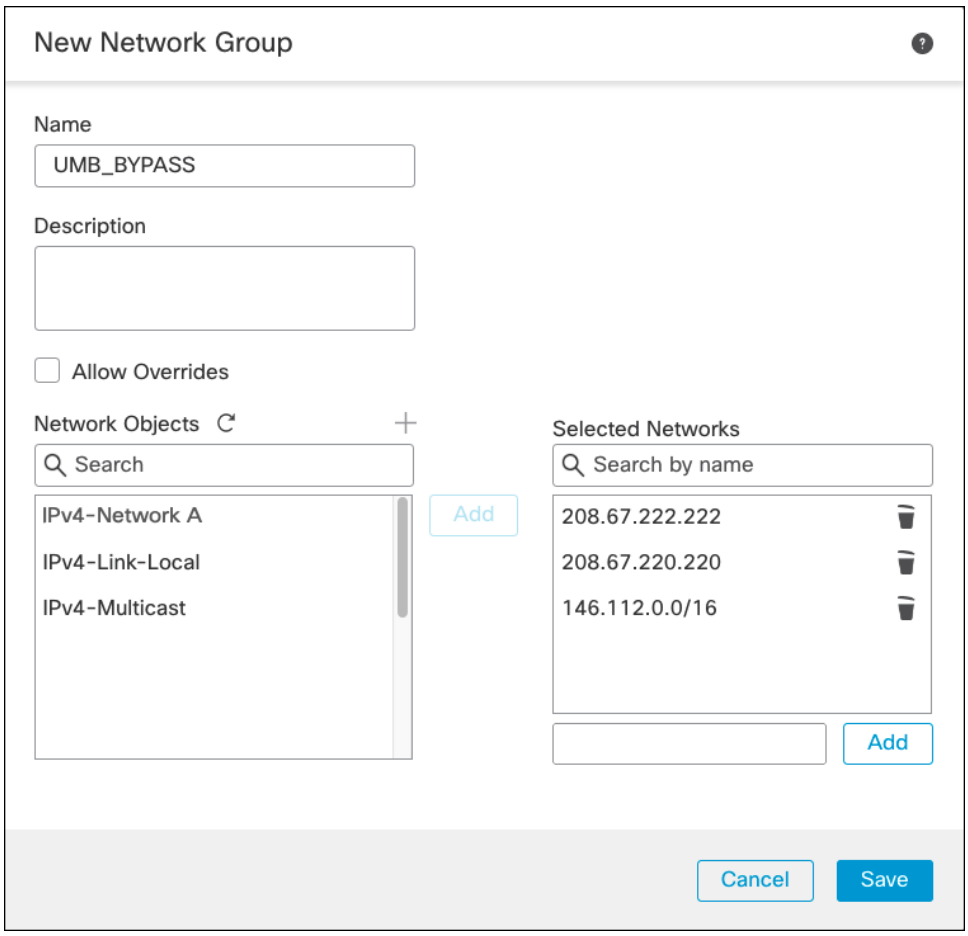
Procedure

1. To start the configuration, log in to your Cisco Secure Firewall Management Center web interface at its IP address or FQDN; for example, `https://FMC_IP_OR_FQDN`.
2. Secure Firewall authenticates to the Secure Access IPsec headend by using a Pre-Shared Key (PSK) and IKEv2 IP identity. Follow the steps in Add Network Tunnel Group to add an FTD device to Secure Access.

   Note

   Secure Access does not support dynamic IP addresses for ASA and Secure Firewall devices.

   The new tunnel appears in Secure Access with a status of `Unestablished`. The tunnel status is updated once the first IKEv2 INIT message containing the tunnel identity is received in one of the Secure Access data centers.
3. Create a network object type "Group": in Secure Firewall, navigate to **Objects** > **Object Management** > **Network** > **Add Network** > **Add Group**, then add the Secure Access resolvers IP address so the DNS queries are not sent through the tunnel.



Note

Optionally, add 146.112.0.0/16 as a network. Web traffic from endpoints with PAC file or Cisco Secure Client as well as proxy chaining traffic can then go outside the IPSec tunnel and achieve higher throughput.

Currently, if the DNS queries are sent through the tunnel it will be NATed to 146.112.0.0/16 IP range and queries will not be linked to the user's dashboard. By bypassing the traffic to the Secure Access resolvers it is possible to add a public IP address to the dashboard (network deployment) and retrain DNS visibility and enforcement capabilities.

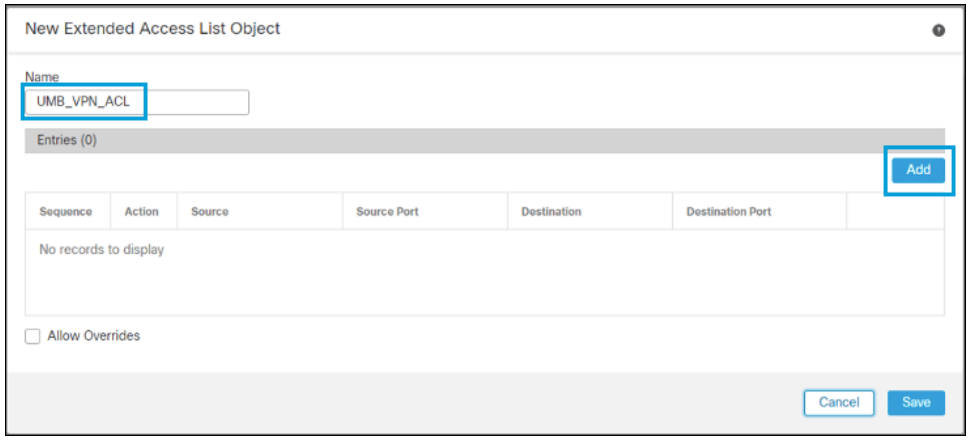
Note

Public IP traffic from SIG users will appear to come from the address ranges 146.112.0.0/16 and 155.190.0.0/16. Depending on your organization, you may be required to inform service providers that you access through the Secure Access service of these additional IP address ranges. For example, some service providers require prior knowledge of the IP address ranges used before allowing access to their service.

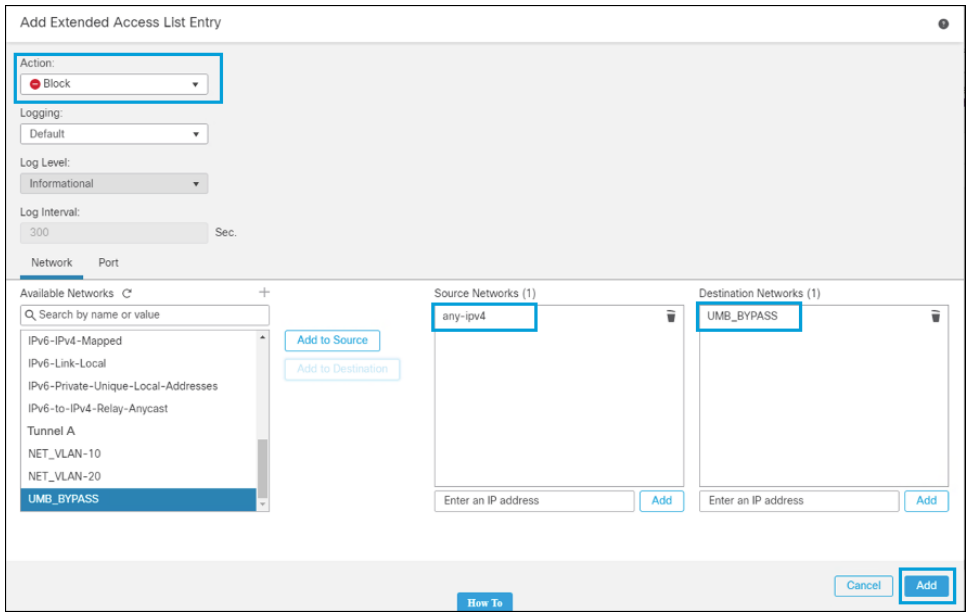
4. **Add the traffic selector ACL:** Navigate to **Objects** > **Object Management** > **Access List** > **Extended** > **Add Extended Access List**.

This ACL is used in the IKEv2 security association negotiation as well as when Secure Firewall makes decisions about when to encrypt traffic. It does not encrypt traffic denied in the ACL when the `deny` statement comes before the `permit` statement.

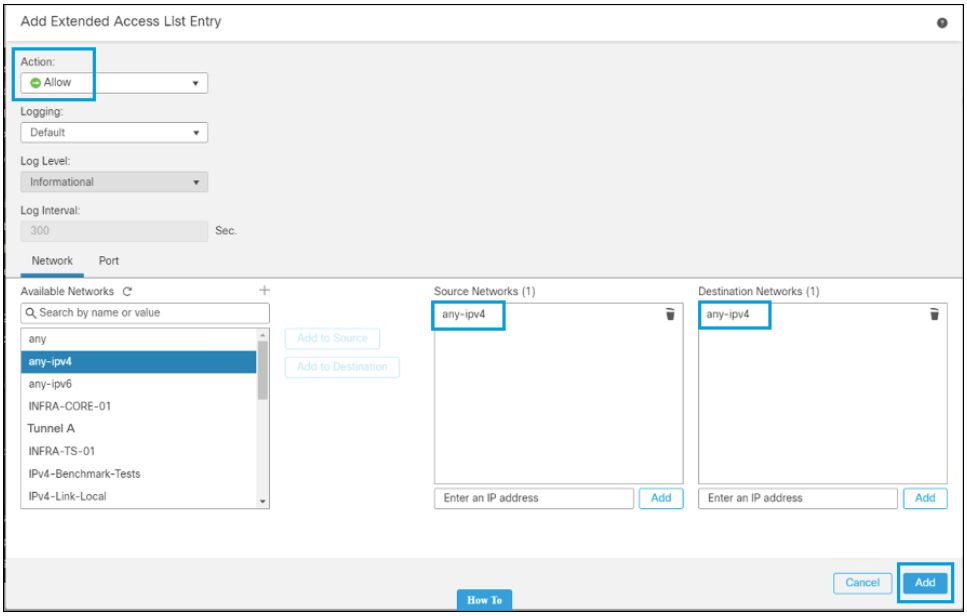
a) Enter a name for the ACL and then click **Add** to add the Access Control Entries (ACE).



b) The first entry denies traffic to the network object type group containing the Secure Access resolvers. Optionally, traffic to the `146.112.0.0/16` and `155.190.0.0/16` subnets can also be denied.

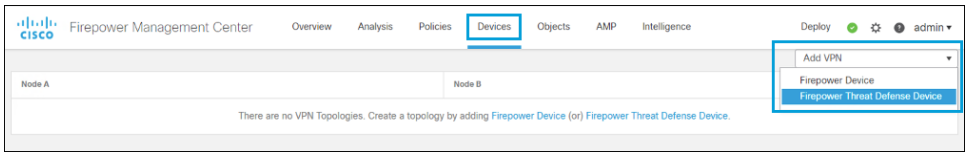


c) The second entry allows traffic from any IPv4 address to any IPv4 address. This is also the entry IKEv2 uses to negotiate the IPSec Security Association (traffic selector).

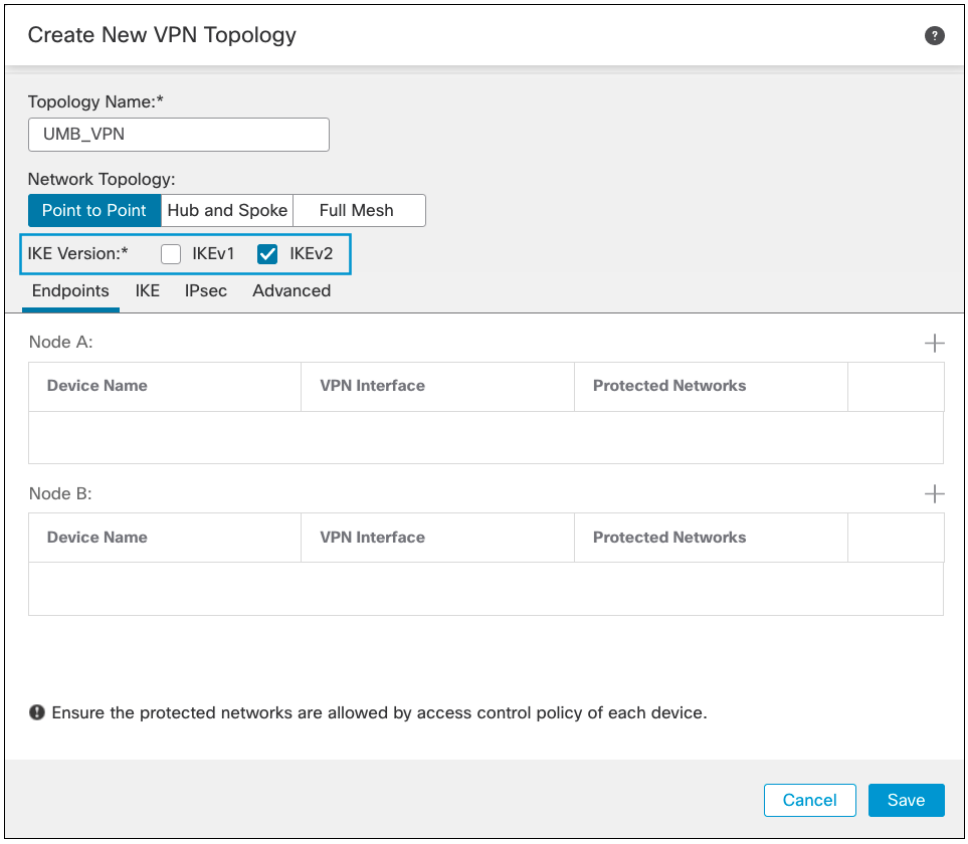


d) Click **Save**.

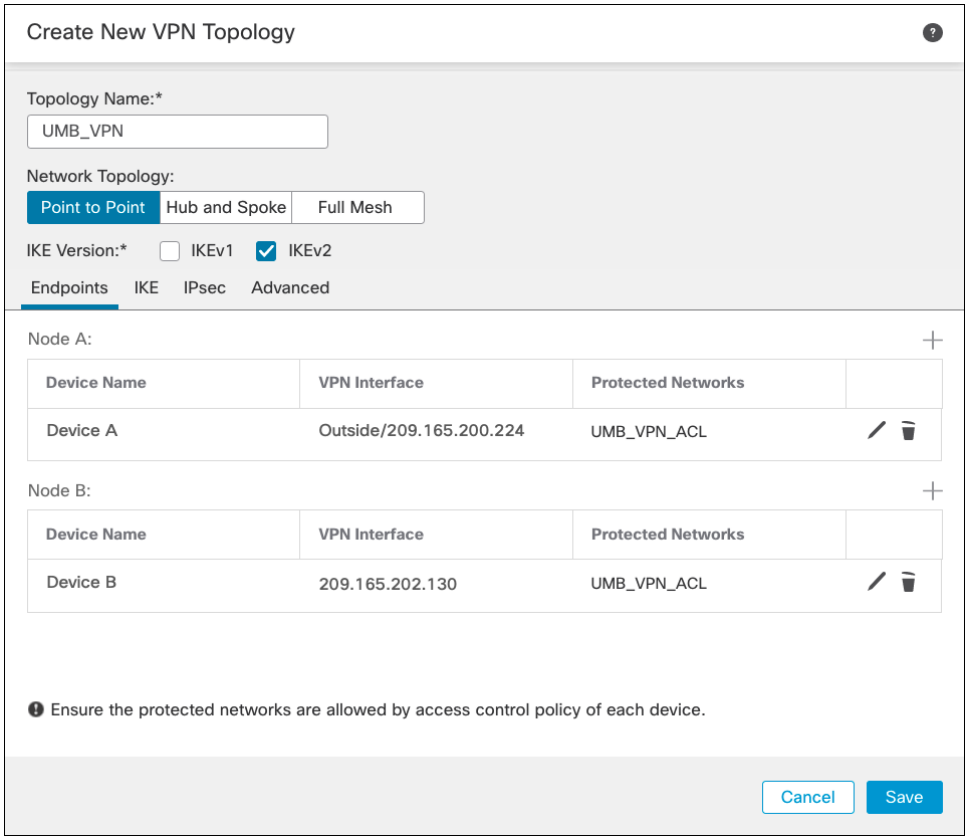
5. You can now configure the site-to-site VPN. Navigate to **Devices** > **VPN** > **Site to Site** > **Add VPN** > **Secure Firewall Threat Defense Device**.



6. Enter a name for the topology. Check IKEv2 box (Secure Access supports IKEv2 only). For more information about supported protocols, see Supported IPSec Parameters.



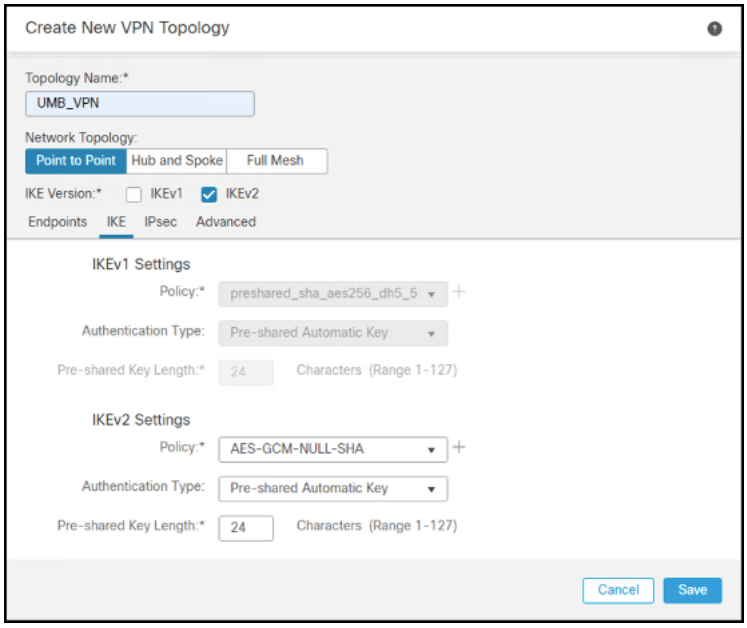
7. Add two peers: the local peer (FTD device) and the remote peer (Secure Access).



a) **Node A**: Click **Add** and select the FTD device as the local peer and the interface sourcing the IPSec connection. The IP address is automatically populated.

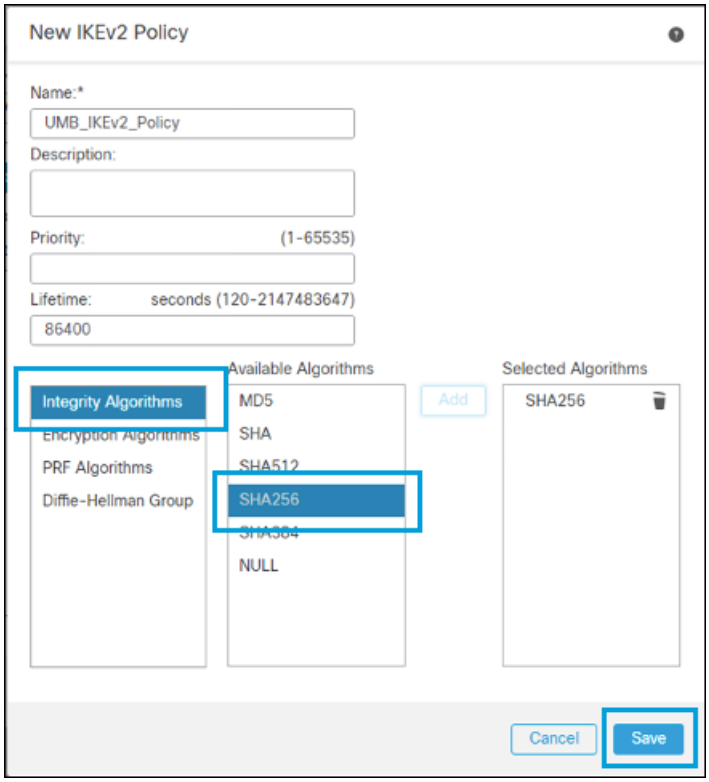
b) **Protected Networks**: Select **Access List (Extended)**, then select the ACL you created in the traffic selector ACL. Click **OK**.
c) **Node B**: Click **Add** to add the remote peer (Secure Access).
d) Select **Extranet** and enter a name. Select **Static**, and enter one of the Secure Access datacenter IP addresses. Then select the same ACL, then click **OK**.

8. Click the **IKE** tab to add a new IKEv2 Policy containing the desired crypto algorithms. For more information about encryption supported by Secure Access, see Supported IPsec Parameters.

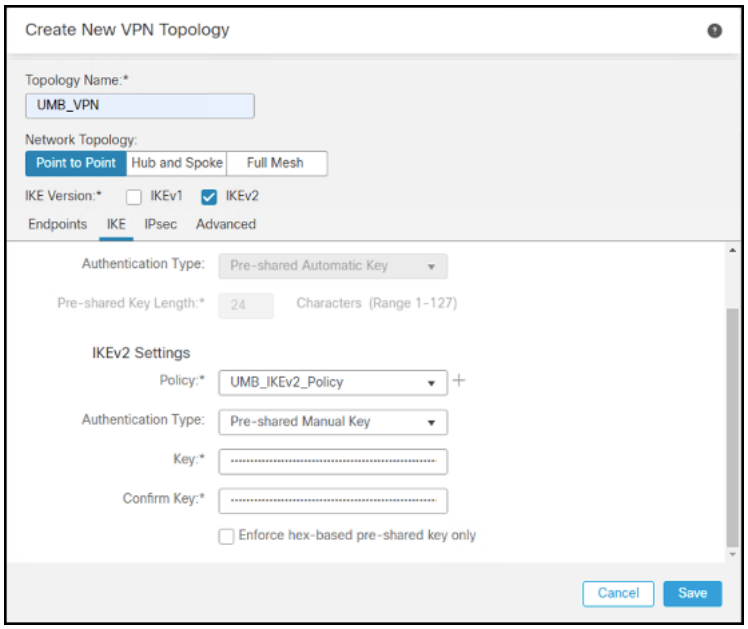


9. Enter a name for the IKEv2 policy, then select the parameters from the Supported IPsec Parameters.

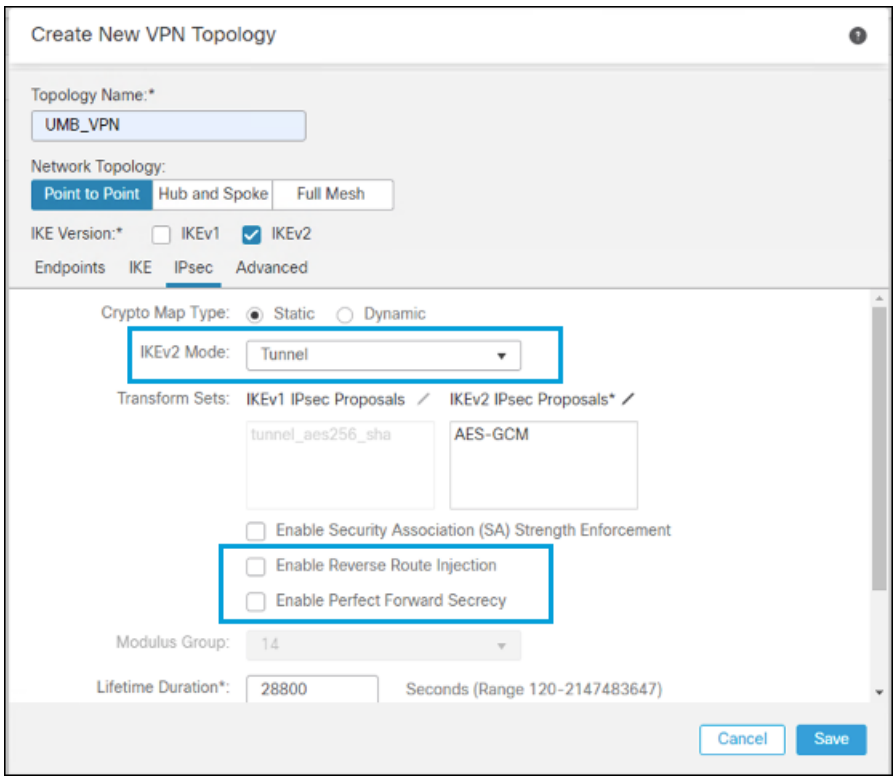
> **Note**
>
> If you create a tunnel to a Cisco SD-WAN device, we strongly recommend configuring the **Lifetime** value to three hours or less; this prevents the cEdge router of the SD-WAN device from rekeying and minimizes the chance of the tunnel going down.



10. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down menu and enter the key.

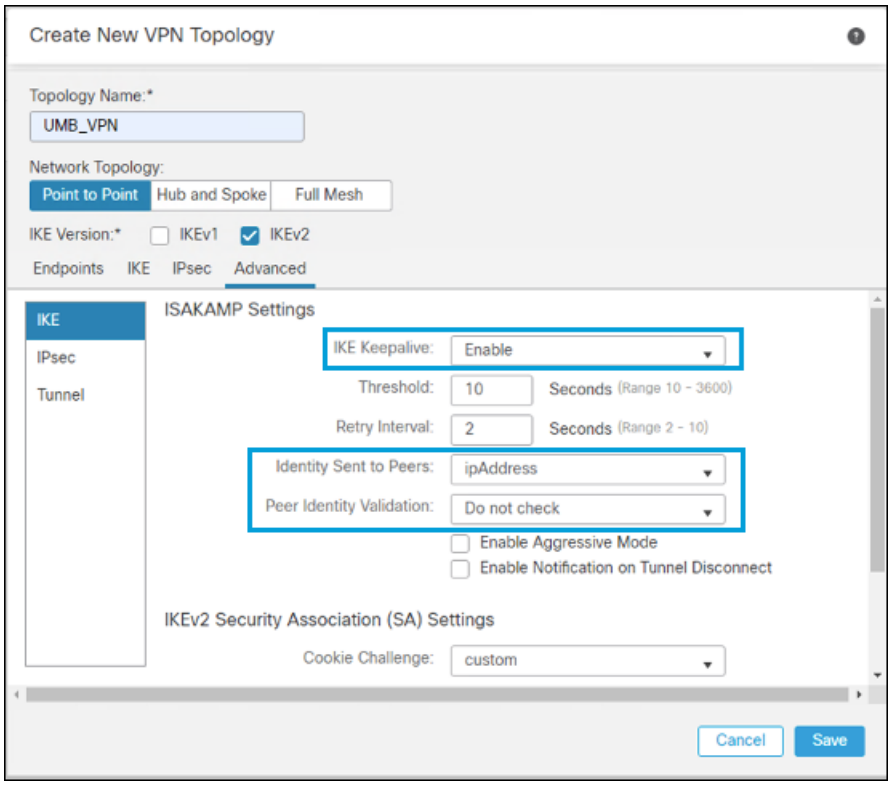


11. Under **IPSec**:

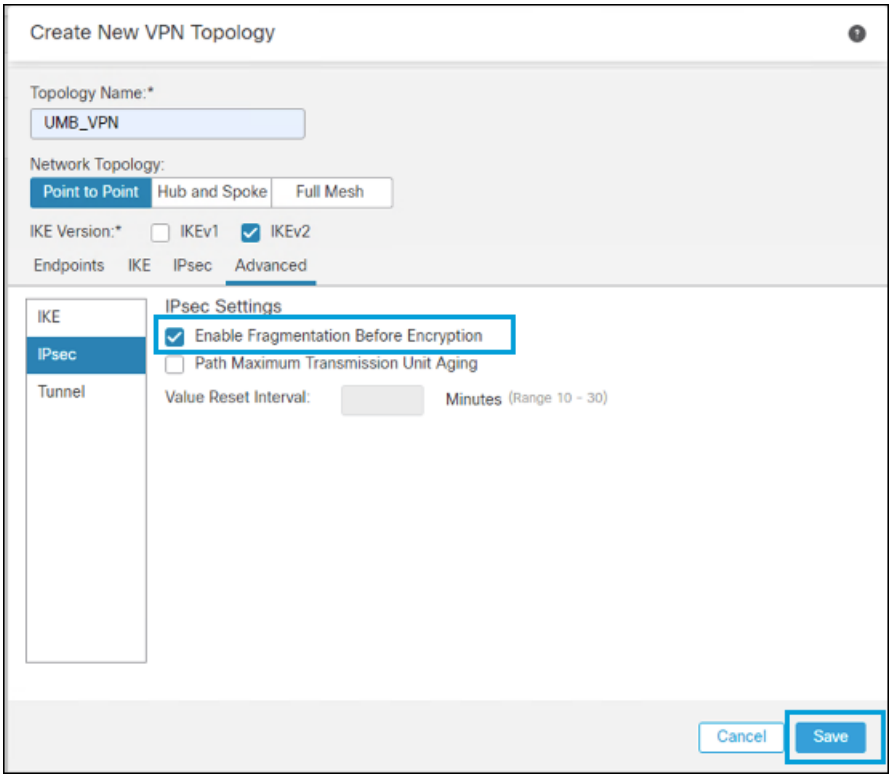


a) **IKEv2 Mode**: Select Tunnel.
b) Add a new **IKEv2 IPsec Proposal** with your crypto algorithms or select an existing profile.
c) Uncheck **Enable Reverse Route Injection**.
d) Uncheck **Enable Perfect Forward Secrecy**.

12. Under **Advanced**:



a) Select **IKE**.
b) **IKE Keepalive**: Select **Enable**.
c) **Identity Sent to Peers**: Select **ipAddress**.
d) **Peer Identity Validation**: Select **Do not check**.
e) Select **IPsec**.



f) **IPsec Settings** check the box to **Enable Fragmentation Before Encryption**.
g) Click **Save**.

Configure NAT Policy

Provides instructions for completing the Configure NAT Policy workflow in Cisco Secure Access. If a NAT policy currently exists in the Secure Firewall device, this policy must be changed to exempt traffic going through the tunnel from being NATed.

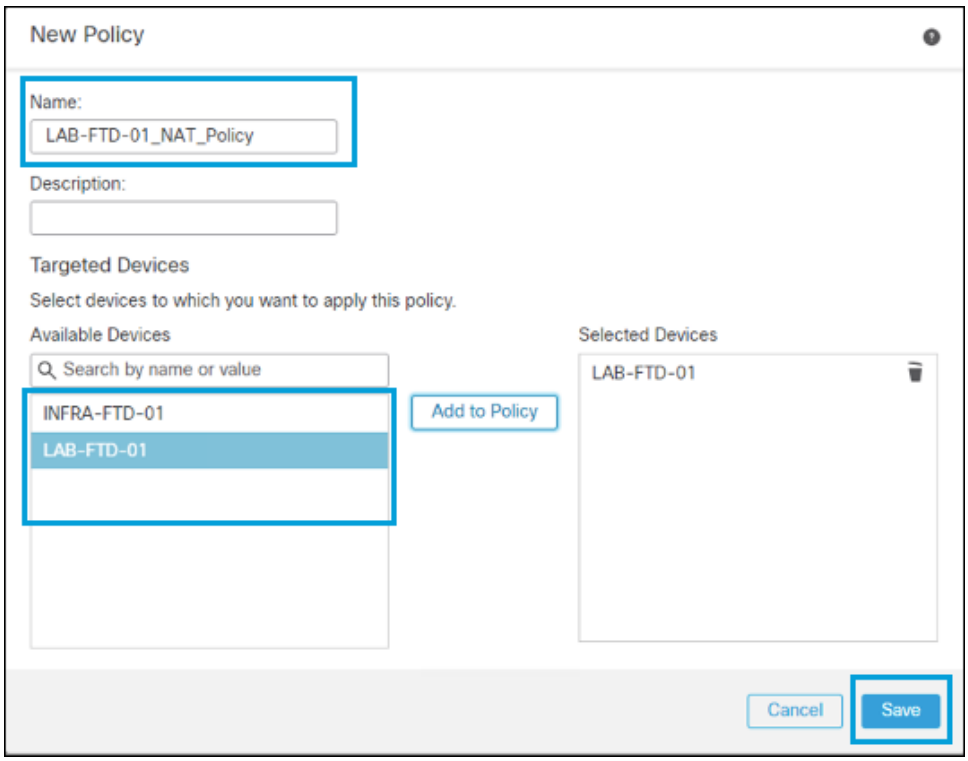
If a NAT policy currently exists in the Secure Firewall device, this policy must be changed to exempt traffic going through the tunnel from being NATed. Secure Access requires the source of the connection to be the client's original private IP address – the public IP is not currently supported.

If you use the public IP in your internal network, you must NAT the traffic to a private IP address pool before sending the traffic to Secure Access, as most of the traffic goes through the Secure Access IPSec tunnel. It is easier to create NAT for the traffic not going through the tunnel and use no NAT for all other traffic.

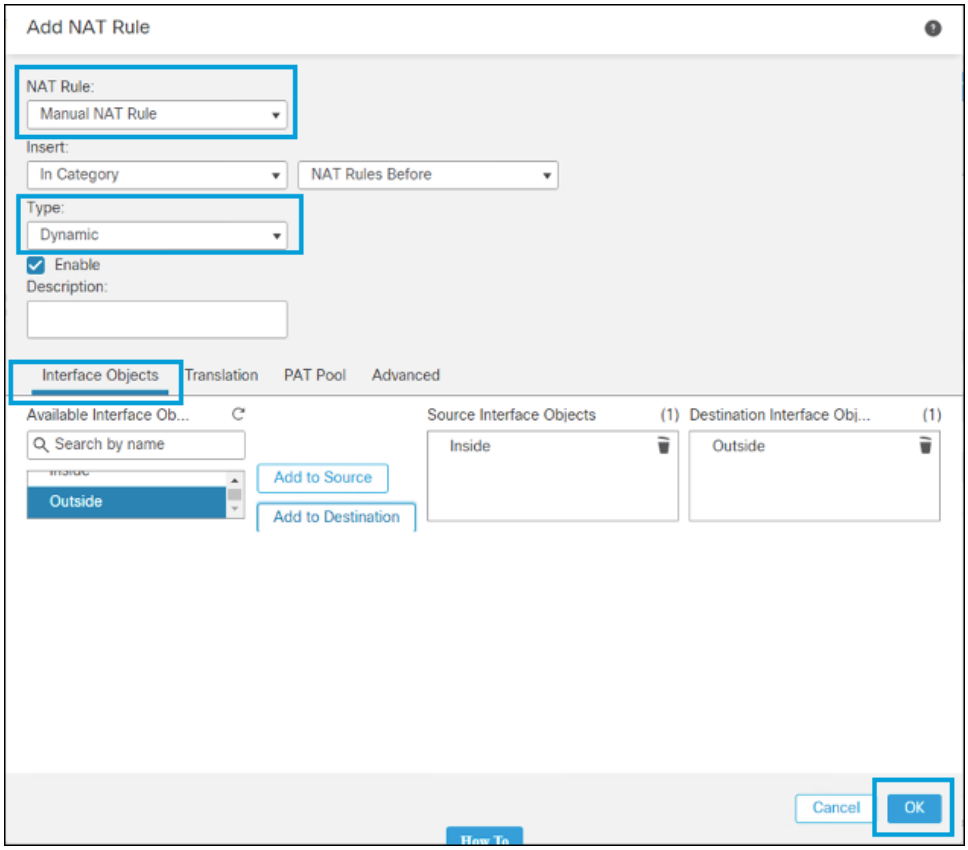
In this example, the network object containing the Secure Access resolvers' IP address is referred to in the NAT statement. All traffic sourced from the internal network with a destination matching the network object will have the source IP NATed to the firewall interface address. All other traffic does not match the NAT statement, and so is forwarded to Secure Access without being NATed.

Procedure

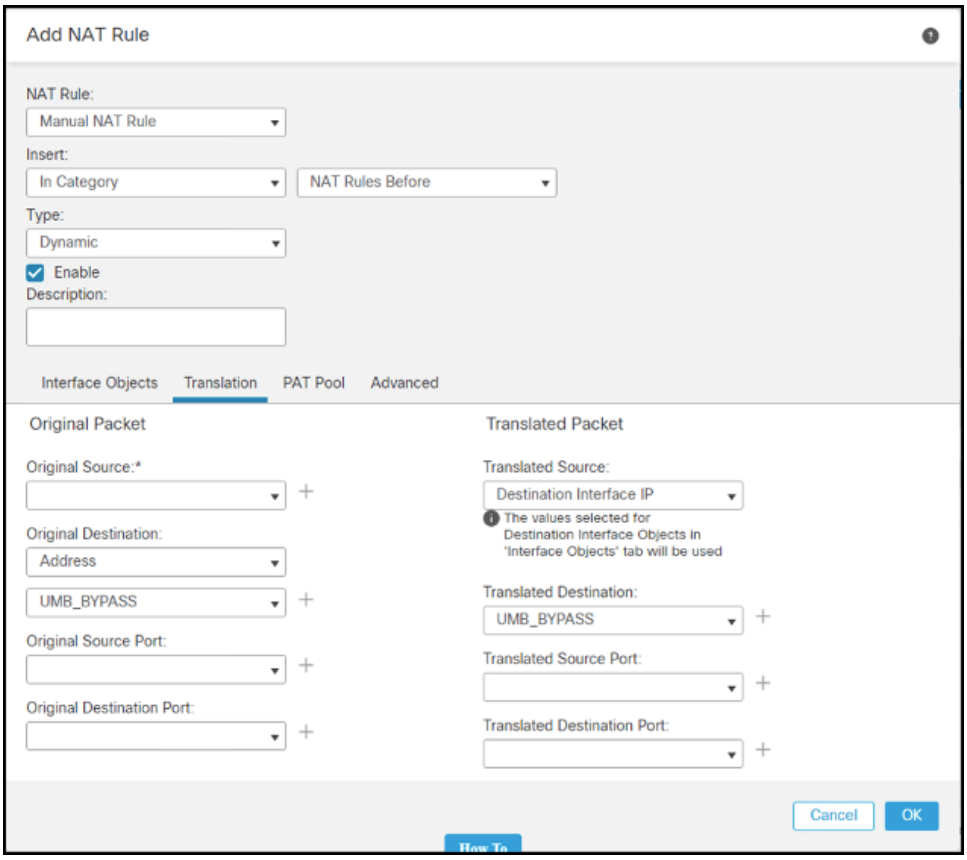
1. In Cisco Secure Firewall Management Center, navigate to **Devices** > **NAT** > **New Policy** > **Threat Defense NAT**.
2. Enter a name, then select the FTD device to apply the policy.



3. Click **Save**.
4. Click **Add Rule**.



a) **NAT Rule**: Select **Manual NAT Rule**.
b) **Type**: Select **Dynamic**.
c) Under **Interface Objects** > **Source Interface Objects** > **, select** > **Inside**.
d) **Destination Interface Objects**: Select **Outside**.
e) Under **Translation** > **Original Source**, select a network object containing the internal subnet.
f) **Original Destination**: Specify the Secure Access bypass network object created previously (`UMB_BYPASS` in this example).



Note

This object contains the Secure Access resolvers' IP address, as well as (optionally) the `146.112.0.0/16` and `155.190.0.0/16` networks, plus any other traffic you may want to exempt from the tunnel. Using this object facilitates the configuration, because when hosts and subnets are added or removed from the object, both the IPsec traffic selector and NAT statement are updated.

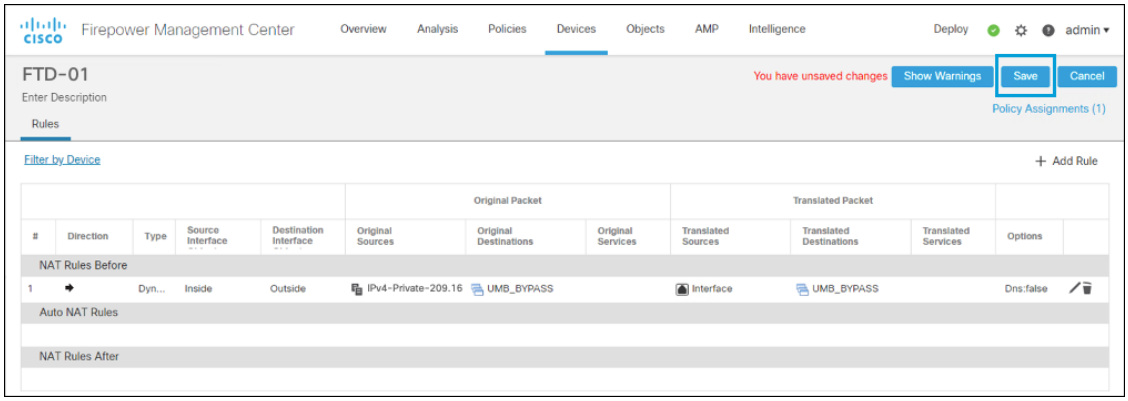
g) **Translated Source**: Select **Destination Interface IP**.

h) **Translated Destination**: Select the same object selected for **Original Destination** (`UMB_BYPASS` in this example).

This ensures that the internal network is NATed to the interface IP address only when the destination is the network object containing the resolver's IP address. Other destinations do not match the NAT statement.

i) Click **OK**.

j) Click **Save**.



The NAT policy is configured.

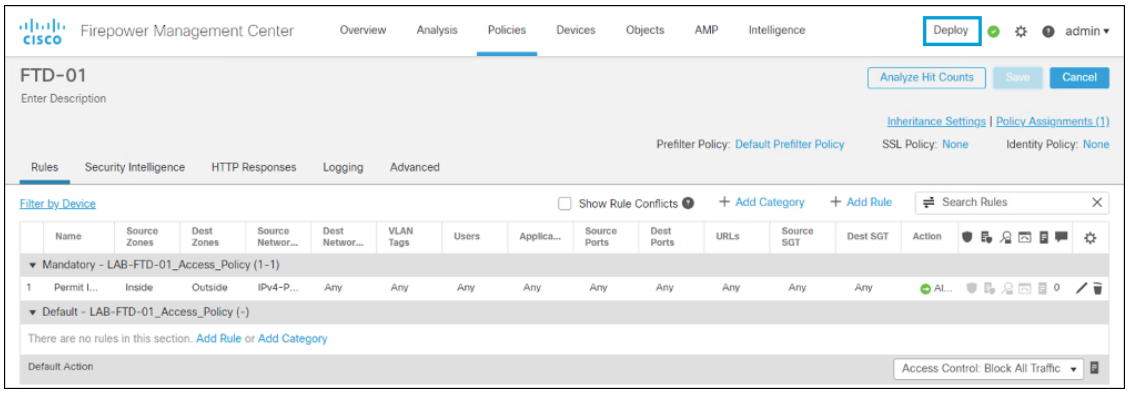
Configure Access Policy

Provides instructions for completing the Configure Access Policy workflow in Cisco Secure Access. At a minimum, an entry permitting inside traffic going out should exist.

The Access Policy in Secure Firewall combines all the other policies (SSL Decryption, DNS, Pre-filter, Identity).

Procedure

1. At a minimum, an entry permitting inside traffic going out should exist. In production environments, you normally add more specific access entries.



2. Enable the policy by clicking **Deploy** in the top configuration bar.

Configure Secure Firewall VTI, PBR, and Per Tunnel Identity

Describes Configure Secure Firewall VTI, PBR, and Per Tunnel Identity in Cisco Secure Access. At a high level, the Secure Firewall configuration process consists of the following steps.

At a high level, the Secure Firewall configuration process consists of the following steps.

1. Configure Site-to-Site VPN
2. Configure Policy-based Routing
3. Configure Access Policy

To start the configuration, log in to your Cisco Secure Firewall Management Center web interface at its IP address or FQDN; for example, `https://FMC_IP_OR_FQDN`.

Configure Tunnels in Secure Access

Describes Configure Tunnels in Secure Access. Threat Defense can authenticate to Secure Access by using a pre-shared key (PSK) and email or IP address identity.

Threat Defense can authenticate to Secure Access by using a pre-shared key (PSK) and email or IP address identity. If the Secure Firewall is behind a NAT device, email identity is the only possible option.

You can use virtual tunnel interface with policy-based routing (PBR) and per-tunnel identity when you configure the Threat Defense side of the tunnel.

Follow the steps in Add Network Tunnel Group to create the Secure Access side of the tunnel for the Threat Defense tunnels. When you configure the network tunnel group, be sure to select email as the tunnel ID.

The new tunnel appears in Secure Access with a status of *UnEstablished*. The tunnel status is updated once the first IKEv2 INIT message containing the tunnel identity is received in one of the Secure Access data centers.

For an end-to-end configuration example of setting up redundant tunnels in Firewall Threat Defense, see *Configure Secure Access with Secure Firewall with High Availability*, https://www.cisco.com/c/en/us/support/docs/security/secure-access/222648-configure-secure-access-with-secure-fire.html.

Configure Site-to-Site VPN

Provides instructions for completing the Configure Site-to-Site VPN workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

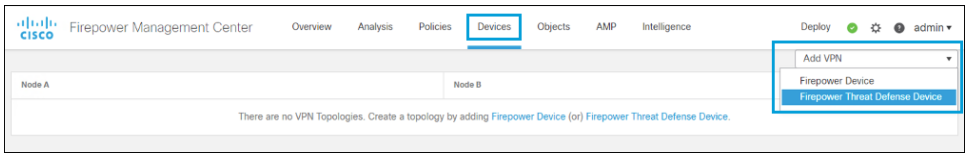
You can now configure the site-to-site VPN.

This example configures a single tunnel to the primary Secure Access hub. You can configure as many tunnels as needed for bandwidth and backup so long as the VTI IP addresses are unique. Simply repeat the process and ensure that you use the email for the primary or the secondary tunnel ID as appropriate for each site-to-site VPN connection. You should have tunnels to both hubs to ensure redundancy in case or failure or when Secure Access performs maintenance.

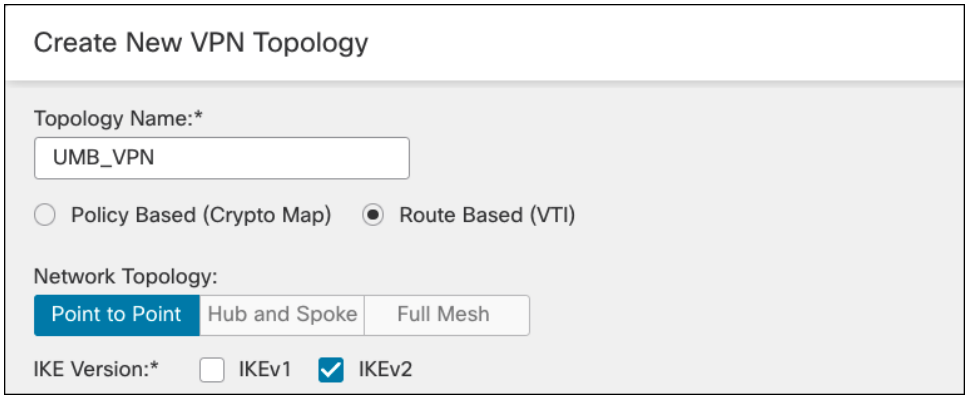
For an example of configuring a single site-to-site VPN connection with both primary and secondary VTIs, see *Configure Secure Access with Secure Firewall with High Availability*, https://www.cisco.com/c/en/us/support/docs/security/secure-access/222648-configure-secure-access-with-secure-fire.html.

Procedure

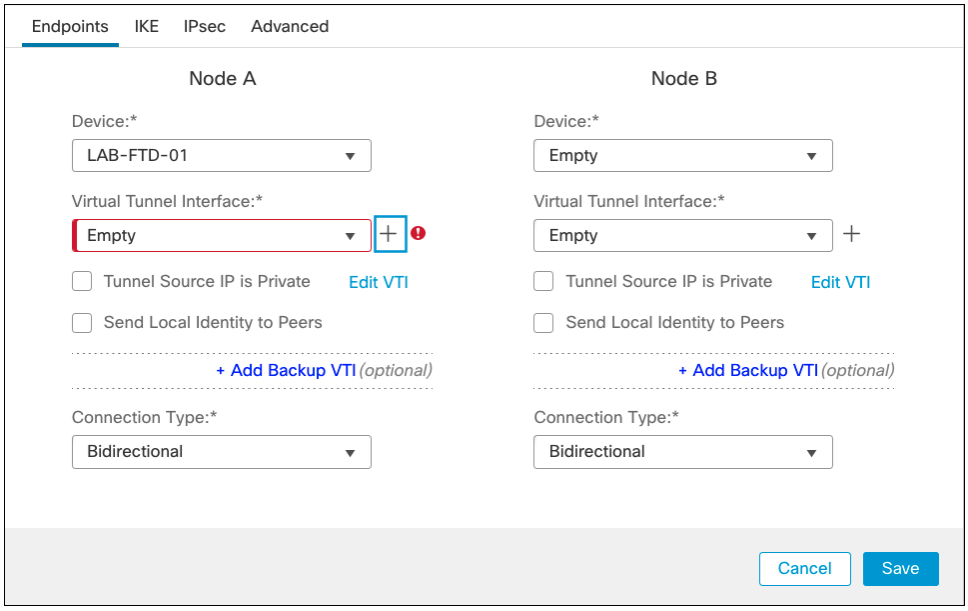
1. Navigate to **Devices** > **VPN** > **Site to Site** > **Add VPN** > **Secure Firewall Threat Defense Device**.



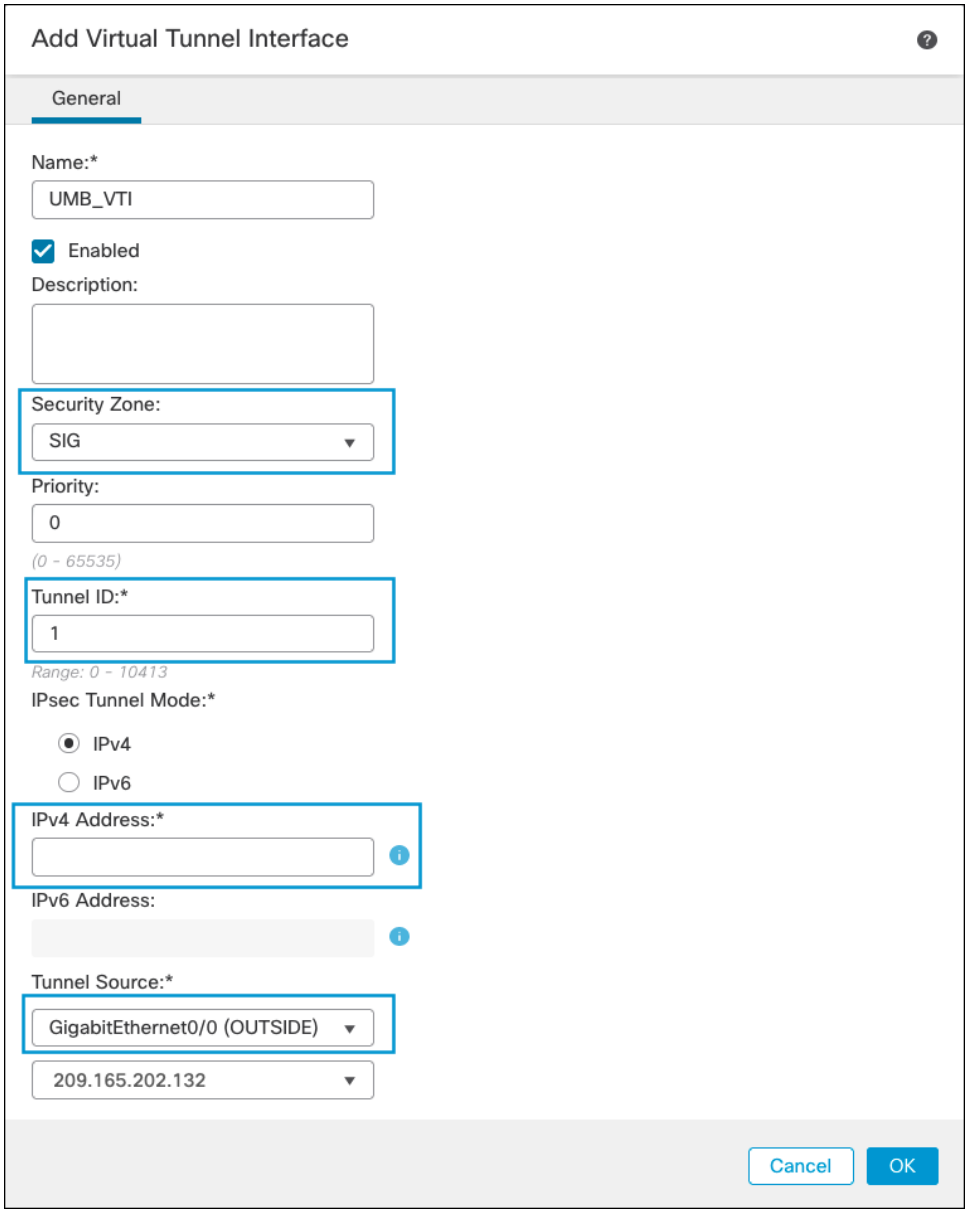
2. Enter a name for the topology, select **Route Based (VTI)**, and check IKEv2 box. For more information about supported protocols, see Supported IPSec Parameters.



3. Choose a Secure Firewall device from the **Device** drop-down list for Node A and click **Add** to add a Virtual Tunnel Interface.

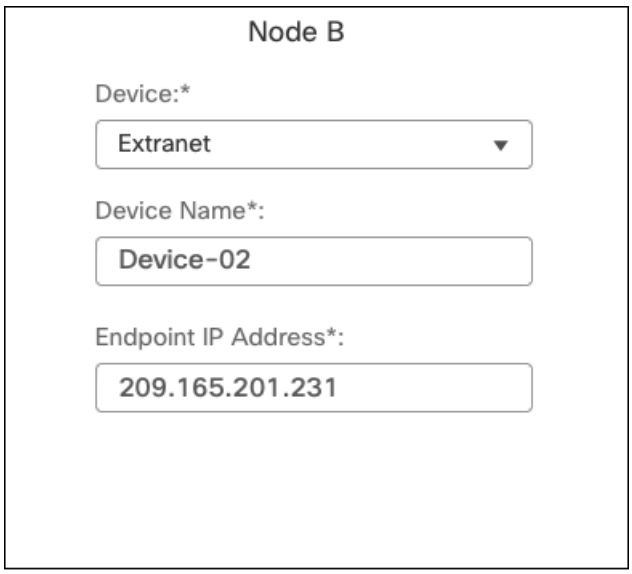


4. Enter a name for the VTI, choose an existing **Security Zone** or create a new for the tunnel, enter a **Tunnel ID** and an IP address (a /30 subnet to accommodate local device and remote IP), and select the **OUTSIDE** interface as tunnel source. Then click **Ok**.

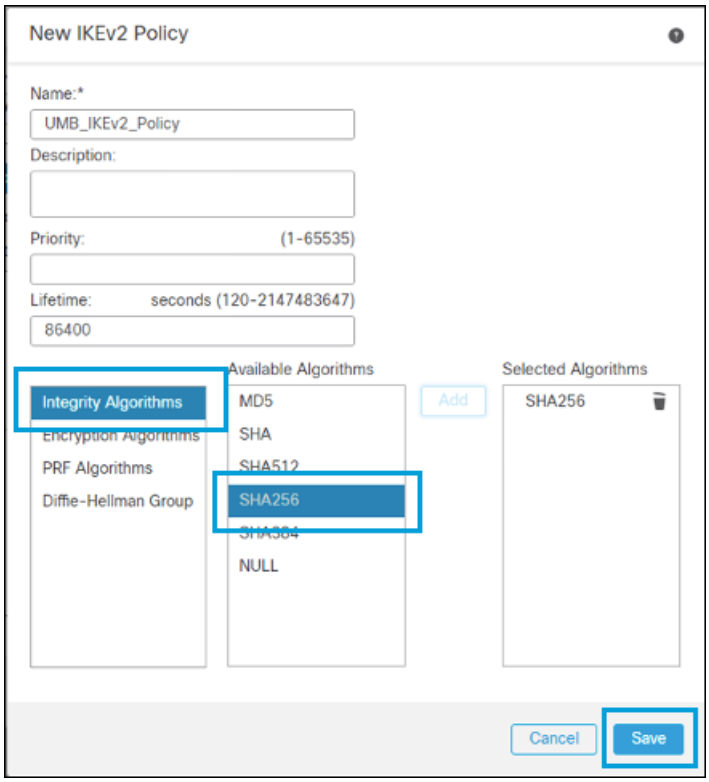


5. Select the VTI you just created and check **Send Local Identity to Peers**.
   a. Select **Email ID** from the **Local Identity Configuration** dropdown.
   b. Enter the email address that is the primary tunnel ID from the Secure Access network tunnel group to which you are connecting.

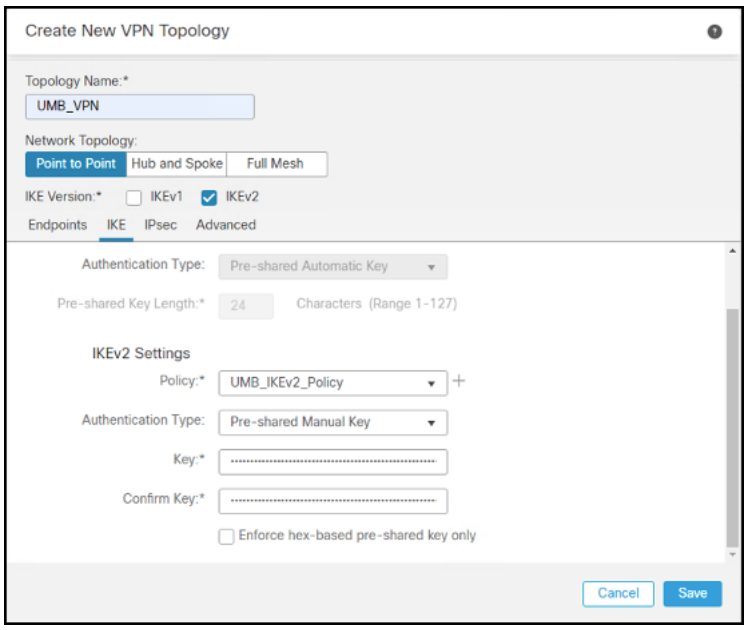
6. Under Node B, choose **Extranet** as the device, enter a name and IP address of a Secure Access data center.



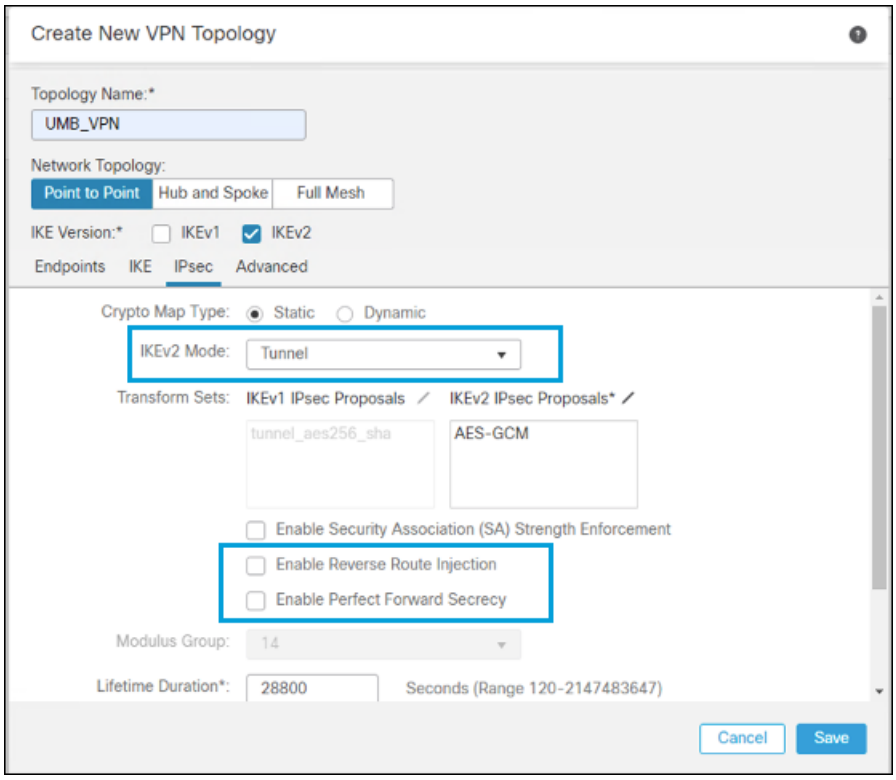
7. Enter a name for the IKEv2 policy, then select the parameters from the list.



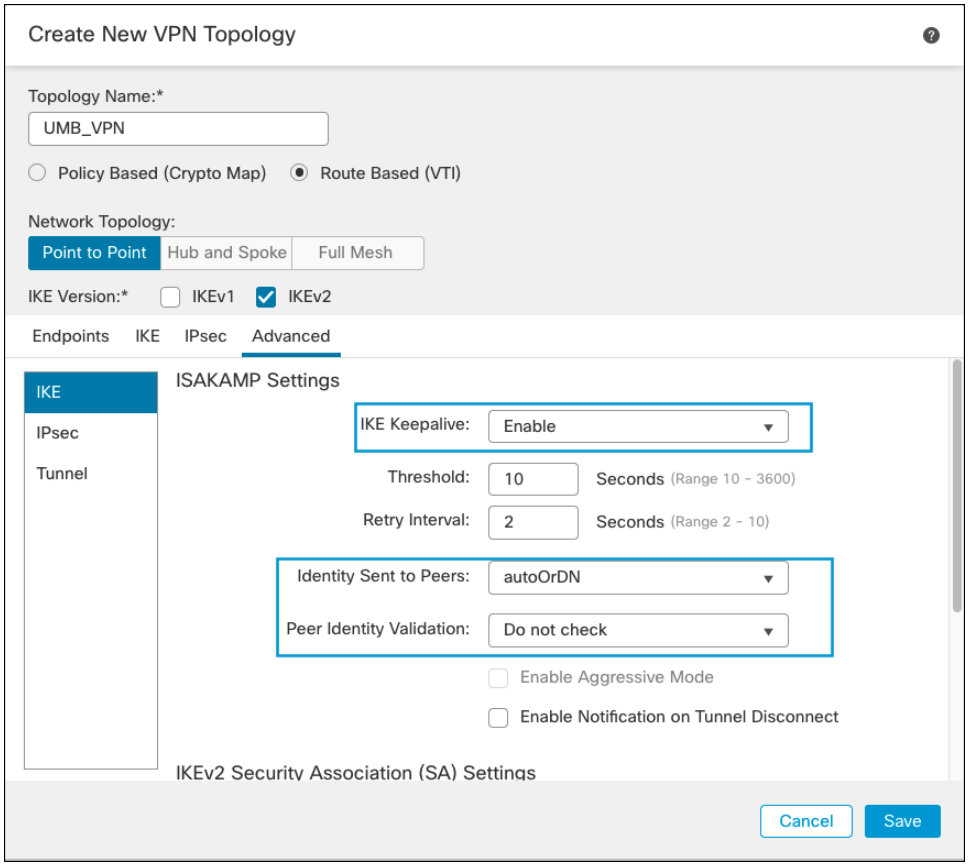
8. After saving the IKEv2 Policy, select it. Choose **Pre-shared Manual Key** from the **Authentication** drop-down list and enter the key.



9. Under **IPSec Configuration**, add a new **IKEv2 IPsec Proposal** with your crypto algorithms or select an existing profile. Select **Tunnel** for **IKEv2 Mode** and uncheck **Enable Reverse Route Injection** and **Enable Perfect Forward Secrecy**.



10. In the **Advanced** tab under IKE, enable **IKE Keepalive**. Select **autoOrDN** as the **Identity Sent to Peers**, and disable **Peer Identity Validation**. Then click **Save**.



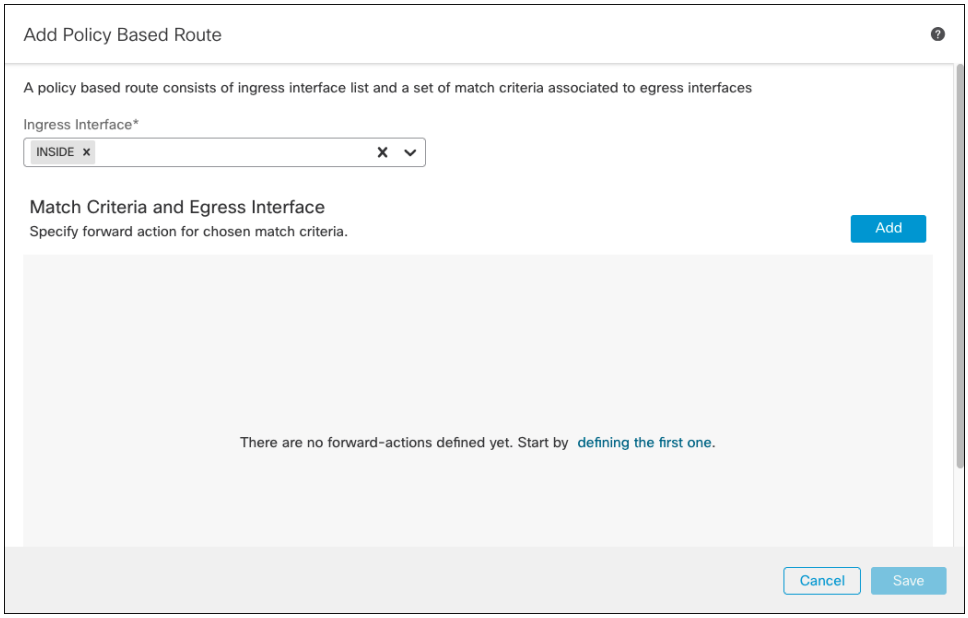
Configure Policy-based Routing

Provides instructions for completing the Configure Policy-based Routing workflow in Cisco Secure Access. Use policy-based routing to determine the traffic that is sent to each tunnel.

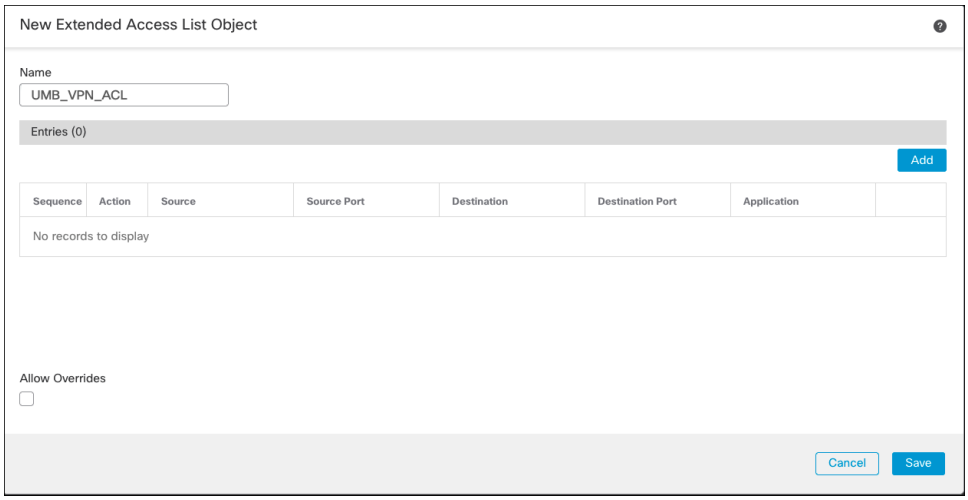
Use policy-based routing to determine the traffic that is sent to each tunnel. If you configure multiple tunnels, use the policy-based routing ACLs to divide traffic appropriately among the tunnels for load balancing.

Procedure

1. Navigate to **Devices > Device Management** and click the name of the device to edit.
2. Under **Routing > Policy Based Routing**, click **Add** to add a new policy
3. Choose the **Inside** for the Ingress Interface (user's facing interface where PBR will be applied) and click **Add**.

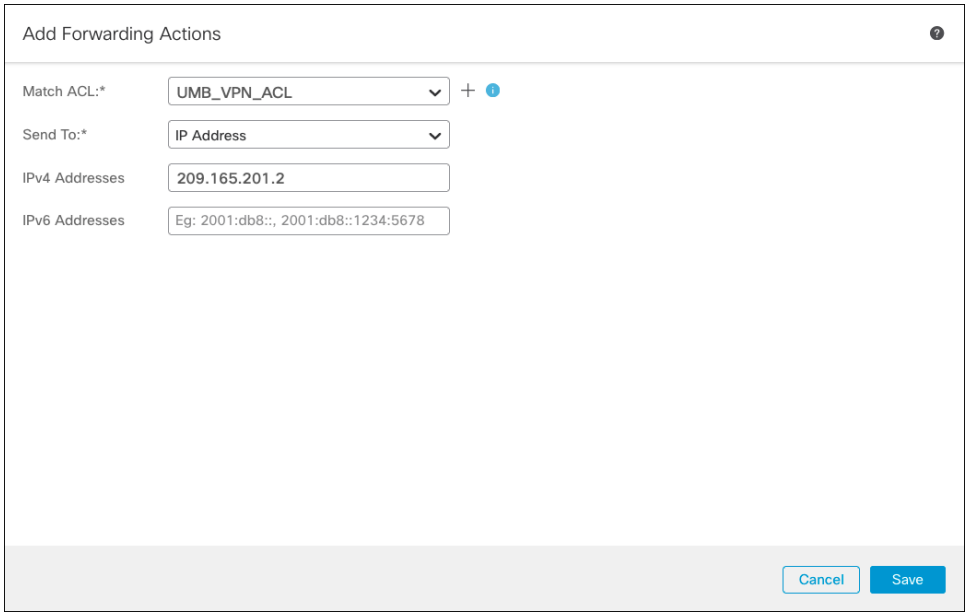


4. Choose the existing extended ACL, and click **Add**.



Alternatively, if you are creating a new ACL, enter a name and add Access Control Entries (ACE) matching the traffic that should be redirected to Secure Access.

5. Click **Save** to add the access entries.
6. Under **Match ACL**, choose the newly created ACL and under **Send To** choose **IP Address**. Type the IP address in the same subnet previously used for VTI and click **Save**



7. Click **Save** to save the configuration and deploy.

Configure Access Policy

Describes Configure Access Policy in Cisco Secure Access. If not yet allowed by the access policy, add an access entry allowing traffic from inside the network to the Secure Access tunnel.

If not yet allowed by the access policy, add an access entry allowing traffic from inside the network to the Secure Access tunnel.

Troubleshooting

Describes Troubleshooting in Cisco Secure Access. Cisco Secure Firewall Management Center has a VPN troubleshooting tab where VPN-related events are displayed.

Cisco Secure Firewall Management Center has a VPN troubleshooting tab where VPN-related events are displayed. By default, only error messages are sent from FTD to Cisco Secure Firewall Management Center, as LINA code (ASA) is responsible for the IPSec tasks the same commands available for troubleshooting the ASA devices are available in FTD.

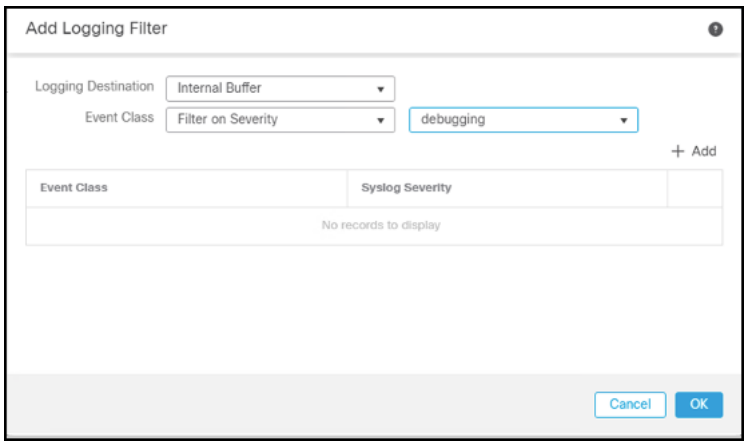
If you need to send VPN debug messages to Cisco Secure Firewall Management Center, change the logging level in the Platform Settings policy. This policy is configured and added in **Devices** > **Platform Settings**. VPN logging to Cisco Secure Firewall Management Center is in the Syslog section of the Platform Settings policy from the Logging Setup tab. It is also possible to send logging messages to other destinations, such as the FTD device internal buffer.

Enable Logging for Debugging

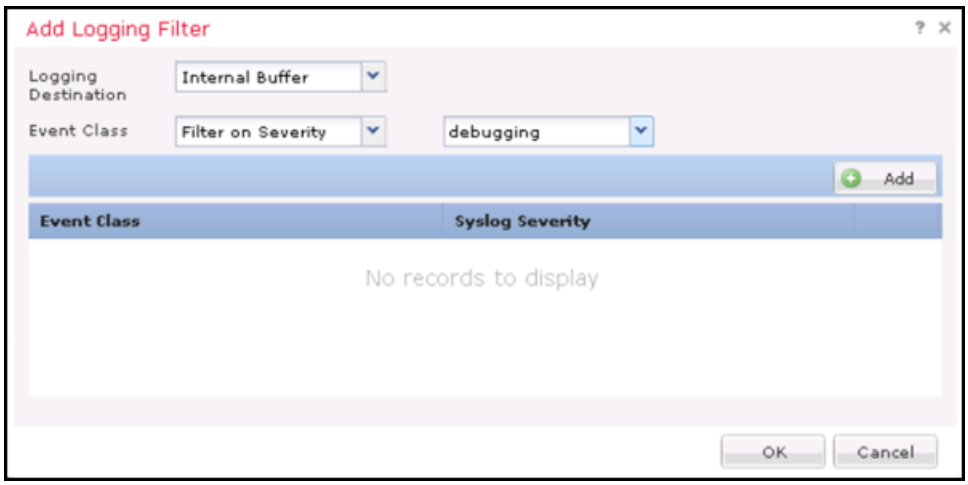
Provides instructions for completing the Enable Logging for Debugging workflow in Cisco Secure Access. In Cisco Secure Firewall Management Center, navigate to Devices Platform Settings .

Procedure

1. In Cisco Secure Firewall Management Center, navigate to **Devices** > **Platform Settings**.
2. Under **Basic Logging Settings**, add a logging destination.



3. Under **Logging Destinations** tab, click **Add**, then select **Internal Buffer** (or another logging destination). Set the logging level to **Debugging**.



When logging is enabled, you can enable IKEv2 debug, SSH to FTD. Then enter type `debug crypto ikev2 platform` and `debug crypto ikev2 protocol`. These two debugging options provide detailed information about IKEv2 negotiation.

```
Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

> debug crypto ikev2
  ha         debug the ikev2 ha
  platform   debug the ikev2 platform
  protocol   debug the ikev2 protocol
  timers     debug the ikev2 timers

> debug crypto ikev2 platform
> debug crypto ikev2 protocol
>
```

4. After enabling debugging in the FTD device, return to Cisco Secure Firewall Management Center and navigate to **Devices** > **VPN** > **Troubleshooting**. IKEv2 negotiation debugging information is available.

   If debug destination internal buffer was configured, going back to the FTD device via SSH is also possible. This enables you to see debug messages in the FTD terminal.

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, 197 messages logged
 Bytes rcv: 24260, Reason: Internal Error
%FTD-7-609002: Teardown local-host identity:188.40.190.251 duration 0:02:54
%FTD-7-609002: Teardown local-host Outside:146.112.97.2 duration 0:02:54
%FTD-7-710005: UDP request discarded from 0.0.0.0/68 to Outside:255.255.255.255/
7
%FTD-7-710005: UDP request discarded from 0.0.0.0/68 to Inside:255.255.255.255/6
```

To access the LINE portion of the code, enter the command `system support diagnostic-cli`.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FF-FTD-01# show ver
FF-FTD-01# show version
--------------[ FF-FTD-01.sig.local ]---------------
Model                     : Cisco Firepower Threat Defense for VMWare (75) Versio
n 6.5.0 (Build 115)
UUID                      : 567ce6e8-deb6-11e9-9e95-b425c64212f5
Rules update version      : 2019-08-12-001-vrt
VDB version               : 327
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.13(1)
SSP Operating System Version 2.7(1.105)

Compiled on Thu 19-Sep-19 17:23 PDT by builders
System image file is "boot:/asa9131-0-smp-k8.bin"
Config file at boot was "startup-config"
```

Configure Tunnels with Meraki MX

Understand the methods that you can use to configure network tunnels between your Meraki MX and Secure Access.

You can configure tunnels from your Meraki MX to Cisco Secure Access, using one of the following methods:

1. Single Manual Tunnel (non-Meraki VPN with no BGP).
   - Step 1: Add a Network Tunnel Group in Secure Access.
   - Step 2: Configure a Tunnel in Meraki MX.
2. Primary and Secondary non-Meraki Tunnels with BGP.
   - See the Meraki guidebook on Meraki SD-WAN Secure Access Design Guide.
   - For failover and BGP, see Cisco Secure Access Meraki BGP Configuration Guide.
3. Integration of Meraki SD-WAN Auto-VPN Tunnels with Cisco Secure Access.
   - Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels.
   - Integrate Cisco SASE with Meraki SD-WAN.

Prerequisites for Tunnels with Meraki MX

Describes Prerequisites for Tunnels with Meraki MX in Cisco Secure Access. Your Cisco Meraki MX/Z4 device must be running the appropriate firmware version based on your tunnel connection method: MX 18.107+ firmware: Required for a Single tunnel.

- Your Cisco Meraki MX/Z4 device must be running the appropriate firmware version based on your tunnel connection method:
  - MX 18.107+ firmware: Required for a Single tunnel.
  - MX 19.1.6+ firmware: Required for Secondary tunnels with Health checks (SIA). For more information, see Cisco Secure Access Meraki SD-WAN Configuration Guide.
  - MX 19.1.6+ firmware: Required for Tunnels with BGP (SIA + SPA). For more information, see Cisco Secure Access Meraki BGP Configuration Guide.
- You must have a valid Cisco Secure Access account.
- You must configure a network tunnel group in Cisco Secure Access; see Add a Network Tunnel Group.

You can check firmware compatibility by navigating to Product Firmware Version Restrictions.

Caveats and Considerations

Describes Caveats and Considerations in Cisco Secure Access. This section discusses important caveats and considerations associated with the Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

This section discusses important caveats and considerations associated with the Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

1. There is no stateful failover to a Secure Access secondary tunnel.
   a. The MX only supports active/cold standby to a single headend.
   b. Traffic from a failed site is required to reestablish the tunnel.
2. Static routing and BGP are both supported. For more information, see the Prerequisites in Configure Tunnels with Meraki MX.
3. Requires traffic to be generated from the LAN side of an MX through the non-Meraki VPN to establish connection.
   a. Remote application access on Meraki networks through an MX is not possible until traffic is initiated from the application side of the MX through the non-Meraki VPN.
   b. Traffic will also need to be consistently generated from the LAN side of the MX over each non-Meraki VPN to keep the tunnel from timing out.
4. ECMP/Load balancing is not supported. Only a single IPSec tunnel is supported between a single Meraki network and a Secure Access network tunnel group.
5. A unique public uplink IP is required for each network.
   a. The public uplink IP is used as the MX peer device IP, and this cannot be changed.
6. In the Secure Access dashboard, the network tunnel group will display the status as **Warning**. This is because the Meraki network cannot build a standby tunnel to the Secondary Hub in the network tunnel group that is provided for intra-region redundancy.

Restrictions for health check

The integration between Cisco Secure Access and Meraki MX uses static routing IPsec tunnels. Meraki MX establishes primary and secondary IPsec tunnels to Cisco Secure Access, and leverages its built in uplink health checks to perform automatic failover between tunnels. This provides a resilient and high-availability configuration for branch connectivity.

These limitations apply to health checks:

- Due to Meraki limitations in health check IP flexibility, only one tunnel group is supported in Private Access mode. If multiple Meraki MX devices need to connect to Secure Access for Private Access, you must either use BGP for dynamic routing, or configure static tunnels.
- Only one Network Tunnel Group can support health checks and high availability. Additional tunnels operate without health monitoring or redundancy.

Supported Use Cases and Requirements

Describes Supported Use Cases and Requirements in Cisco Secure Access. The following sections describe supported use cases for Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

The following sections describe supported use cases for Meraki Third Party (non-Meraki) VPN tunnel configuration to Secure Access.

Remote Access VPN and ZTA

Single Manual Tunnel (No BGP):

- The Meraki networks will need to be tagged.
- Use the Umbrella IKEv2 configuration.
- No default exit hub.
- No spokes.

BGP Tunnels, see Cisco Secure Access Meraki BGP Configuration Guide.

Branch-to-Branch through Secure Access

One of the following options is required to enable Secure Access policy enforcement to apply to branch-to-branch communication. Otherwise, all traffic will traverse Meraki AutoVPN between Meraki networks directly.

1. Each network hosting applications is in a separate org; or
2. All networks are in a single org. **Note:** If this is the case, contact Support to have hub-to-hub communication turned off.

Secure Internet Access with Non-Meraki VPN

The following are requirements for this configuration:

- No AutoVPN default route.
- Local route configuration 0.0.0.0/0.

Step 1: Add a Network Tunnel Group in Secure Access

Provides instructions for completing the Step 1: Add a Network Tunnel Group in Secure Access workflow in Cisco Secure Access. Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.

Secure Access enables fast, reliable, and secure private network connections to your applications through IPsec (Internet Protocol Security) IKEv2 (Internet Key Exchange, version 2) tunnels.

Tunnels and tunnel groups are core concepts in managing connections between your data centers and Cisco Secure Access. A network tunnel group provides the framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources.

Procedure

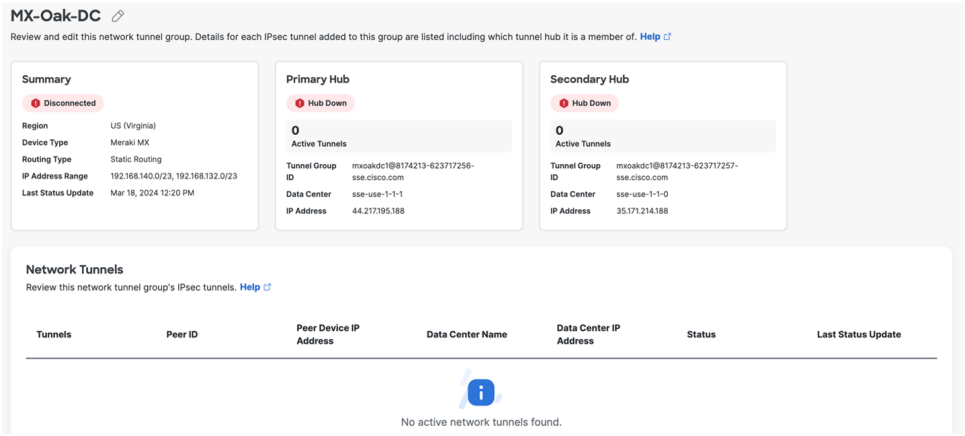
1. Follow the steps in Add a Network Tunnel Group.
2. Make note of the **Tunnel ID** and **Passphrase** you enter when configuring the network tunnel group. These values are needed when you configure your Meraki IPsec tunnel.

   > **Note**
   >
   > Secure Access provides the option to download a CSV file with the network tunnel group details.

3. Remember to select **Static routing** under routing options.

What to do next

The new network tunnel group appears in the Secure Access dashboard as **Disconnected**, and with the **Primary Hub** and **Secondary Hub** status showing as **Hub Down**. The network tunnel group status is updated once it is fully configured and connected with Meraki MX.



See the Verification and Troubleshooting section for additional information about how to evaluate the network tunnel group status.

Step 2: Configure a Tunnel in Meraki MX

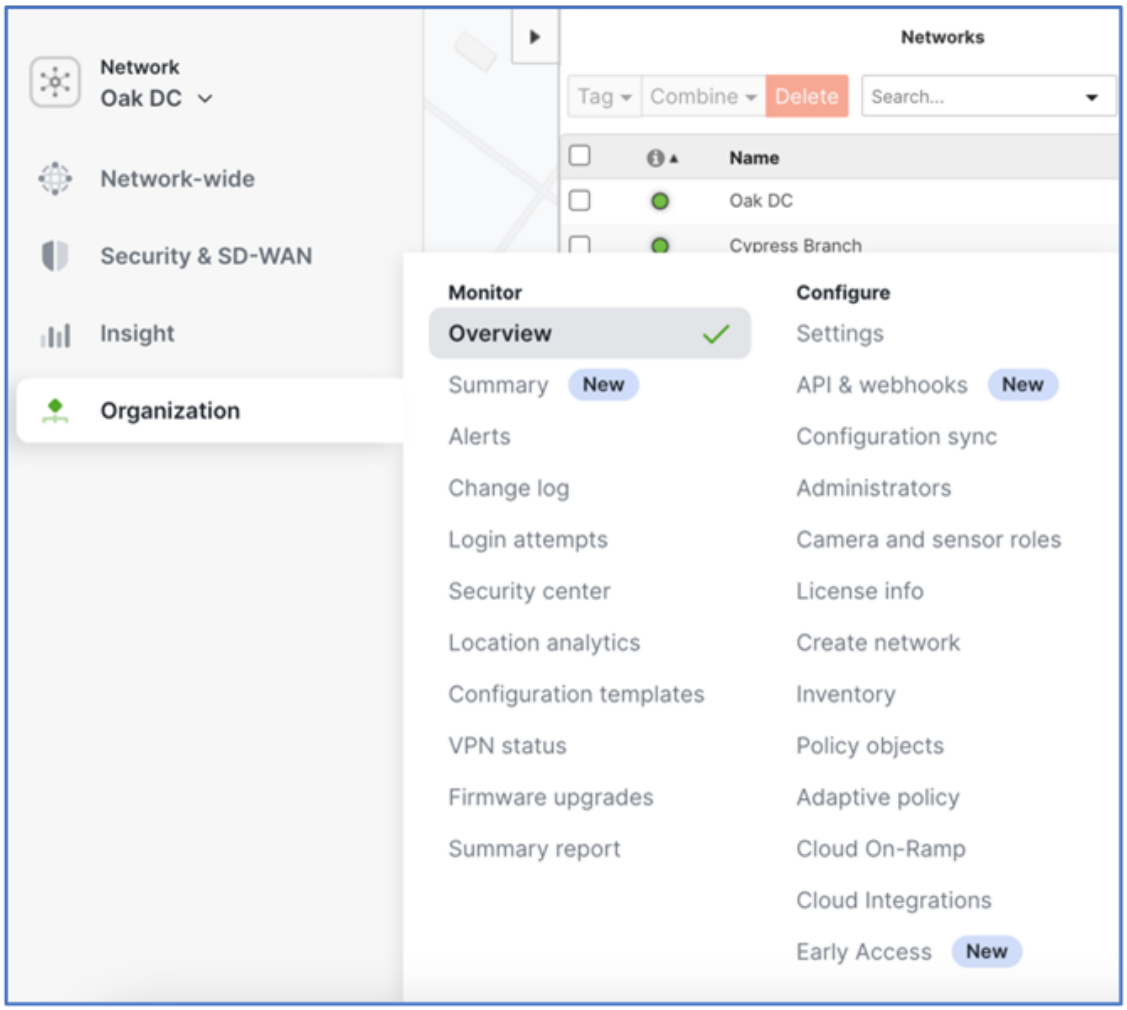
Provides instructions for completing the Step 2: Configure a Tunnel in Meraki MX workflow in Cisco Secure Access. Configure a Meraki Third Party (non-Meraki) VPN tunnel to connect a Meraki MX/Z4 series device to Cisco Secure Access.

Configure a Meraki Third Party (non-Meraki) VPN tunnel to connect a Meraki MX/Z4 series device to Cisco Secure Access.

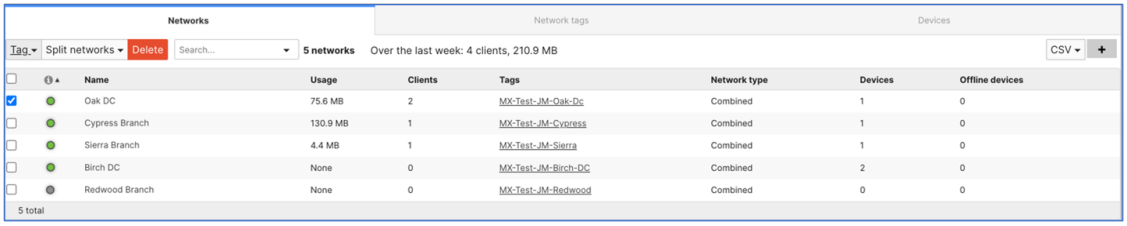
Procedure

1. In the Meraki MX dashboard, navigate to the **Organization** > **Monitor** > **Overview** page.

   If the page is not expanded by default, expand the **Networks** list by clicking the left-facing arrow at the top of the network list.

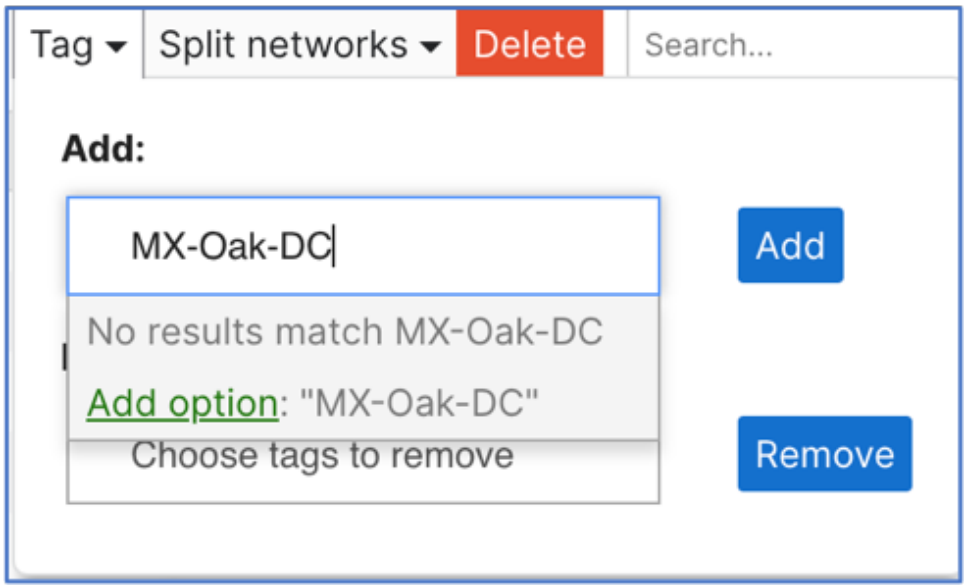


2. Select the desired network from the networks **Name** list. Select only the network that will connect to the Secure Access Network Tunnel Group.

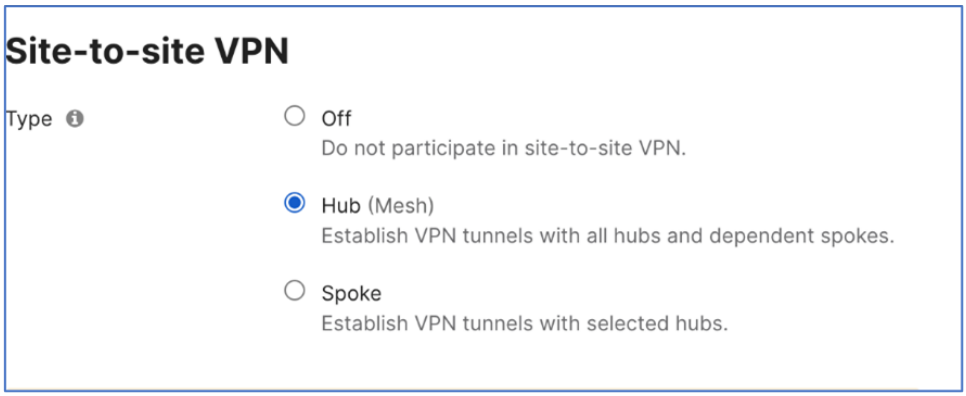


3. Add a Network tag to the selected network. Select the **Tag** dropdown menu from the top left. A tag can be created by typing into the field and then clicking **Add**.

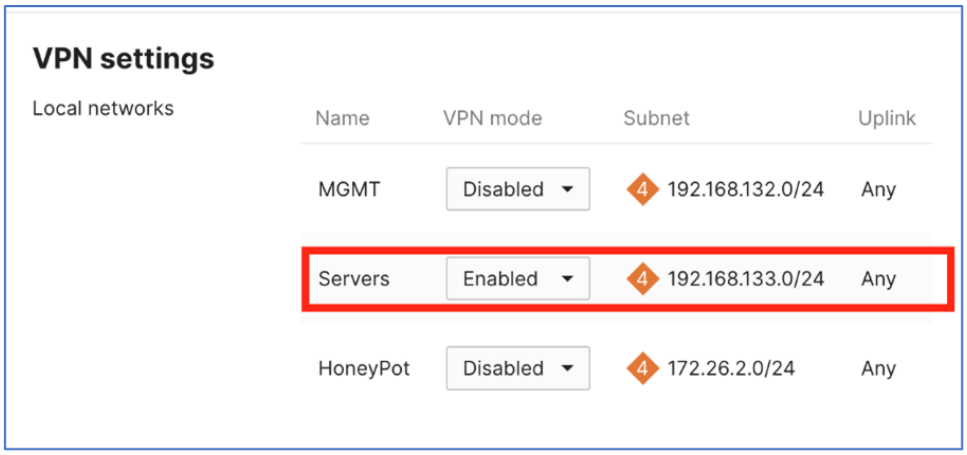
> **Note**
>
> It is recommended that the same name is used for the Meraki Network Tag as the Secure Access Network Tunnel Group.



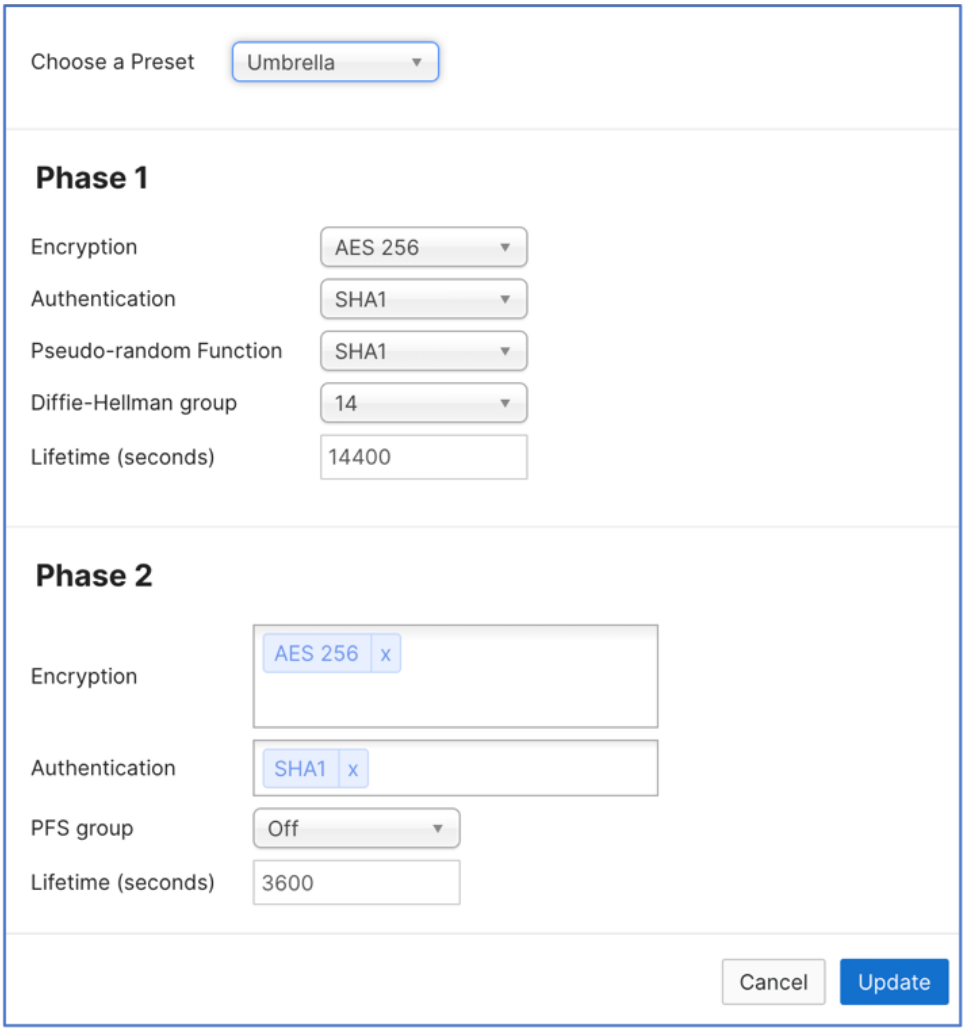
4. While in the Meraki dashboard, navigate to **Security & SD-WAN** > **Site-to-site VPN**, and choose **Hub (Mesh)**.



5. Next, in the same section, find the **VPN settings** and choose **Enabled** for the VLANs that will use the new Secure Access network tunnel group.



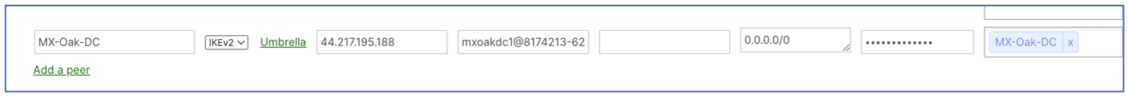
6. Scroll down to find **Organization-wide settings** to locate the **Non-Meraki VPN Peers** section. Click **Add a peer** and then add the tunnel ID and tunnel passphrase that you created in Step 1: Add a Network Tunnel Group in Secure Access.
7. Configure the IPsec parameter settings:
   - **Name**–Provide a meaningful name for the tunnel.
   - **IKE Version**–Select IKEv2.
   - **IPsec policies** Choose the predefined Umbrella configuration; see Supported IPsec Parameters.



- **Public IP**–IP address to connect to Secure Access Network Tunnel Group Primary Data Center IP.
- **Local ID**–The Primary Tunnel ID for the Network Tunnel Group.
- **Remote ID**–Leave this blank.
- **Private subnets**–There are 2 common configurations for Private Subnets:
  - If the desired behavior is to use Secure Internet Access and Secure Private Access to access applications on tunnel-enabled vlans/subnets, then the only entry here should be 0.0.0.0/0. This will route all traffic to Secure Access for either Secure Internet Access, Remote Access VPN, or ZTA clients.
  - If only Remote Private Application access is required, then all subnets that are used by the Secure Access infrastructure must be entered:
    a. CGNAT 100.64.0.0/10
    b. RA VPN and Management IP Pool subnets.
- **Preshared secret**–This is the **Passphrase** for the Network Tunnel Group created in Secure Access.
- **Availability**–Enter the Network tag you defined earlier for the MX appliance that builds the tunnels to Secure Access.

Important

Do not leave this field blank. Ideally this field should match the Network tag entered in Step 3 above. Leaving this field blank, "All Networks", or entering a tag that is associated with multiple networks could cause one or more tunnels to become unstable. This could lead to unexpected behavior and cause an NMVPN tunnel to not be established.



8. Click **Save**.

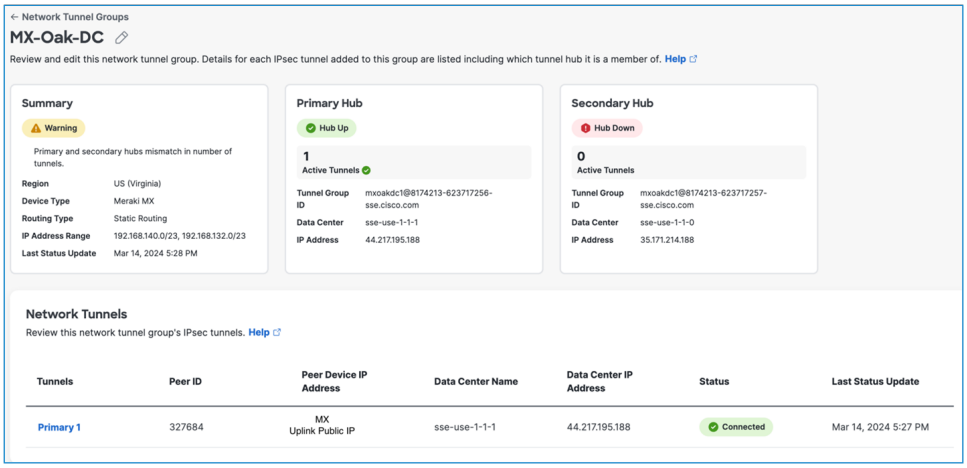
   Upon completion of these steps, you should have a functioning tunnel routing your traffic as intended.

Verification and Troubleshooting

Provides instructions for completing the Verification and Troubleshooting workflow in Cisco Secure Access. The Secure Access Network Tunnel Group will move from Disconnected Status to Warning.

Procedure

1. The Secure Access Network Tunnel Group will move from **Disconnected** Status to **Warning**. This change could take several minutes and may require a test ping described in step 2 below.



Note

Network Tunnel Group Status

The Network Tunnel Group will never move from a **Warning** status to **Connected**. This is because the Network Tunnel Group is designed to have a Primary and Secondary tunnel connected to each Hub for failover. Traffic will pass to the **Primary Hub** even if the Network Tunnel Group status is **Warning**.

2. Run `ping` tests from the new VLAN to the internet. For more information, see Using the Ping Live Tool.
3. Check the status of the VPN tunnel. For more information, see VPN Status Page.
4. Follow the VPN troubleshooting procedures. For more information, see Troubleshooting Non-Meraki Site-to-site VPN.

Note

Cisco Meraki does not support policy based routing. It is not possible to do client side routing to determine if specific traffic belongs inside or outside the tunnel. However, it is possible to choose if an entire VLAN is tunneled to Secure Access.

Optional Configurations

Describes Optional Configurations in Cisco Secure Access. To create a VLAN for the subnet to redirect to Secure Access, see Configuring VLANs on the MX Security Appliance.

1. To create a VLAN for the subnet to redirect to Secure Access, see Configuring VLANs on the MX Security Appliance.
2. To create a new SSID for the VLAN, see Configuring Simple Guest and Internal Wireless Networks.

Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels

Understand how to enroll Meraki SD-WAN sites with Secure Access using Meraki auto-VPN tunnels.

Cisco SASE (Secure Access Service Edge) securely connects users, devices, and applications from anywhere with minimal effort. Meraki Auto-VPN tunnels can be enrolled to seamlessly connect Meraki sites as network tunnel groups in Secure Access.

For complete documentation of Cisco SASE with Cloud Managed Meraki SD-WAN and Secure Access, refer to SASE in Meraki documentation.

Before you begin

Before you begin, review the following prerequisites.

- A Cisco Meraki MX/Z4 device (running Security and SD-WAN (MX,Z) version 19.1+ firmware). For more information, refer to Meraki Security and SD-WAN (MX,Z) Features Directory.
- A valid Meraki SD-WAN license or subscription.
- A valid Cisco Secure Access subscription.
- An integration established between Secure Access and Security Cloud Control. For more information, refer to About Cisco Security Cloud Control.
- A Cisco SASE integration established between Cloud Managed Meraki SD-WAN and Secure Access. For more information, refer to Integrate Cisco SASE with Meraki SD-WAN in Secure Access Integrations documentation and SASE in Meraki Integrations documentation.

Procedure

Enrolling a Meraki Site

Perform the following steps to enroll a Meraki site. For more information, refer to Cisco SASE: Sites Connectivity.

1. In the Meraki dashboard, navigate to **SASE** > **Sites**.
   a) Click **+ Add Site**.
   b) In the **Assign regions to networks** menu, select an unassigned Meraki branch.
   c) Click the **Assign a region** dropdown list and select a Secure Access region. The branch will now be listed under **Newly assigned regions**.
   d) Click **Next**.
   e) Under **Review and confirm**, verify your Meraki branch selection, then click **Save and Finish**.
   The Sites table displays the newly enrolled site.
   f) To verify the enrollment and monitor VPN status, navigate to **Security & SD-WAN** > **Monitor** > **VPN Status**.
   This page shows the cloud hubs and their VPN registry information.
2. In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
   a) Search for your Meraki site by region to verify that the Auto-VPN tunnel connection created a network tunnel group in Secure Access.
   b) Click the tunnel group name to view details. The Meraki site name will match the Secure Access network tunnel names in the network tunnel group.

   For more information, refer to View Network Tunnel Group Details.

What to do next

Configure Access Policy

Once the Auto-VPN tunnels are connected, Meraki sites appear as network tunnel groups in Secure Access. Protect one or more Meraki sites by configuring Secure Access private and internet access rules.

For more information, refer to Manage the Access Policy in Secure Access documentation and Cisco SASE: Policy in Meraki documentation.

Configure Tunnels with NEC IX2000 Series Router

Understand how to configure an IPsec tunnel between an NEC IX2000 Series Router and Secure Access.

The content provided here explains how you can configure an IPsec tunnel with NECIX2000 Series Router. The objective is to protect devices behind the NEC IX2000 Series Router through a route-based IPsec tunnel. Follow these steps to connect the Cisco router to Secure Access.

Refer to Supported IPsec Parameters.

Before you begin

The following prerequisites must be met for the tunnel to work successfully.

Licensing

- A valid Cisco Secure Access account.
- A Cisco Secure Access organization ID. For more information, see Find Your Organization ID.

Network Access

- You must select a Secure Access data center IP address when creating the Network Tunnel Group (IPsec tunnel). In the sample commands, `<sse_primary_dc_ip,sse_secondary_dc_ip>` refers to this IP address. We recommend choosing the IP address based on the data center located closest to your device.
- Open UDP ports 500 and 4500 before connecting to the tunnel.

NEC IX router devices do not require public static IPv4 address(es) configured on the interface that will connect to the public internet and Cisco Secure Access Network Tunnel Group. They can be behind a NAT device. This is because we can specify a text as its IKE ID. This ID in combination with the PSK is used to successfully authenticate the NEC IX router devices with the Cisco Secure Access Network Tunnel Group. Refer to NEC IX router Configuration Guide (Example).

Procedure

1. Follow the steps mentioned in Add a Network Tunnel Group.
2. Configure the WAN and the LAN interface.

```
interface GigaEthernet0.0
  description WAN1
  ip address <WAN ip-address>
  ip tcp adjust-mss auto

interface GigaEthernet1.0
  description LAN1
  ip address <LAN ip-address>
```

3. Create an IKEv2 authentication.

```
ikev2 authentication psk id rfc822-addr <sse-primary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)> key char <sse-tunnel-passphrase>
ikev2 authentication psk id rfc822-addr <sse-secondary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)> key char <sse-tunnel-passphrase>
```

4. Create an IKEv2 profile.

```
ikev2 profile SSE-primary
  child-lifetime 3600
```

```
  child-pfs off
  child-proposal enc aes-gcm-256-16
  child-proposal integrity sha1
  dpd interval 10
  local-authentication psk id rfc822-addr <sse-primary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)>
  sa-lifetime 14400
  sa-proposal enc aes-gcm-256-16
  sa-proposal dh 2048-bit

ikev2 profile SSE-secondary
  child-lifetime 3600
  child-pfs off
  child-proposal enc aes-gcm-256-16
  child-proposal integrity sha1
  dpd interval 10
  local-authentication psk id rfc822-addr <sse-secondary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)>
  sa-lifetime 14400
  sa-proposal enc aes-gcm-256-16
  sa-proposal dh 2048-bit
```

5. Create a tunnel interface.

```
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip address 169.254.0.4/31
  ip tcp adjust-mss 1280
  ikev2 connect-type auto
  ikev2 local-authentication id rfc822-addr <sse-primary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)>
  ikev2 nat-traversal keepalive 20
  ikev2 peer <sse_primary_dc_ip>

interface Tunnel1.0
  tunnel mode ipsec-ikev2
  ip address 169.254.0.8/31
  ip tcp adjust-mss 1280
  ikev2 connect-type auto
  ikev2 local-authentication id rfc822-addr <sse-secondary-tunnel-id (e.g.
xxxx@xxxx-xxxx-sse.cisco.com)>
  ikev2 nat-traversal keepalive 20
  ikev2 peer <sse_secondary_dc_ip>
```

6. Create a BGP routing.

```
router bgp <local AS number>
  neighbor 169.254.0.5 remote-as 32644
  neighbor 169.254.0.5 update-source Tunnel0.0
  neighbor 169.254.0.9 remote-as 32644
  neighbor 169.254.0.9 update-source Tunnel1.0
  address-family ipv4 unicast
    network <advertised route>
```

7. Create two static routes for the BGP peer addresses.

```
ip route 169.254.0.5/32(BGP peer address) Tunnel0.0
ip route 169.254.0.9/32(BGP peer address) Tunnel1.0
```

8. Apply the IKEv2 outgoing interface to the tunnel interfaces.

```
interface Tunnel0.0
  ikev2 outgoing-interface GigaEthernet0.0 <WAN next-hop-ip-address>
interface Tunnel1.0
  ikev2 outgoing-interface GigaEthernet0.0 <WAN next-hop-ip-address>
```

9. Permit for tunnel establishment between sse dc ip addresses.

```
ip access-list sse-ipsec permit ip src <sse_primary_dc_ip> dest any
ip access-list sse-ipsec permit ip src <sse_secondary_dc_ip> dest any
ip route <sse_primary_dc_ip> <WAN next-hop-ip-address>
ip route <sse_secondary_dc_ip> <WAN next-hop-ip-address>
interface GigaEthernet0.0
  ip filter sse-ipsec 1 in
```

10. After completing the NEC IX router deployment and updating the route table, the deployment is ready for testing. Use the following commands on the NEC IX router to verify the tunnel connectivity status and traffic processing:

```
show ikev2 sa
show ikev2 child-sa
show logging (logging subsystem ikev2)
show ip bgp
show ip route
```

Site-to-Site VPN tunnels with Microsoft Azure

Understand how to configure an Azure site-to-site VPN tunnel between an Azure Private Network and Secure Access.

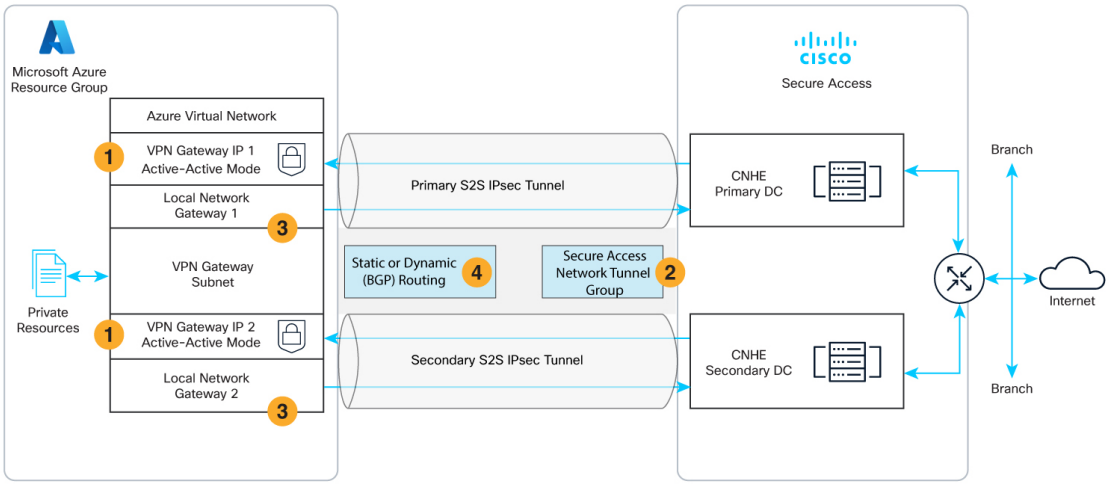
Overview of Azure Site to Site VPN

An Azure site-to-site (S2S) VPN tunnel between an Azure Virtual Network and Secure Access supports the following:

- Tunnel redundancy with high availability for branch site connections to Secure Access and your Azure virtual network. For more information, refer to Tunnel throughput, capacity, and scaling and Failover for Branch Connections in Secure Access Data Centers.
- Connection over IPsec (Internet Protocol Security) with authentication negotiated and traffic encrypted by IKEv2 (Internet Key Exchange, version 2). For more information, refer to Supported IPsec Parameters.
- Static or dynamic (BGP) routing. For more information, refer to Routing Options and Guidelines.

Microsoft Azure supports several methods of connecting to its VPN Gateway. The S2S VPN topology depends on components configured in the following order. Components in the diagram are numbered by order of configuration.

1. An Azure virtual network with a VPN gateway in active-active mode for tunnel redundancy. In active-active mode, Azure provides two VPN gateway IPs that Secure Access can use to establish a network tunnel group. Traffic will use the primary tunnel. In the event of a tunnel failover, the switch to the secondary tunnel will be automatic, immediate, and without interruption.
2. A Secure Access network tunnel group with two IPsec/IKEv2 tunnels and a pre-shared key (PSK) for connection with the Secure Access cloud native head end (CNHE) service.
3. Two local network gateways in Azure that establish S2S connections between the Azure VPN Gateway client and the Secure Access DC.



4. Branch and internet routing.
   - The static routing use case requires an Azure VPN Gateway route table.
   - The dynamic routing use case requires an Azure VPN Gateway autonomous system number (ASN) and Azure local network gateway BGP peer IP addresses.

For more information about VPN and tunnels in Secure Access, refer to Manage Virtual Private Networks and Manage Machine Tunnels.

Note

By default, the Perfect Forward Secrecy (PFS) setting is disabled in the Azure VPN portal; because the PFS is disabled, the Azure gateway client does not process the full proposal list as required by RFC 7296 when Secure Access is the platform to initiate the Child SA rekey. As a result the entire exchange is rejected and the CHILD SA rekey experiences a retry loop for a significant amount of time while the tunnel data plane is still active.

To safely incorporate the CHILD SA rekey we recommend following **one** of the following alternative configurations:

- **Shorten the Azure CHILD SA lifetime**. In the Azure dashboard navigate to **VPN Gateway** > **Connections** and select your connection, then select **IPsec / IKE policy**. Locate the **Default** setting to **Custom** and then change the **IPsec SA lifetime in seconds** value to **<3000**.
- **Configure an alternate PFS setting.** In the Azure dashboard navigate to **VPN Gateway** > **Connections** and select your connection, then select **IPsec / IKE policy**. Locate the **Default** setting to **Custom** and then change the **PFS** value. For example, set the new PFS value to a DH group.

More Information

For more information about Azure, refer to Microsoft documentation:

- What is Azure VPN Gateway?
- Azure VPN Gateway topology and design: Site-to-site VPN
- Design highly available gateway connectivity for cross-premises and VNet-to-VNet connections: Active-active VPN gateways
- Tutorial: Create a site-to-site VPN connection in the Azure portal

- Azure: Create, change, or delete a route table
- Azure: BGP and routing

> **Note**
>
> Microsoft may update their documentation without notice.

Configure Azure S2S Tunnels with Static Routing

Provides instructions for completing the Configure Azure S2S Tunnels with Static Routing workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Follow these steps to deploy a site-to-site (S2S) VPN tunnel from Azure Virtual Network connects to Cisco Secure Access using an Azure route table for static routing to branch and internet destinations.

Use static routing for small, simple networks where predictable routes are needed and manual configuration is manageable. For more information, see Static Routing.

Before you begin

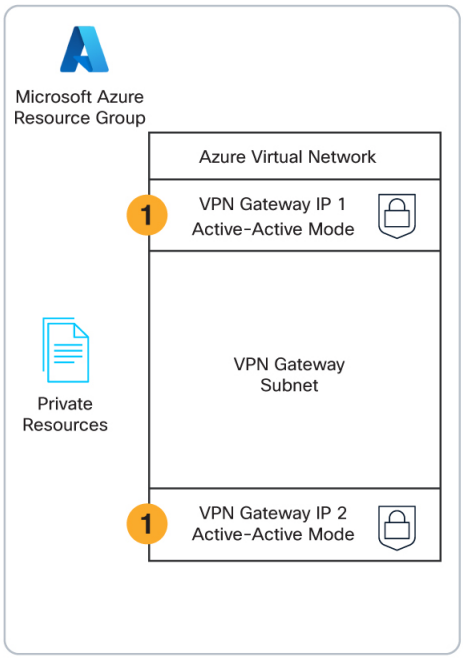
Prerequisites include the following.

- A valid Cisco Secure Access account.
- An Azure account with an active subscription.

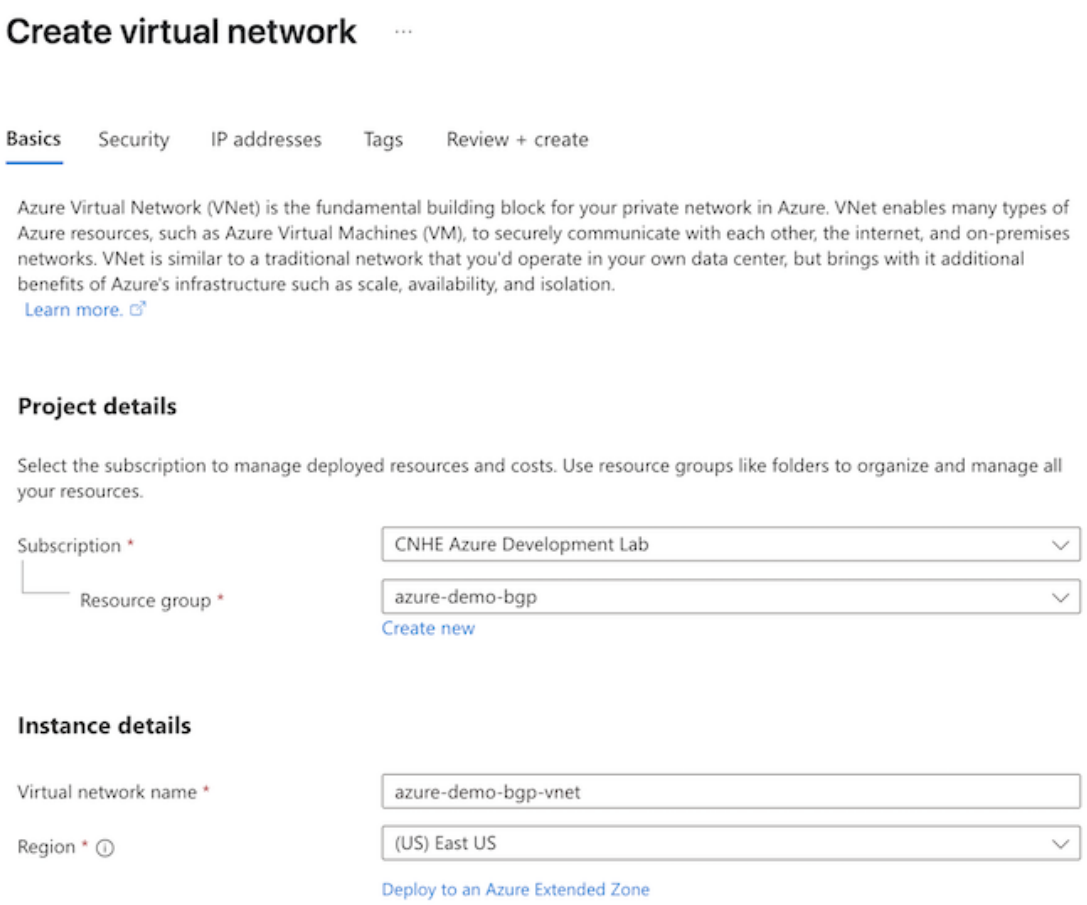
Procedure

Component 1: Create a VPN Gateway in Microsoft Azure

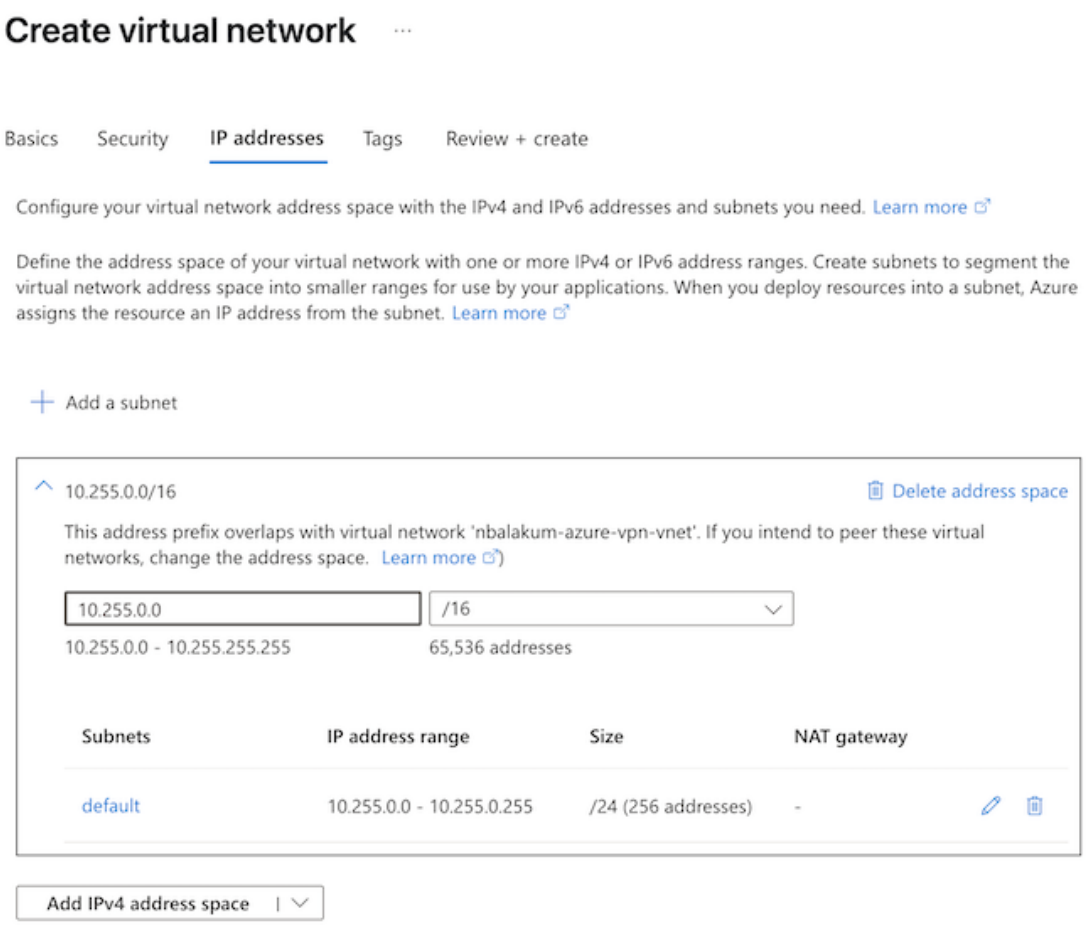
> **Note**
>
> The Azure S2S IPsec tunnel is sourced from the VPN Gateway. If you have already deployed a VPN Gateway in your Azure environment, skip ahead to Component 2.



1. In the Azure admin portal, navigate to your resource group and click **Create**.
2. Search the marketplace for **Virtual network**, then click **Create**.
3. Configure the virtual network.
   a) **Basics**: Select the **Subscription** and **Resource group** with the resources that you want to make available via the S2S VPN tunnel.

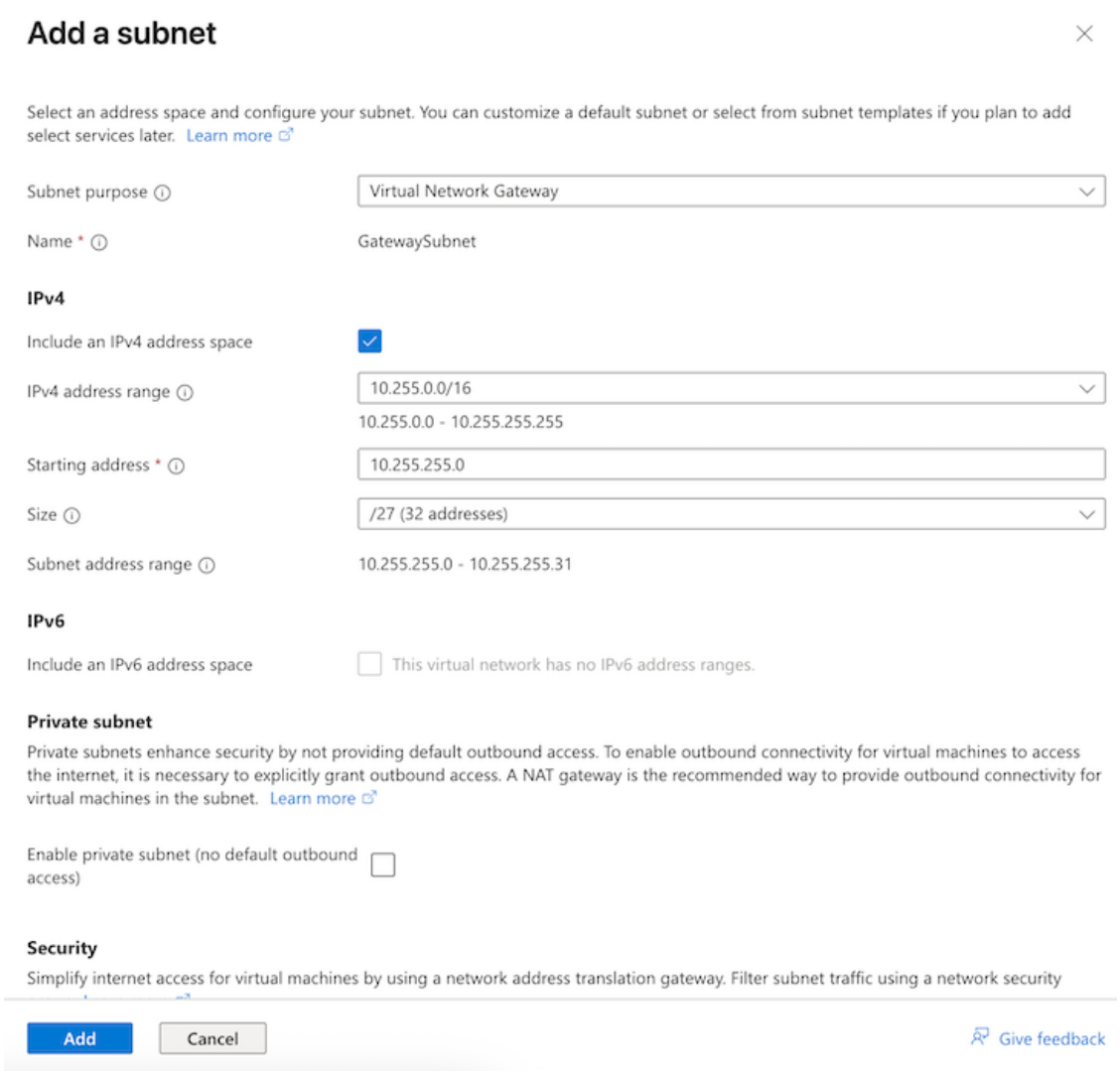


b) **IP addresses**: Configure a virtual network address with the IPv4 addresses and subnets you need. This example uses the range 10.255.0.0/16.



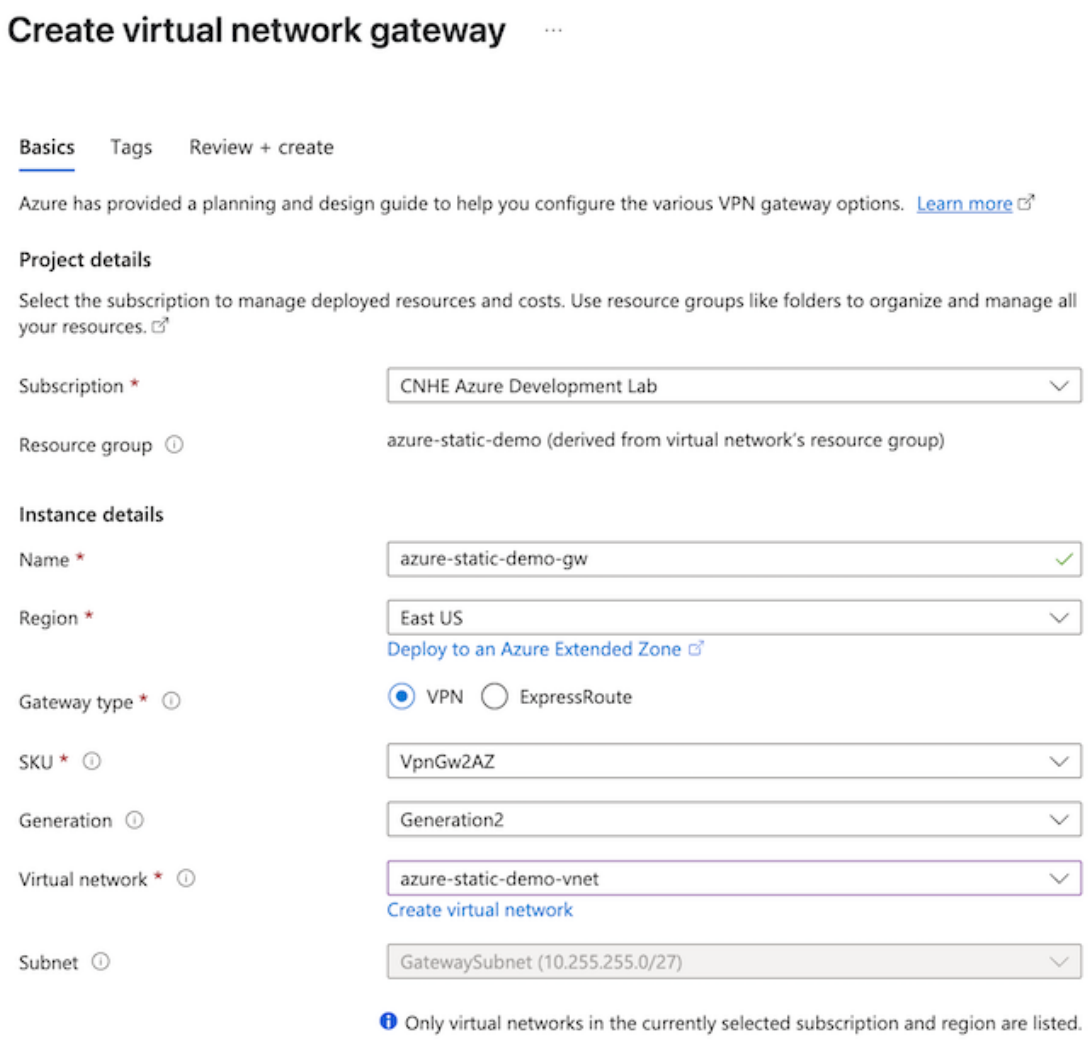
c) Review the configuration and click **Create**.
Azure will deploy the virtual network and update the dashboard when deployment is complete.

4. Create the gateway subnet.



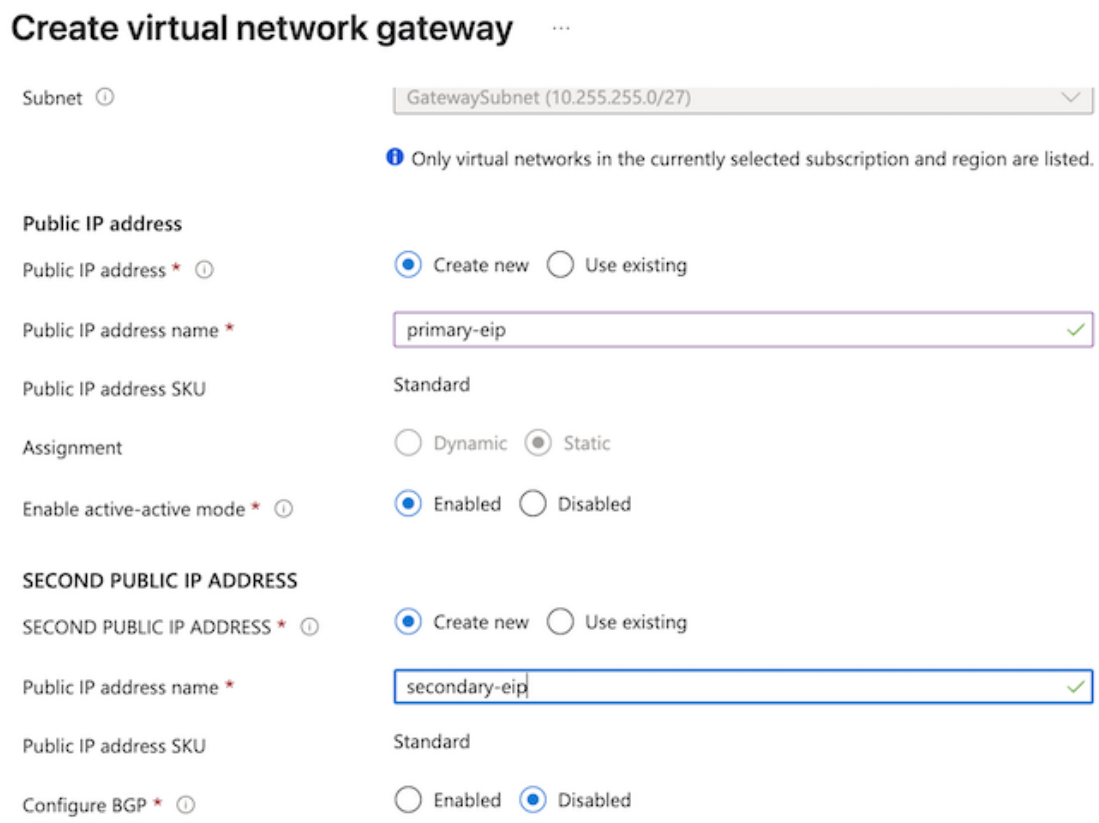
a) Navigate to **Go to resource** > **Settings** > **Subnets**.
b) Click **+ Subnet**.
c) **Subnet purpose**: Choose Virtual Network Gateway.
d) Enable **Include an IPv4 address space** (it is enabled by default).
e) **IPv4 address range** will default to the address space you configured when you created the virtual network. This example uses the range `10.255.0.0/16`.
f) **Starting address**: This example uses `10.255.255.0`.
g) **Size**: This example uses `/27` (32 addresses)
h) Click **Add**.

5. Create the virtual network gateway.
   a) Navigate to **Overview** > **Resource group (click the name of your resource group)** > **+ Create**.
   b) Search the marketplace for **Virtual network gateway**, then click **Create**.
6. Configure the virtual network gateway.

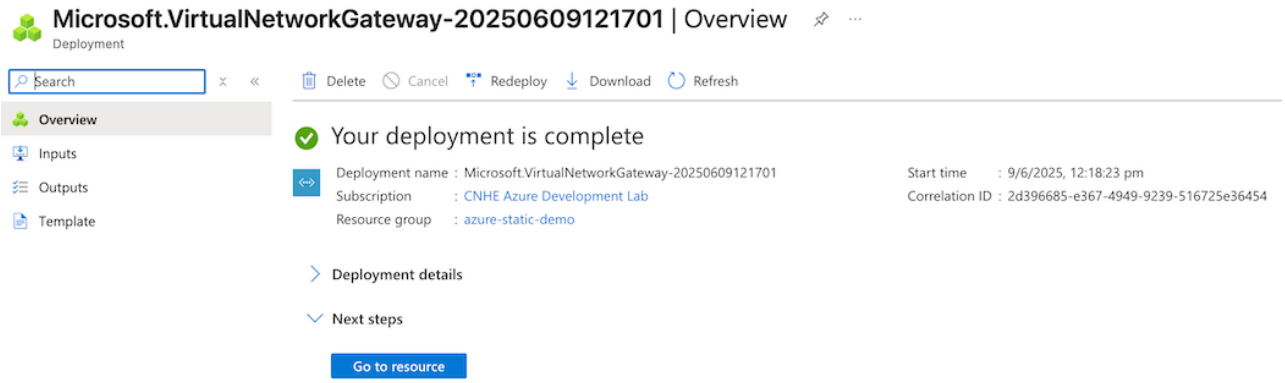


a) **SKU**: Choose **VpnGw2AZ**. For more information, see About gateway SKUs.
b) **Generation**: Choose **Generation2**.
c) **Virtual network**: Select the virtual network you created in the previous step.
d) **Public IP address**: Chose **Create new**.
e) **Public IP address name**: Enter a descriptive name for the primary IP address.
f) **Enable active-active mode**: Choose **Enabled**.
g) **SECOND PUBLIC IP ADDRESS**: Choose **Create new**.
h) **Public IP address name**: Enter a descriptive name for the primary IP address.
i) **Configure BGP**: Choose **Disabled**.

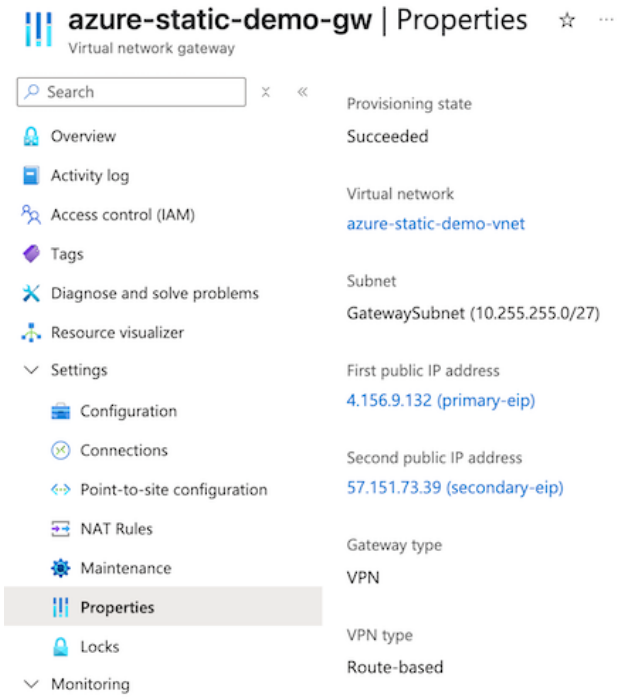
7. Review the configuration, then click **Create**.



Azure will deploy the virtual network gateway and update the dashboard with the two public IP address resources when deployment is complete.

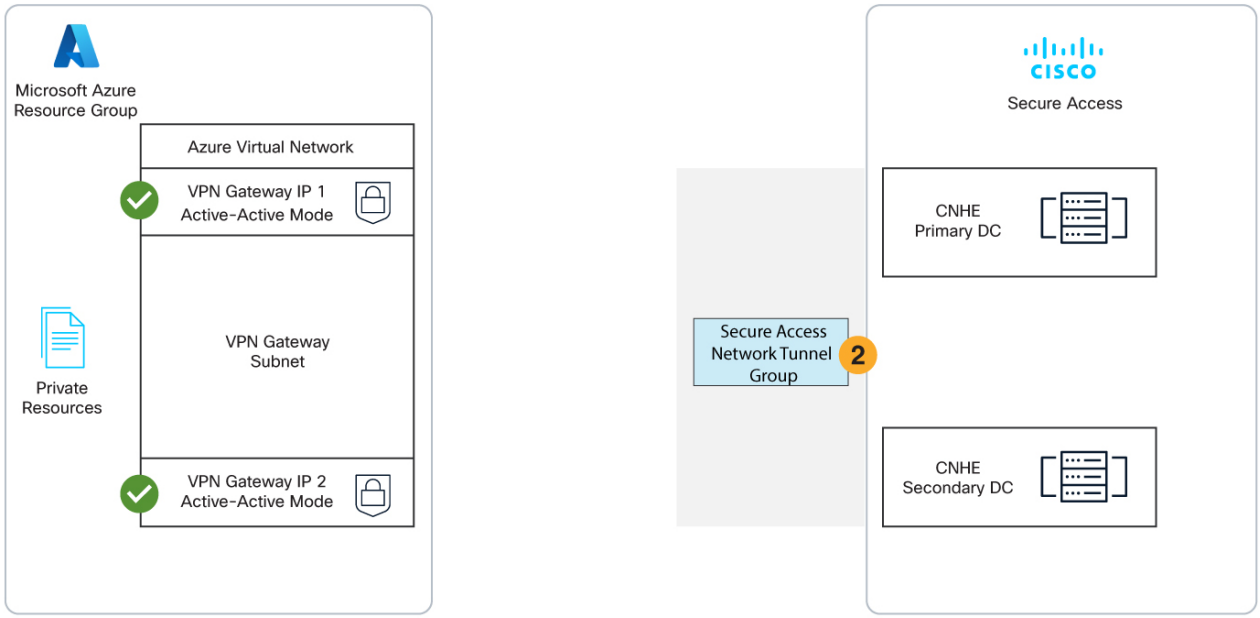


> **Note**
>
> To review your configuration after deployment is complete, navigate to **Settings** > **Properties**.



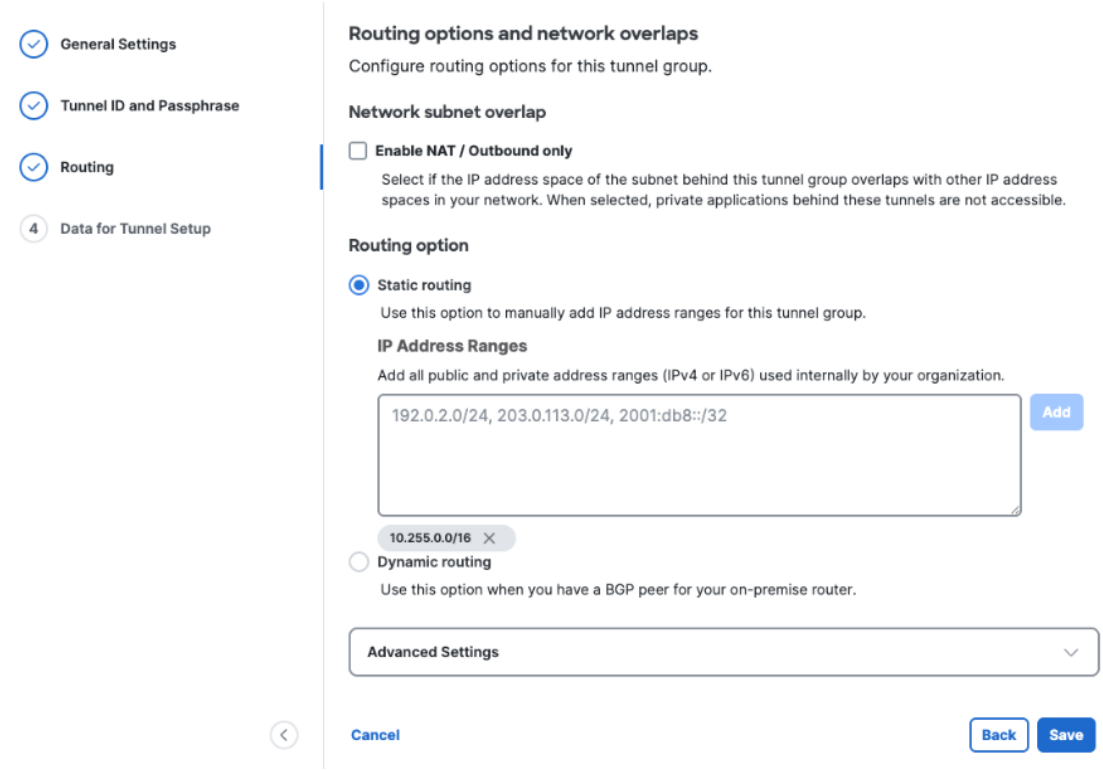
Component 2: Create a network tunnel group in Secure Access

Create a network tunnel group in Secure Access with the following configuration. For a more detailed procedure, see Add a Network Tunnel Group.

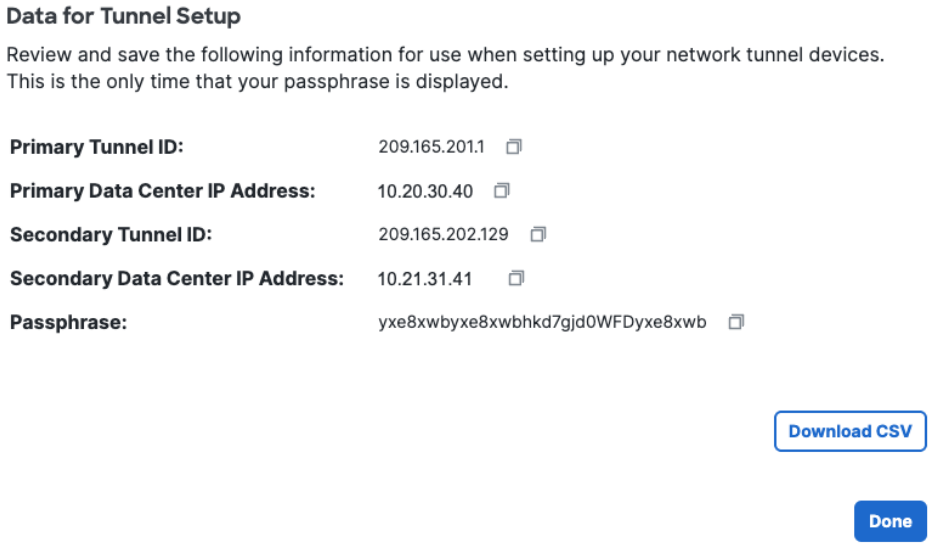


8. **Step 1 - General Settings**: Set **Device Type** to AZURE.

9. **Step 2 - Tunnel ID and Passphrase**: Enter the primary and secondary public IPs from the Azure virtual network gateway and create a passphrase.
10. **Step 3 - Routing**: Select **Routing option** > **Static routing**, then add all public and private IPv4 address ranges used internally for your Azure virtual network. This example uses the range 10.255.0.0/16.



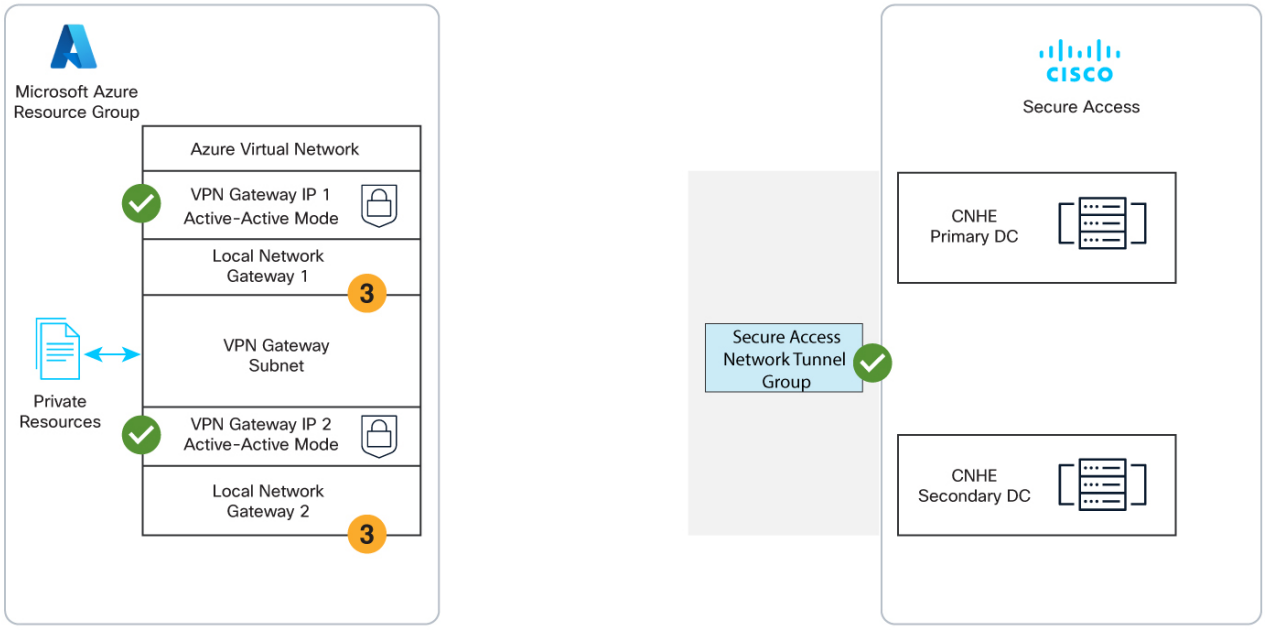
11. **Step 4 - Data for Tunnel Setup**: Copy or download the primary and secondary tunnel IDs, data center (DC) IP addresses, and the passphrase you created.



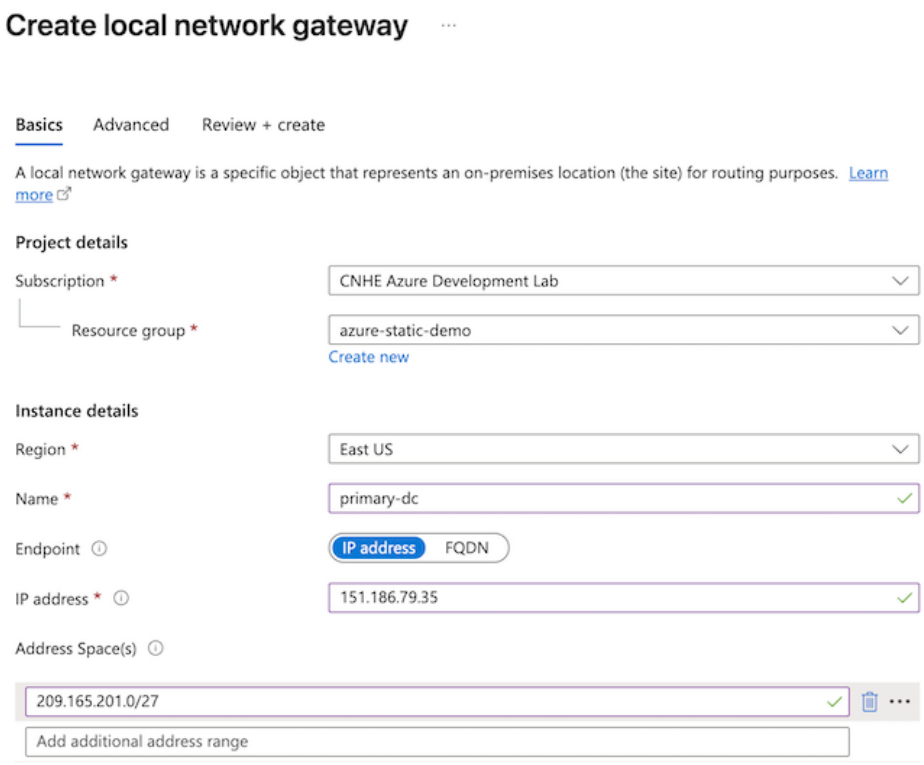
> **Note**
>
> This is the only time your passphrase will be displayed.

Component 3: Create two local network gateways in Azure with S2S connections

Create and configure two local network gateways in Azure, then connect them to Secure Access. The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.



12. In the Azure admin portal, navigate to **Overview** > **Resource group** > **Click the name of your resource group** > **+ Create**.
13. Search the marketplace for **Local network gateway**, then click **Create**.
14. Configure the **Basics tab** of the first local network gateway.



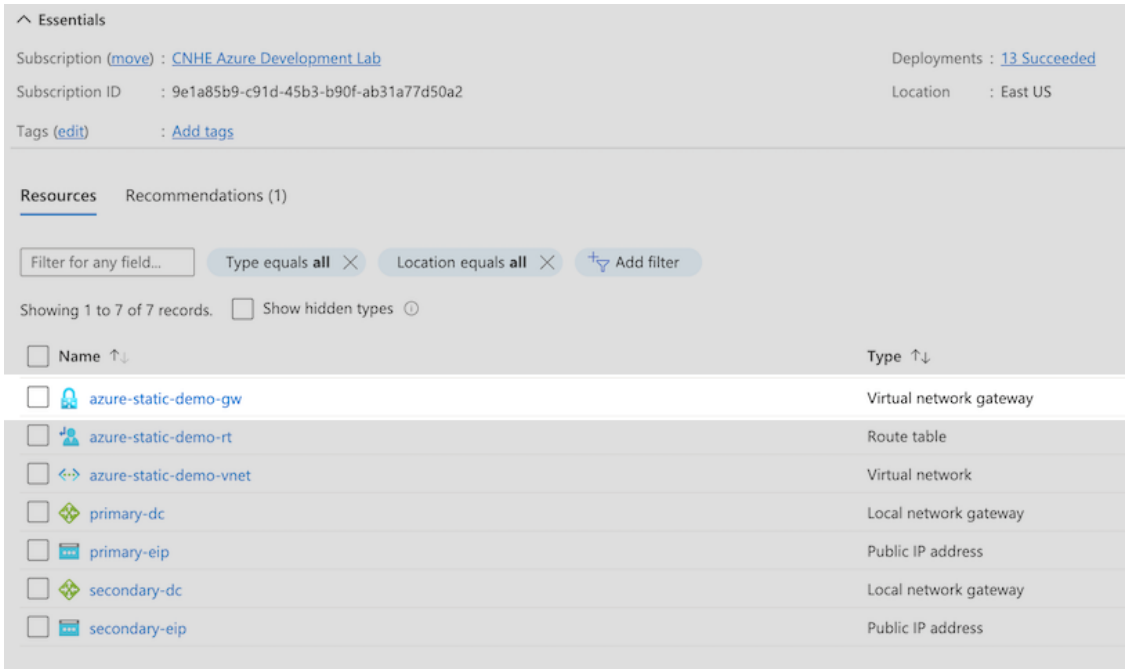
a) Select the **Subscription** and **Resource group** of your virtual network.
b) **Name**: This example uses primary-dc.
c) **Endpoint**: Select **IP address**
d) **IP address**: For the first local network gateway, enter the **Primary DC IP Address** from **Secure Access Step 4 - Data for Tunnel Setup**.
e) **Address Space(s)**: Add one or more IP ranges for branch sites that will connect to the Secure Access network tunnel group. Address spaces should not overlap with other IP ranges in your network. This example uses `209.165.201.0/27`.

Restriction

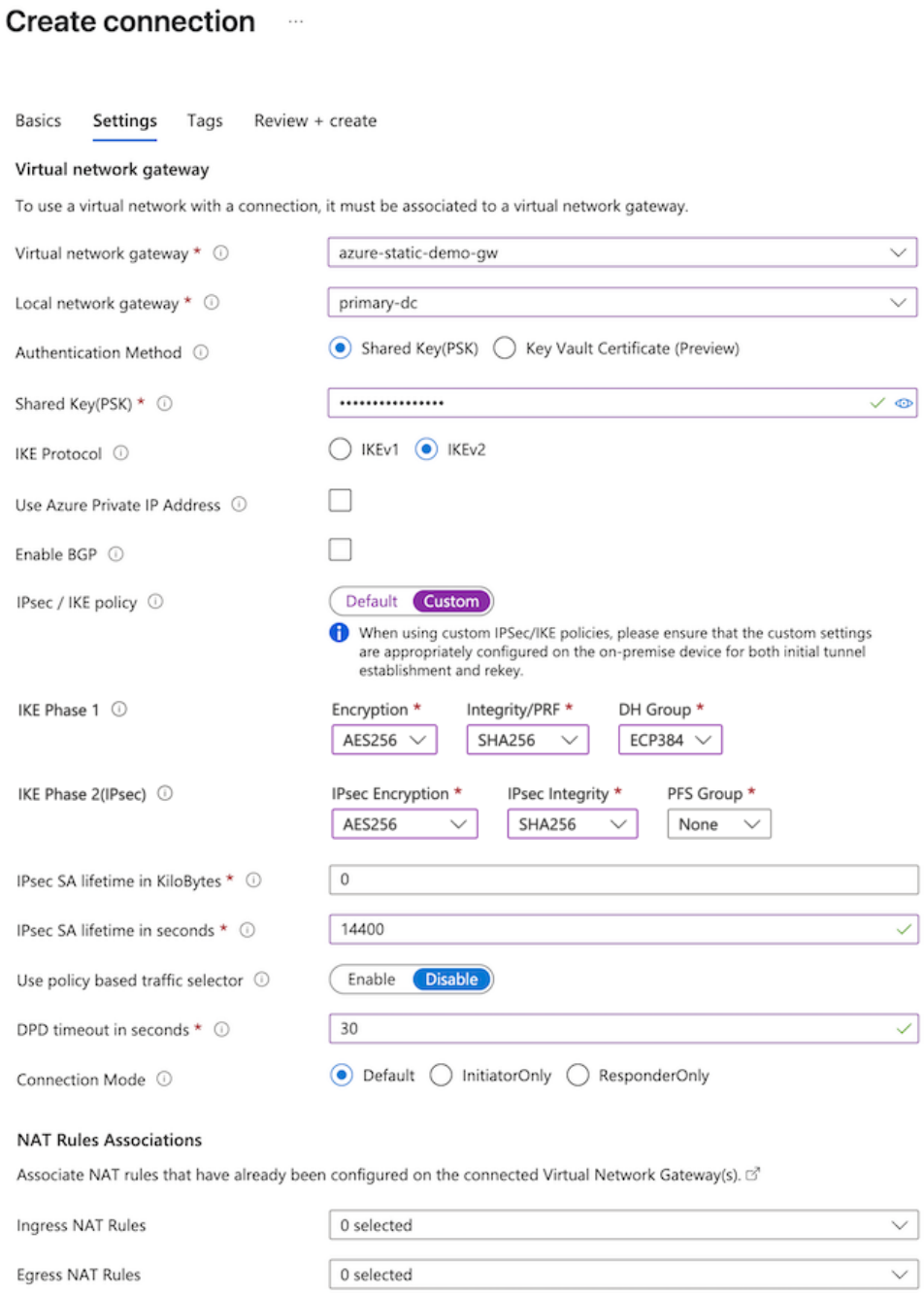
Azure does not support adding the address range `0.0.0.0/0` in the Address Space configuration for local network gateways. To work around this limitation, split the range into two separate entries:

- `0.0.0.0/1`
- `128.0.0.0/1`

15. Review the configuration, then click **Create**.
Azure will deploy the local network gateway and update the dashboard with the local network gateway resource when deployment is complete.
16. Repeat the previous step to create the secondary local network gateway with the **Secondary DC IP Address** from Secure Access.



17. Create the S2S connection for the primary local network gateway.



a) In the Azure admin portal, navigate to **Overview** > **Resource group** > **Click the name of your resource group** > **Resources**, then click the name of your virtual network gateway.
b) Navigate to **Connections**, then click **+ Add**.
c) In the **Basics tab**, select the **Subscription** and **Resource group** of your virtual network.
d) **Connection type**: **Select Site-to-site (IPsec)**.
e) In the **Settings tab** of the connection, select your virtual network gateway.
f) **Local network gateway**: Select the primary gateway.
g) **Shared Key (PSK)**: Enter the passphrase configured for the Secure Access network tunnel group.
h) **IPsec / IKE policy**: Select **Custom**.
i) Select parameters for **IKE Phase 1**.

- **Encryption** – Select **AES256** (recommended).

- **Integrity/PRF** – Select **SHA256** (recommended).
- **DH Group** – Select **ECP384** (recommended).

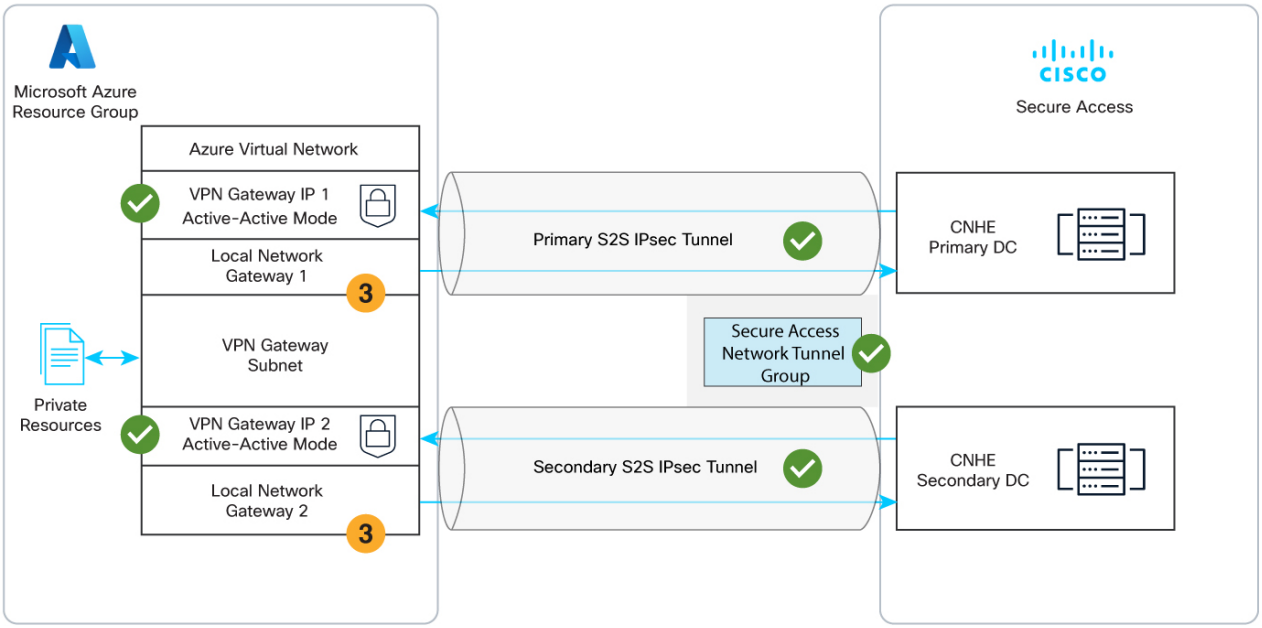
j) Select parameters for **IKE Phase 2 (IPsec)**.

- **IPsec Encryption** – Select **AES256** (recommended).
- **IPsec Integrity** – Select **SHA256** (recommended).
- **PFS Group** – **None** is the default setting in Secure Access, but disabling this option fails to process the full proposal list and cuses the SHILD SA rekey experience to loop whie the data plane is still active. We recommend one of the following actions in the Azure dashboard instead:
  - **Shorten the Azure CHILD SA lifetime**. Navigate to **VPN Gateway** > **Connections** and select your connection, then select **IPsec / IKE policy**. Locate the **Default** setting to **Custom** and then change the **IPsec SA lifetime in seconds** value to **<3000**.
  - **Configure an alternate PFS setting**. Navigate to **VPN Gateway** > **Connections** and select your connection, then select **IPsec / IKE policy**. Locate the Default setting to **Custom** and then change the **PFS** value. For example, set the new FPS value to a DH group.

> **Note**
>
> For information about cipher parameters supported by Secure Access, see Supported IPsec Parameters. For information about cipher parameters supported by Azure, see Microsoft documentation on Default IPsec/IKE parameters.

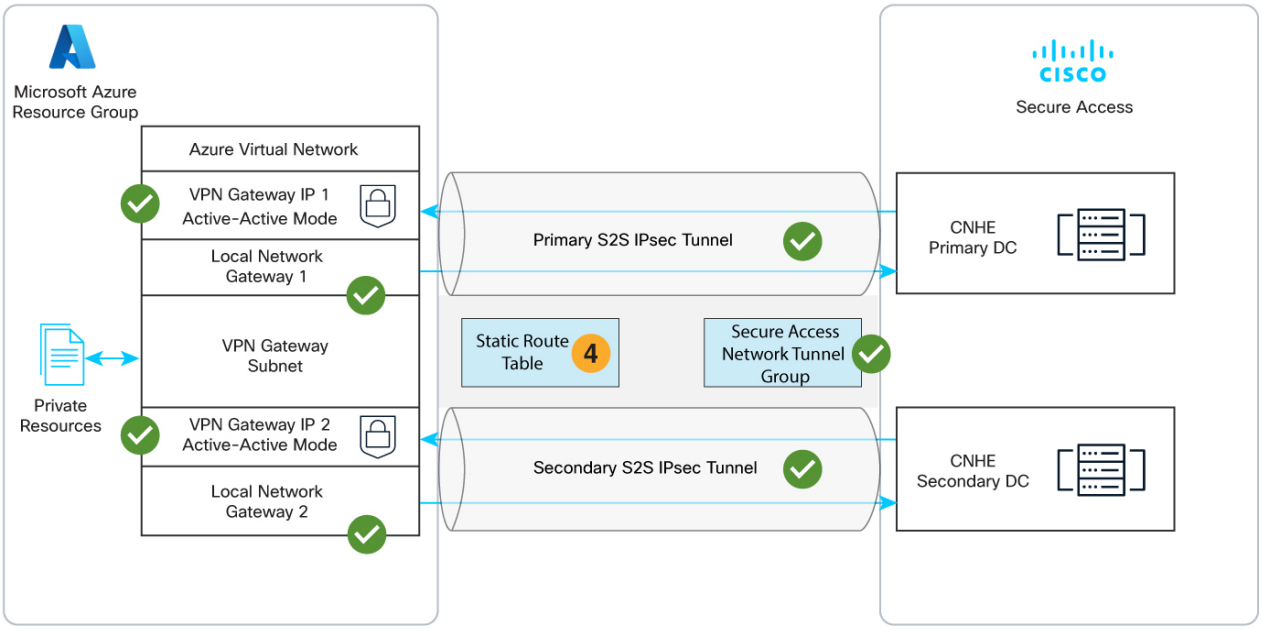
k) **IPsec SA lifetime in seconds:** Set to 14400.
l) **DPD timeout in seconds:** Set to 30.
m) Review the configuration, then click **Create**.
Azure will deploy the S2S connection and update the dashboard when deployment is complete.

18. Repeat the previous step for the secondary local network gateway.
19. Both S2S VPN tunnels are now established with static routing between your Azure virtual network gateway and the Secure Access DC.



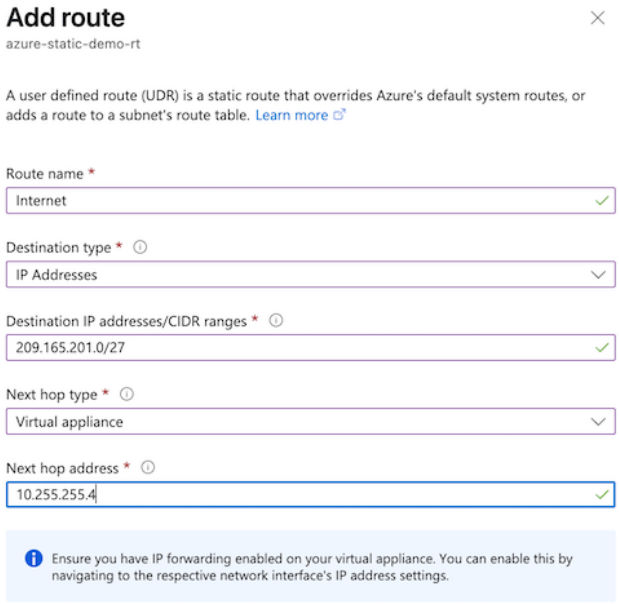
Component 4: Create a static route table in Azure

Add a table of branch routes and internet routes to the primary VPN gateway and associate the route table with any required subnets. For more information, see Azure: Create, change, or delete a route table.



20. In the Azure admin portal, navigate to **Overview** > **Resource group (click the name of your resource group)** > **+ Create**.
21. Search the marketplace for **Route table**, then click **Create**.
22. Navigate to the **Basics tab** of the route table, then select the **Subscription** and **Resource group** of your virtual network.
23. Review the configuration, then click **Create**.
    Azure will deploy the route table and update the dashboard when deployment is complete.
24. Navigate to **Overview** > **Resource group (click the name of your resource group)** > **Resources**, then click the name of your route table.

25. Click **+ Add**.
26. Configure a route.

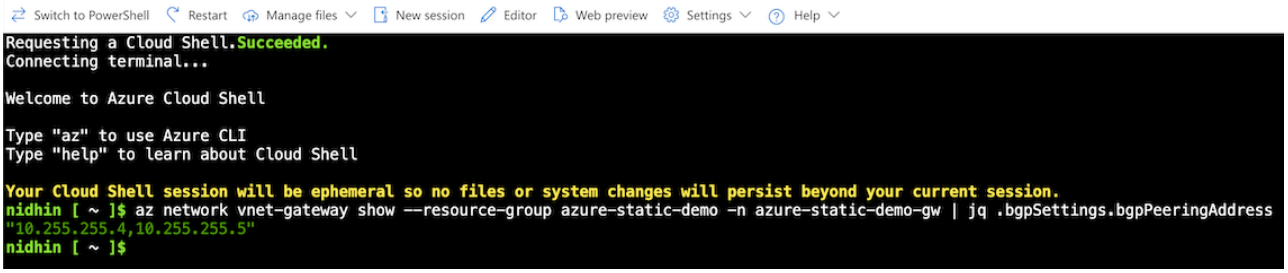


Remember

Along with your user-defined routes, add two routes to the Azure route table for the internet prefixes `0.0.0.0/1` and `128.0.0.0/1`.

a) **Route name**: This example uses Internet.
b) **Destination type**: Select IP Addresses.
c) **Destination IP addresses/CIDR ranges**: Enter the IP ranges for branch sites configured as address spaces for Azure local network gateways. This example uses `209.165.201.0/27`.
d) **Next hop type**: Select Virtual appliance.
e) **Next hop address**: Enter the first IP address returned by the Azure CloudShell command shown below. In this example, the next hop address is `10.255.255.4`.

```
az network vnet-gateway show --resource-group \<Resource Group Name> -n
\<VNET Gateway Name> | jq .bgpSettings.bgpPeeringAddress
```



> **Note**
>
> The CloudShell command returns the BGP peering addresses for the primary and secondary local network gateways.
>
> By creating a static route to the primary local network gateway connection, Azure will route all traffic to the primary DC via the primary S2S tunnel when both tunnels are up. When the primary tunnel is down, Azure will route all traffic to the secondary DC via the secondary S2S tunnel.

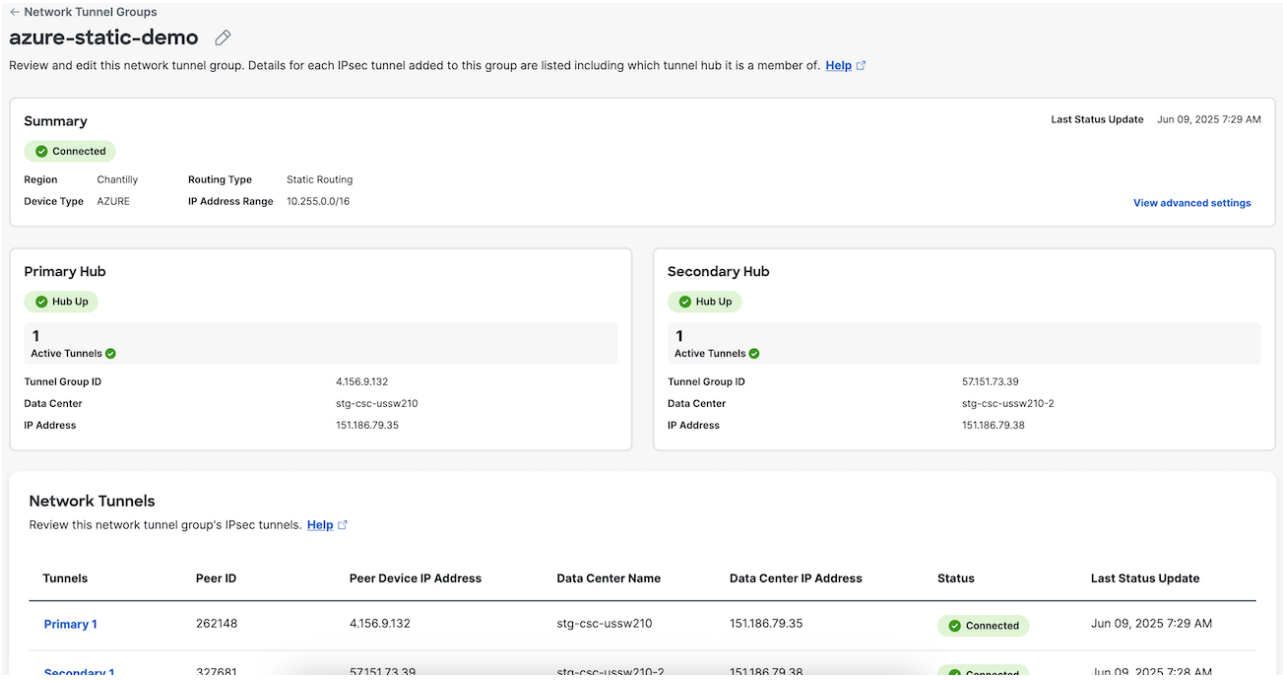
27. Associate a subnet.

a) Navigate to **Settings** > **Subnets**.
b) Select the virtual network.
c) **Subnet**: Select default.
d) Click **OK**.

What to do next

Verify tunnel status in Secure Access

In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click the name of the network tunnel group to review the connection status with Azure.



Resources in your Azure virtual network are now protected by the site-to-site (S2S) IPsec/IKEv2 VPN tunnel with Cisco Secure Access.

For information about managing and monitoring your network tunnel group, see Manage Network Tunnel Groups.

Configure Azure S2S Tunnels with Dynamic Routing with BGP

Provides instructions for completing the Configure Azure S2S Tunnels with Dynamic Routing with BGP workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Follow these steps to deploy a site-to-site (S2S) VPN tunnel from Azure Virtual Network connects to Cisco Secure Access using Azure BGP for dynamic routing to branch and internet destinations.

Use dynamic routing for large, complex networks with multiple connections where automatic route updates and optimal path selection are crucial, especially when dealing with internet connectivity or service provider traffic. For more information, see Dynamic Routing with BGP.

Before you begin

Prerequisites include the following.

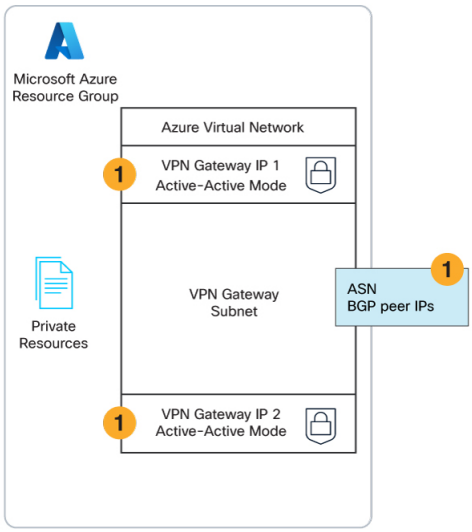
- A valid Cisco Secure Access account.
- An Azure account with an active subscription.

Procedure

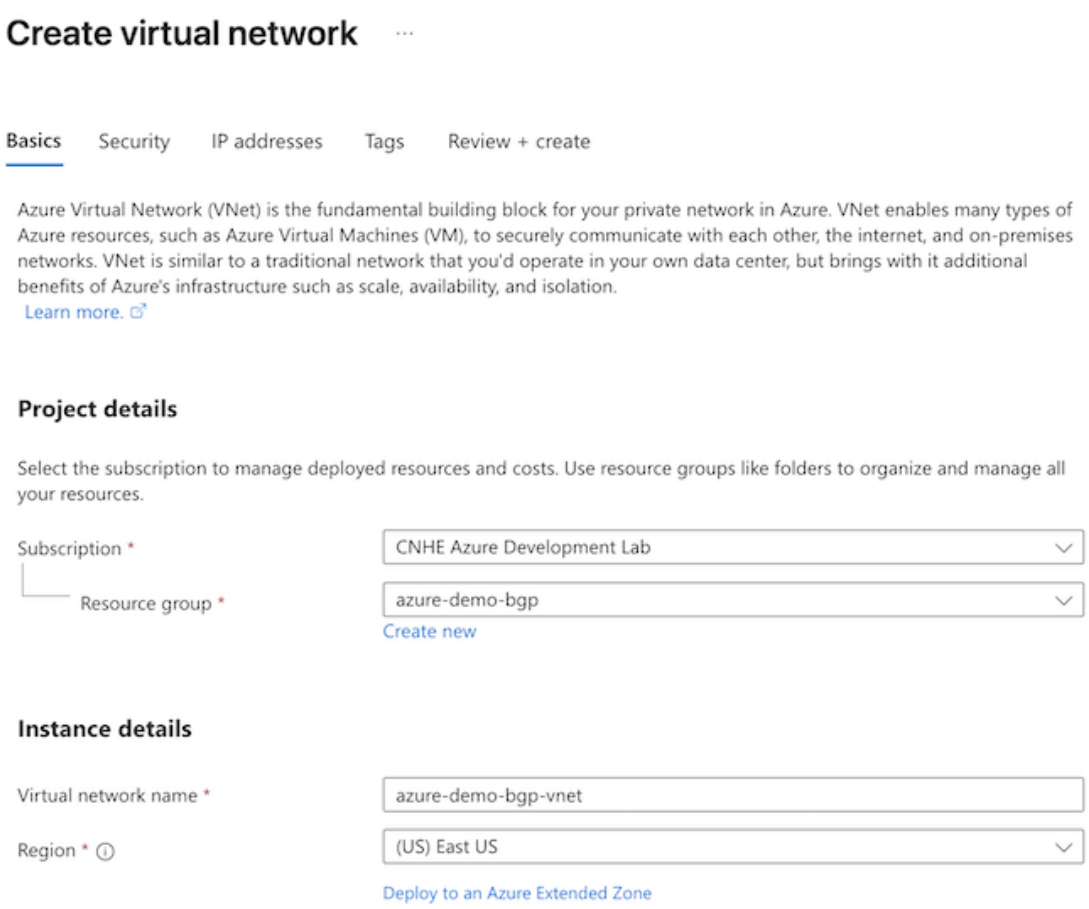
Component 1: Create a VPN Gateway in Microsoft Azure

Note

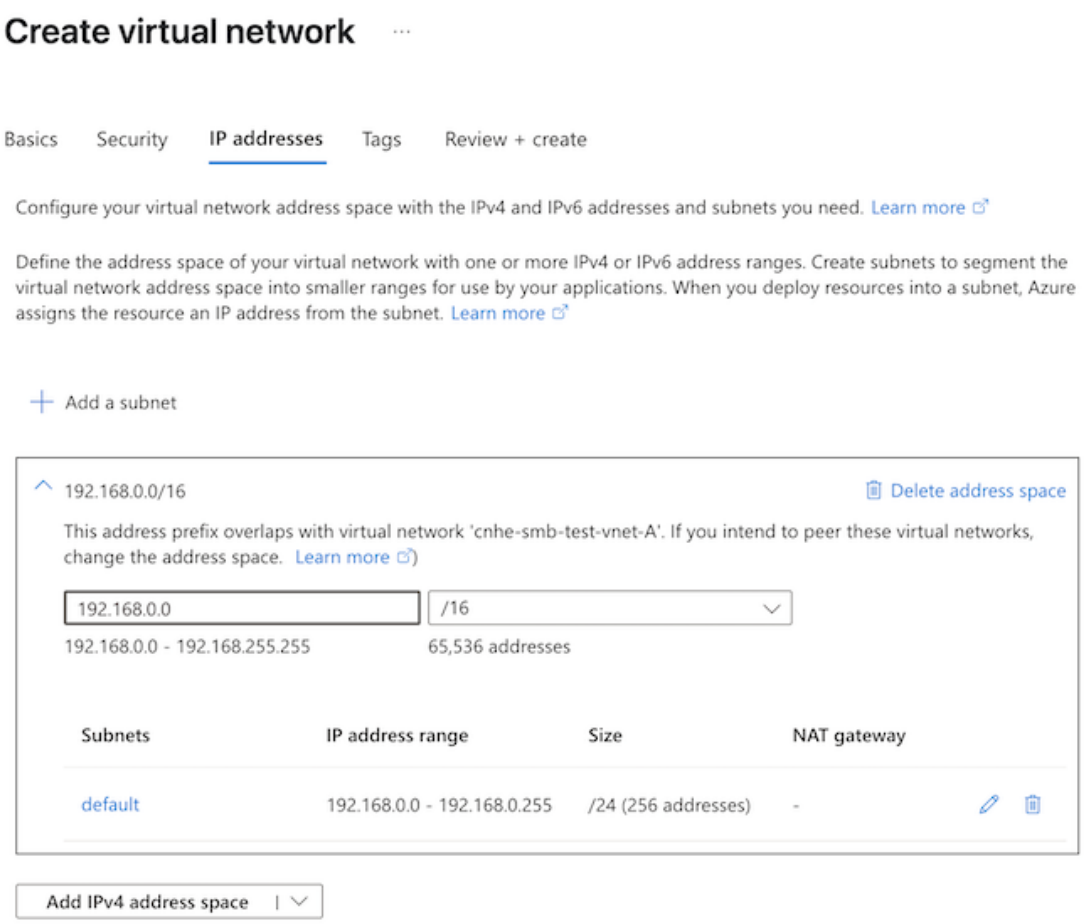
The Azure S2S IPsec tunnel is sourced from the VPN Gateway. If you have already deployed a VPN Gateway in your Azure environment, you can skip this section.



1. In the Azure admin portal, navigate to your resource group and click **Create**.
2. Search the marketplace for Virtual network, then click **Create**.
3. Configure the virtual network.
   a) **Basics**: Select the **Subscription** and **Resource group** with the resources that you want to make available via the S2S VPN tunnel.



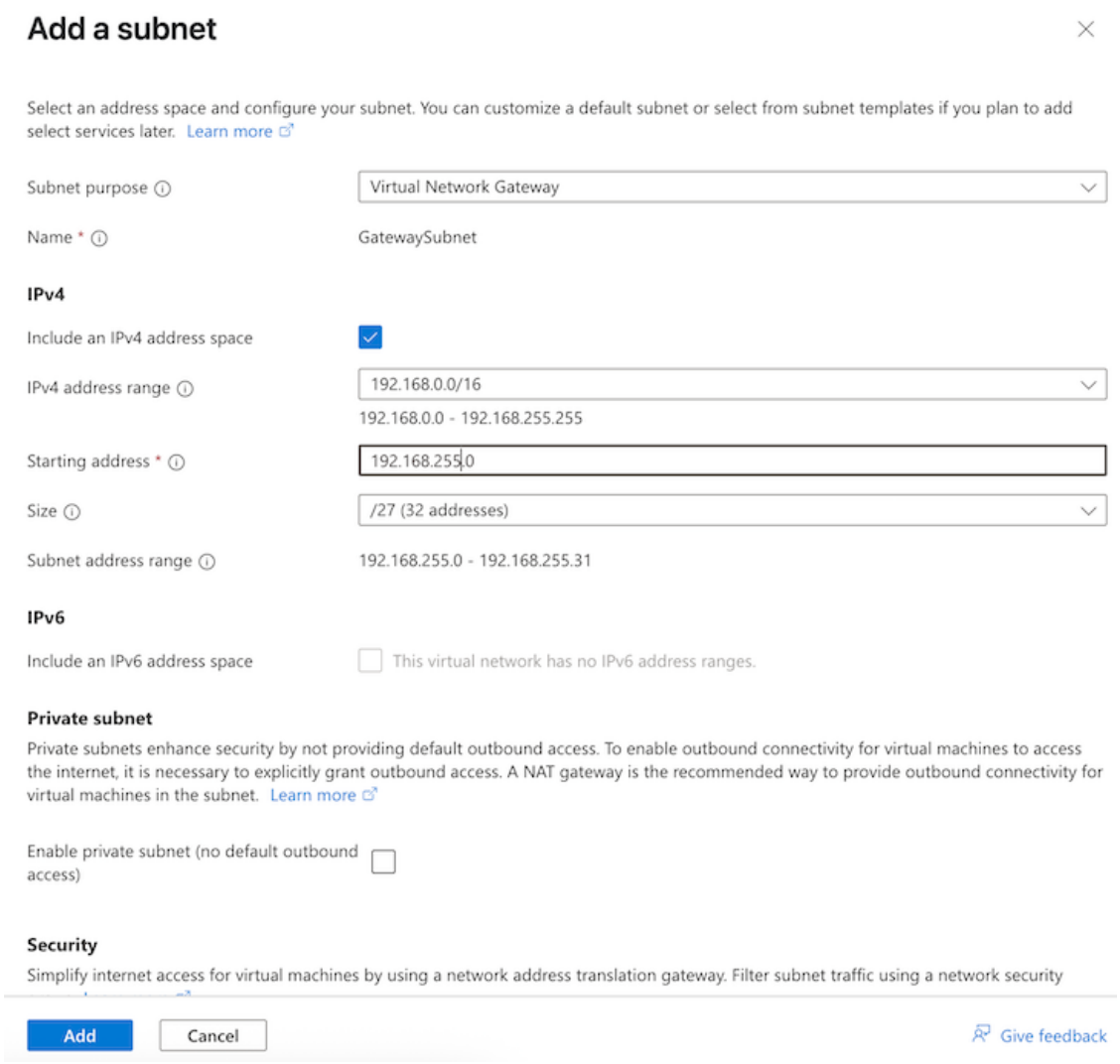
b) **IP addresses**: Configure a virtual network address with the IPv4 and IPv6 addresses and subnets you need. This example uses the range `192.168.0.0/16`.



c) Review the configuration and click **Create**.

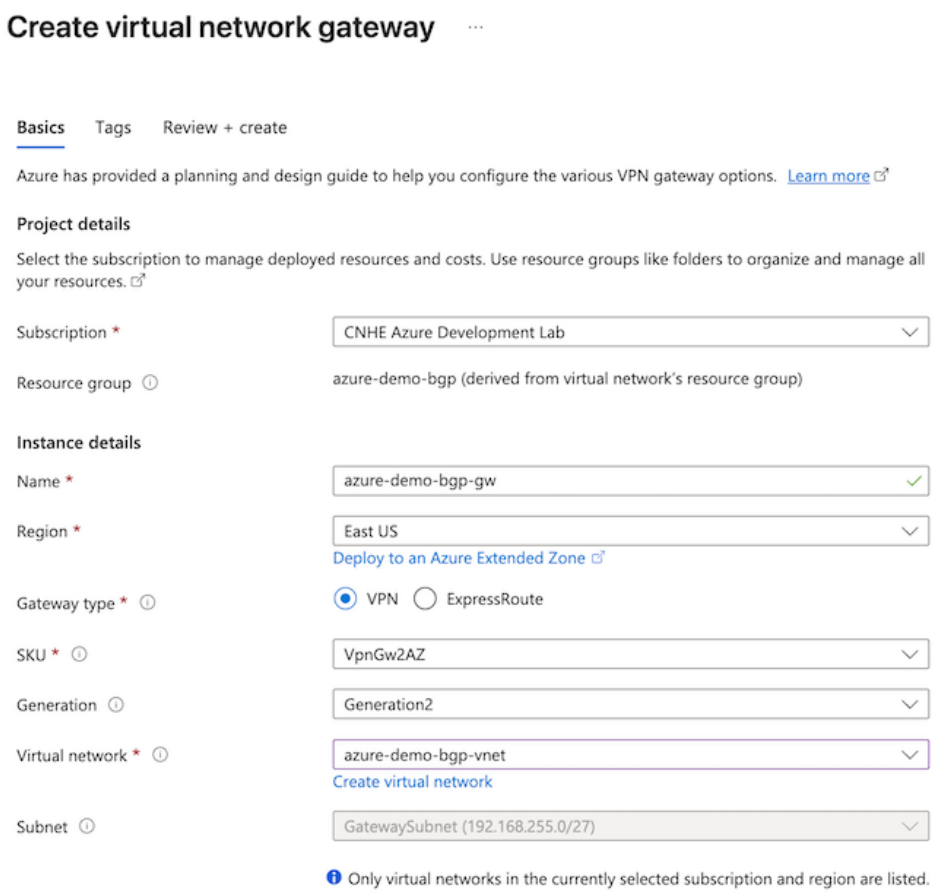
Azure will deploy the virtual network and update the dashboard when deployment is complete.

4. Create the gateway subnet.



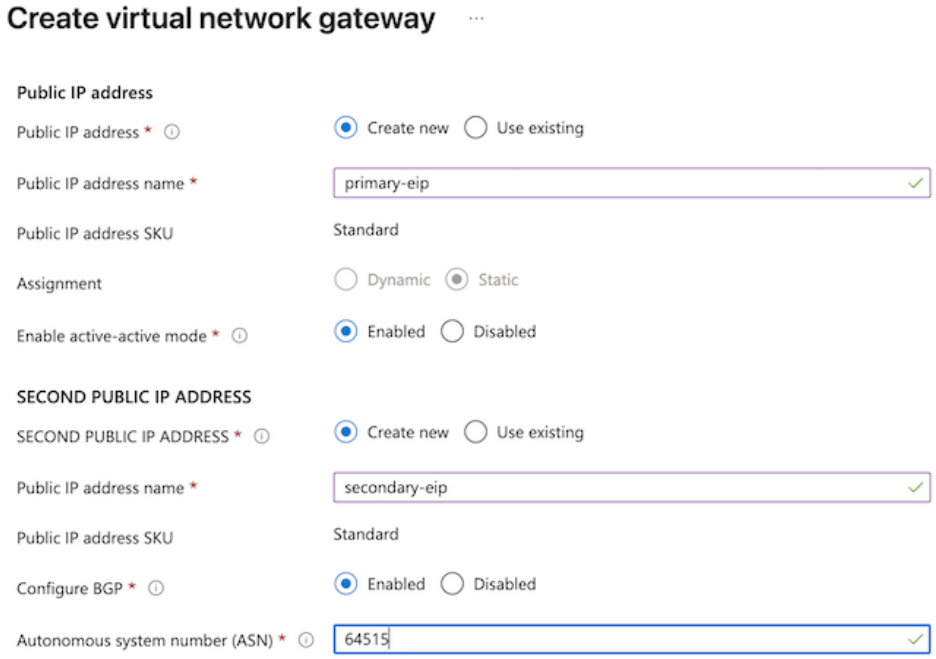
a) Navigate to **Go to resource** > **Settings** > **Subnets**.
b) Click **+ Subnet**.
c) **Subnet purpose**: Select **Virtual Network Gateway**.
d) Enable **Include an IPv4 address space** (it is enabled by default).
e) Confirm **IPv4 address range** defaulted to the address space you configured when you created the virtual network. This example uses the range `192.168.0.0/16`.
f) **Starting address**: This example uses `192.168.255.0`.
g) **Size**: This example uses **/27 (32 addresses)**
h) Click **Add**.

5. Create the virtual network gateway.



a) Navigate to **Overview** > **Resource group (click the name of your resource group)** > **+ Create**.
b) Search the marketplace for **Virtual network gateway**, then click **Create**.

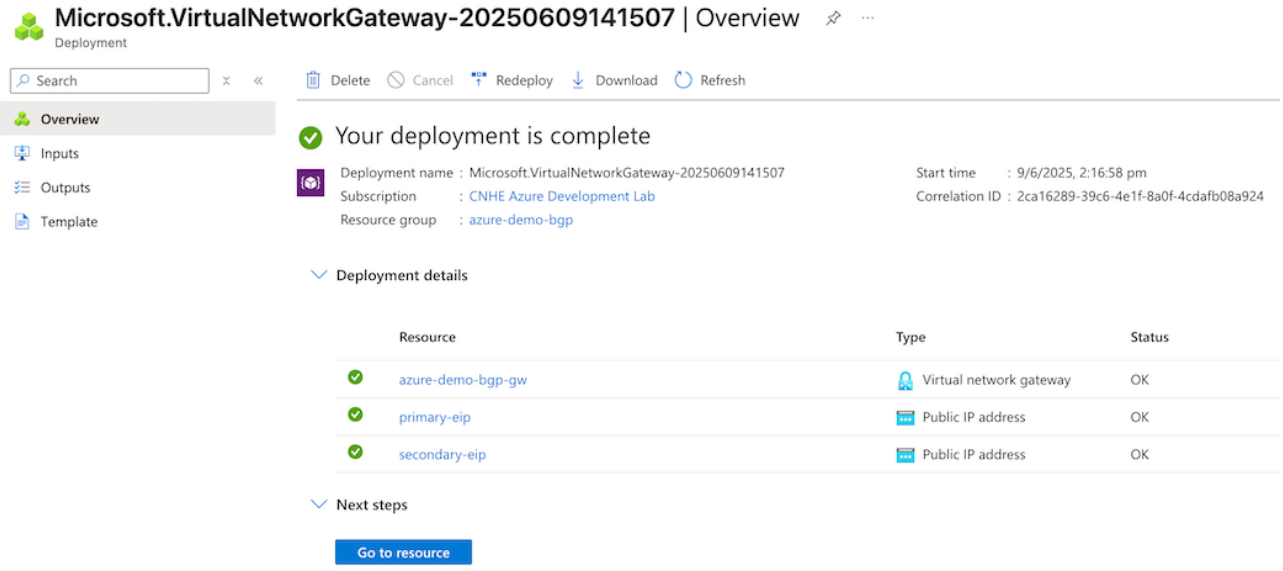
6. Configure the virtual network gateway.



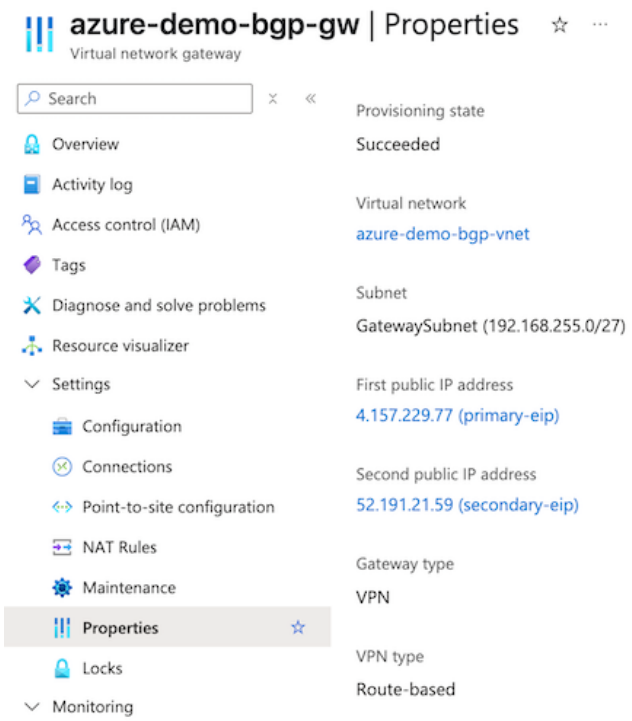
a) **SKU**: Select **VpnGw2AZ**. For more information, see About gateway SKUs.
b) **Generation**: Select **Generation2**.

c) **Virtual network**: Select the virtual network you created in the previous step.
d) **Public IP address**: Select **Create new**.
e) **Public IP address name**: Enter a descriptive name for the primary IP address.
f) Enable **Enable active-active mode**.
g) **SECOND PUBLIC IP ADDRESS**: Select **Create new**.
h) **Public IP address name**: Enter a descriptive name for the primary IP address.
i) Enable **Configure BGP**.
j) **Autonomous system number (ASN)**: Enter an ASN that is not in use by your other branches and that is not reserved by Azure or IANA. This example uses ASN 64515. For more information, see Microsoft Azure documentation on BGP and routing.
k) You do not need to enter custom Azure APIPA BGP IP addresses.

7. Review the configuration, then click **Create**.
Azure will deploy the virtual network gateway and update the dashboard with the two public IP address resources when deployment is complete.

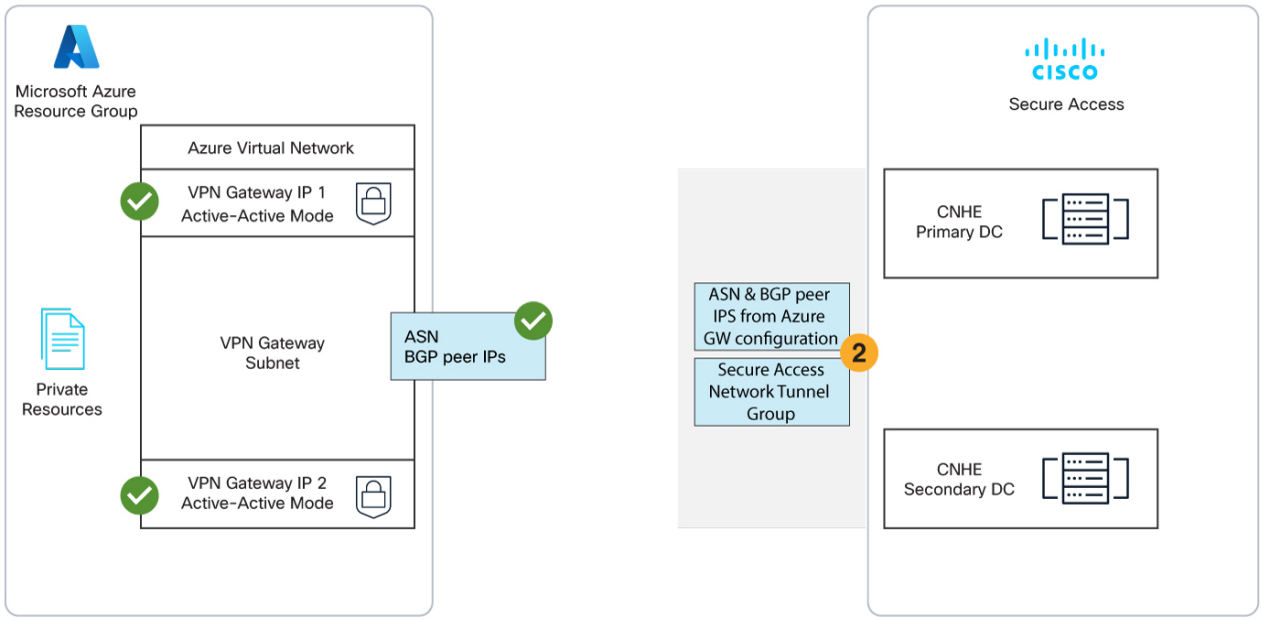


8. To review your configuration after deployment is complete, navigate to **Settings** > **Properties**.

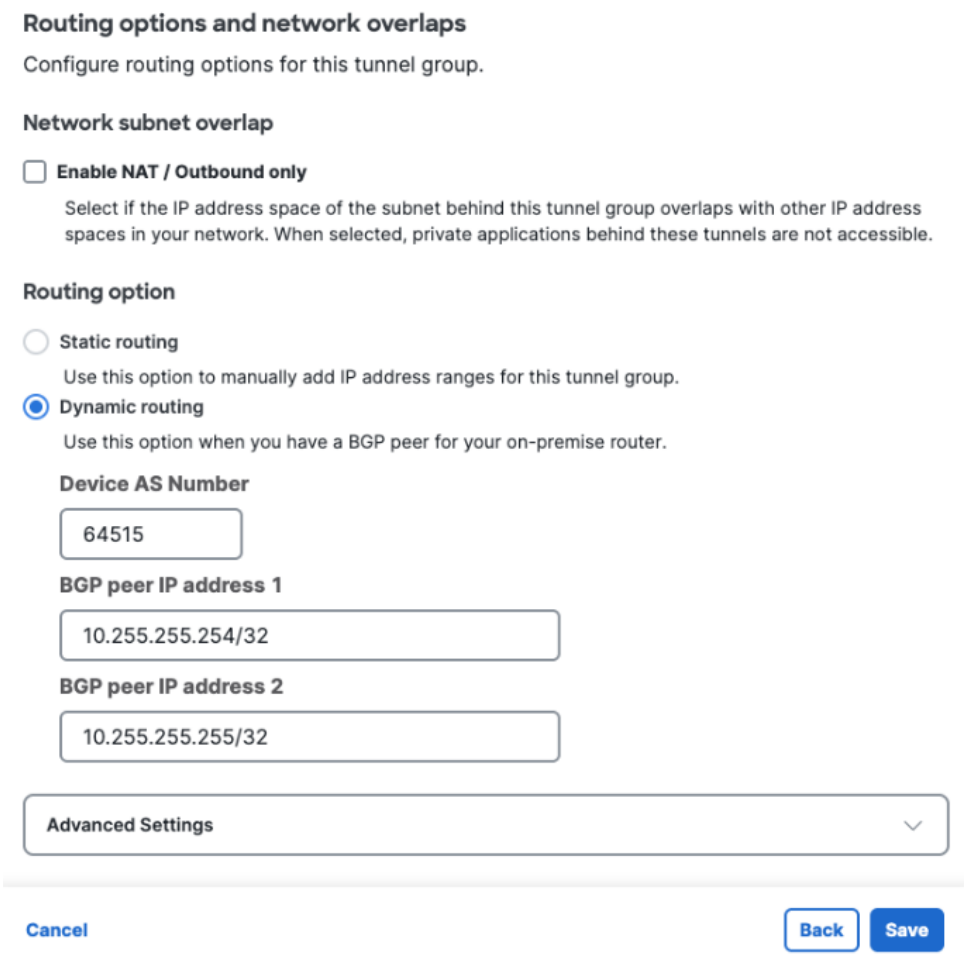


Component 2: Create a network tunnel group in Secure Access.

Configure a network tunnel group in Secure Access. For a more detailed procedure, see Add a Network Tunnel Group.



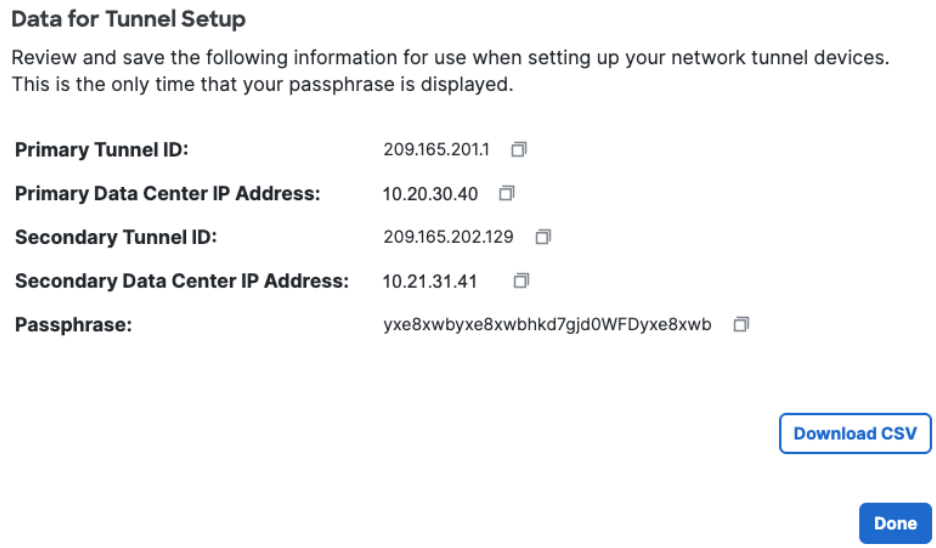
9. In **Step 1 – General Settings**: Set **Device Type** to AZURE.
10. In **Step 2 – Tunnel ID and Passphrase**: Enter the primary and secondary public IPs from the Azure virtual network gateway and create a passphrase.
11. In **Step 3 – Routing**:



a) Select **Dynamic routing**.
b) **Device AS Number**: Enter the ASN configured for the Azure virtual network gateway. This example uses `64515`.
c) **BGP peer IP address 1 and 2**: Enter two private IP address ranges (RFC1918). This example uses `10.255.255.254/32` and `10.255.255.255/32`.

> **Tip**
>
> BGP peer IP address compatibility between Azure and Secure Access
>
> By default, Secure Access listens for BGP peer requests in the the APIPA address range 169.254.0.0/24. Azure does not initiate BGP connections to peers in the range 169.254.0.0/16. To work around this limitation, configure the Secure Access tunnel group to listen for BGP peer requests from two RFC1918 private IP ranges. These ranges should not overlap with 169.254.0.0/16 or with ranges assigned to your other branches that connect to Secure Access.

12. In **Step 4 - Data for Tunnel Setup**: Copy or download the primary and secondary tunnel IDs, data center (DC) IP addresses, and the passphrase you created.

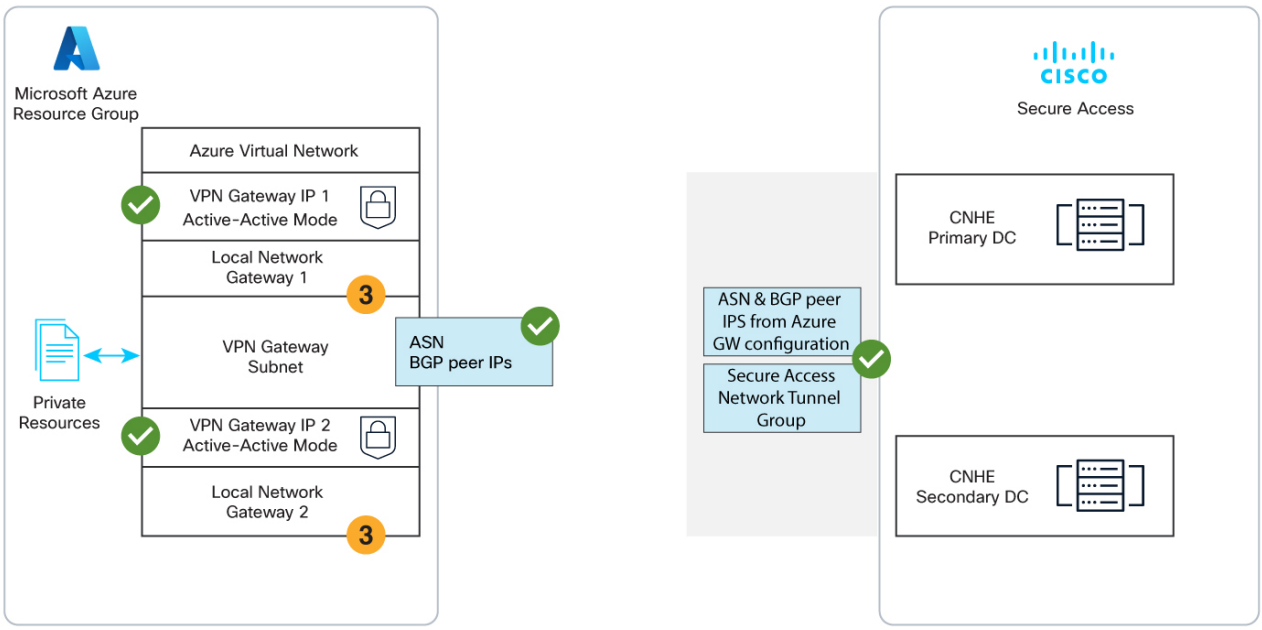


Important

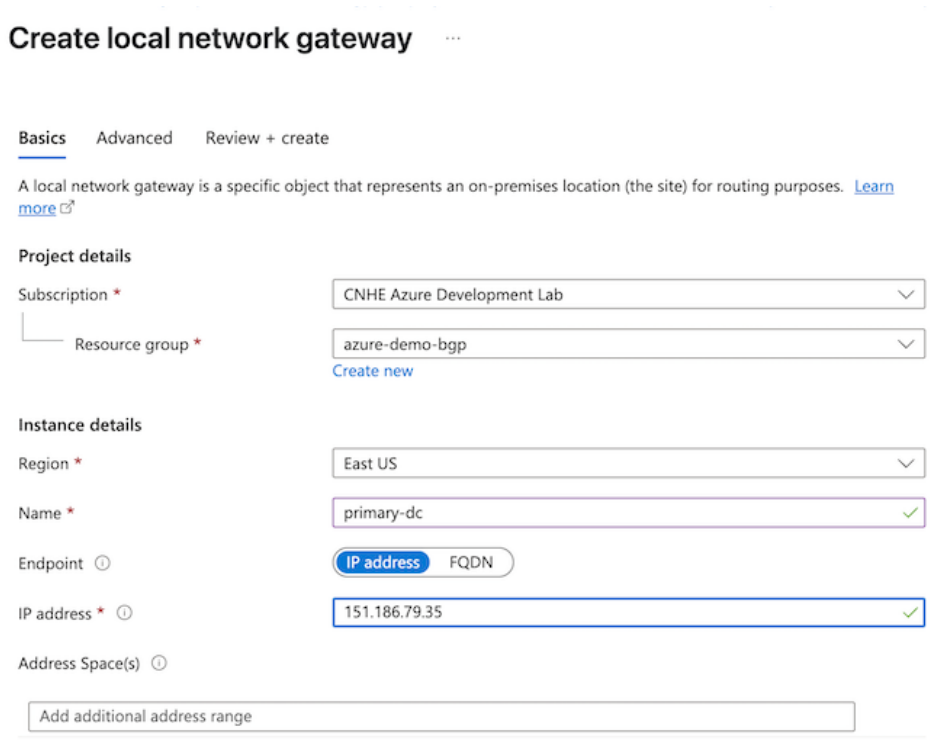
This is the only time your passphrase will be displayed.

Component 3: Create two local network gateways in Azure with S2S connections.

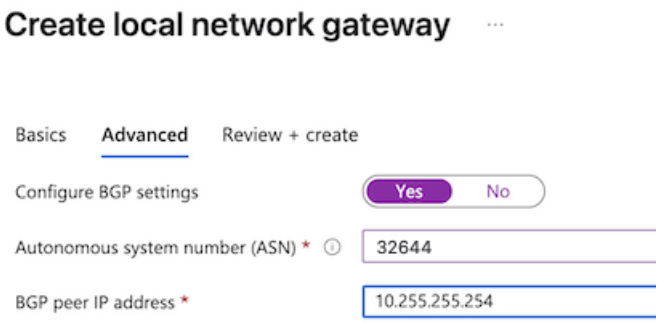
Create and configure two local network gateways in Azure, then connect them to Secure Access. The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.



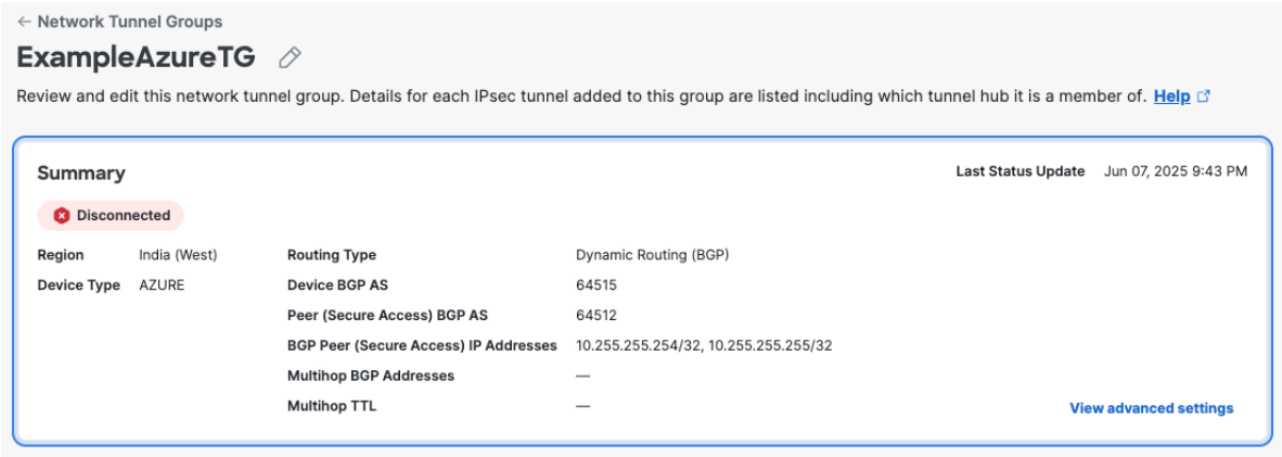
13. In the Azure admin portal, navigate to **Overview** > **Resource group (click the name of your resource group)** > **+ Create**.
14. Search the marketplace for **Local network gateway**, then click **Create**.



15. Configure the **Basics tab** of the first local network gateway.
    a) Select the **Subscription** and **Resource group** of your virtual network.
    b) Enter a **Name**. This example uses `primary-dc`.
    c) **Endpoint**: Select **IP address**.
    d) **IP address**: For the first local network gateway, enter the Primary DC IP Address from Secure Access **Step 4 – Data for Tunnel Setup**.
    e) Leave **Address space(s)** blank.
16. Configure the **Advanced tab** of the first local network gateway.

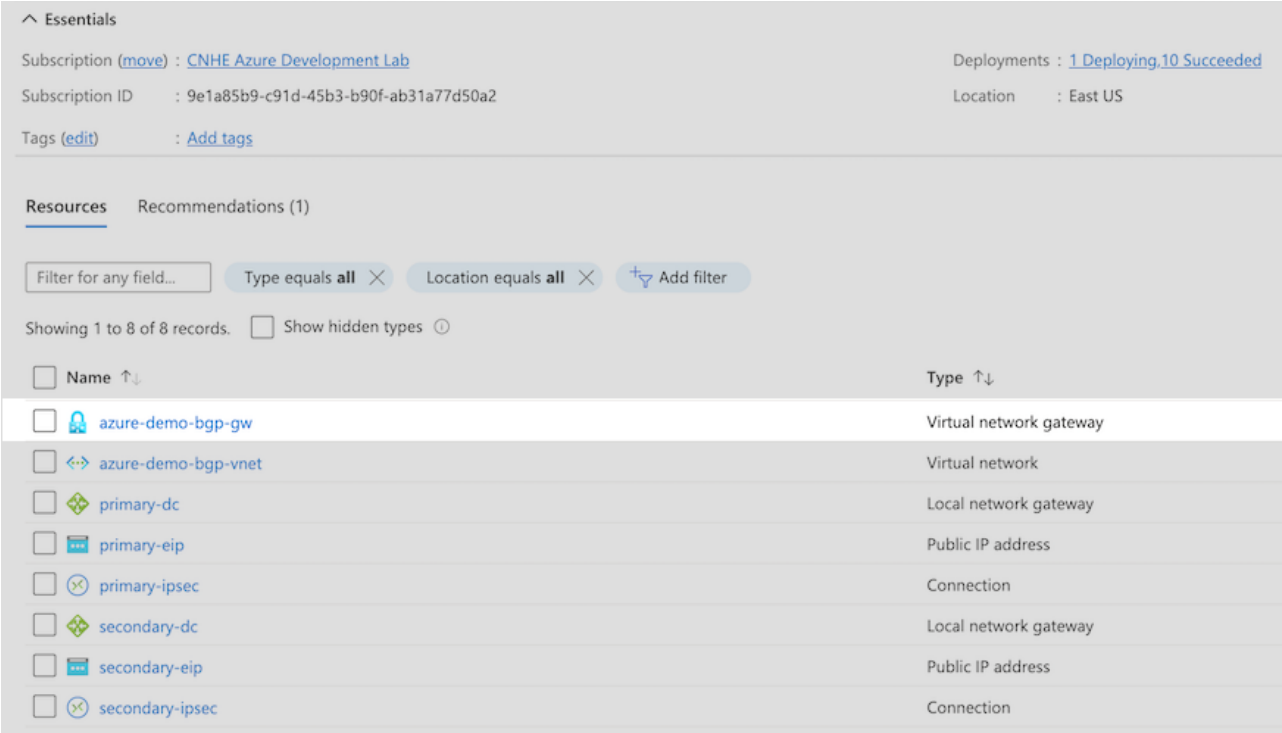


    a) **Configure BGP settings**: Select **Yes**.
    b) **Autonomous system number (ASN)**: Enter the **Peer (Secure Access) BGP AS** number from the Secure Access network tunnel group created earlier. This example shows the ASN `32644`. You can also find this ASN in the Summary section of your network tunnel group in Secure Access.
    c) **BGP peer IP address**: For the first local network gateway, enter the **BGP peer IP address 1** that you configured in **Secure Access Step 3 – Routing**. You can also find the BGP peer IP address in the Summary section of your network tunnel group in Secure Access.
17. Review the configuration, then click **Create**.



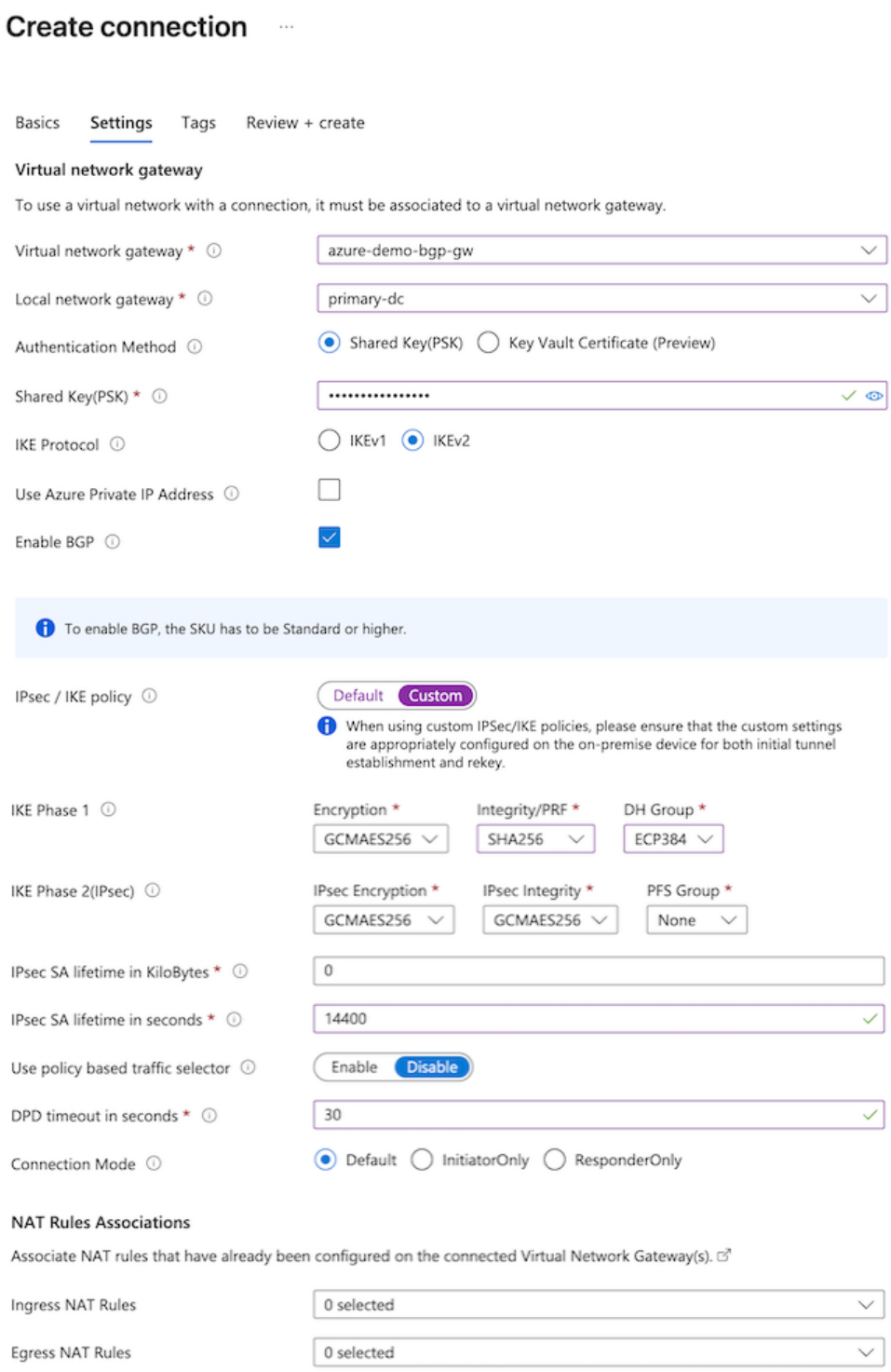
Azure will deploy the local network gateway and update the dashboard with the local network gateway resource when deployment is complete.

18. Repeat steps 3 and 4 to create the secondary local network gateway with the **BGP peer IP address 2** and the **Secondary DC IP Address** from Secure Access.

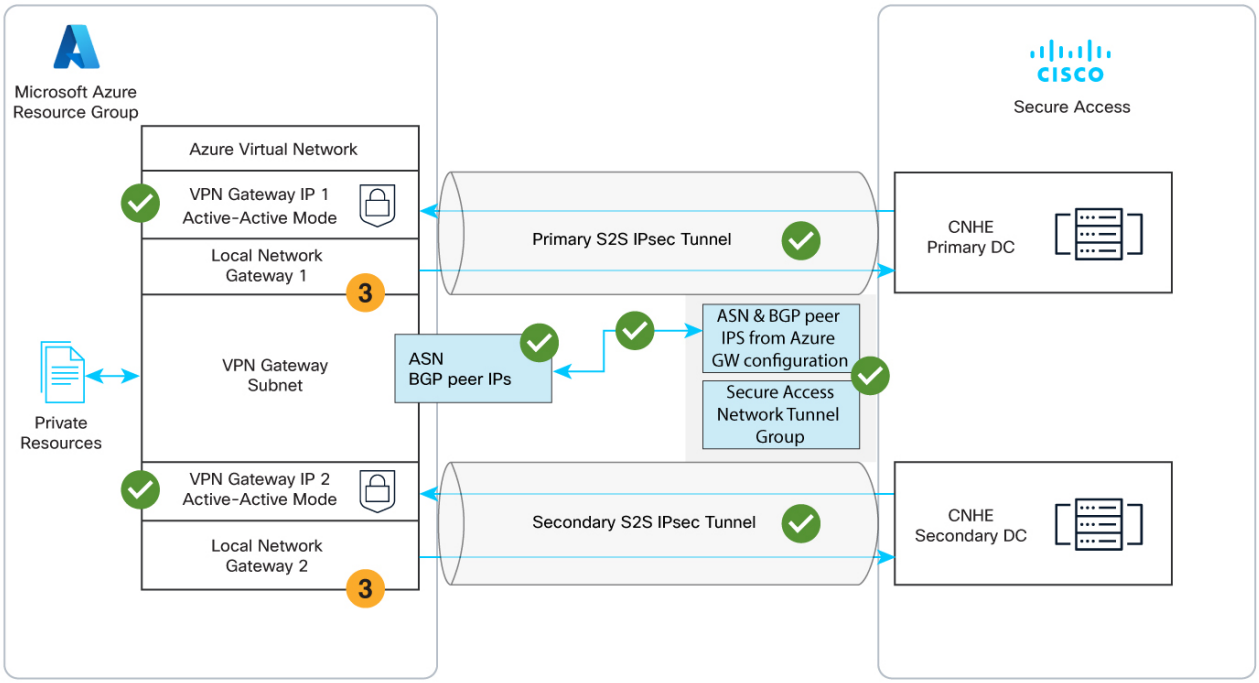


19. Create the S2S connection for the primary local network gateway.
    a) In the Azure admin portal, navigate to **Overview** > **Resource group (click the name of your resource group)** > **Resources**, then click the name of your virtual network gateway.
    b) Navigate to **Connections**, then click **+ Add**.
    c) Navigate to the **Basics tab**, then select the **Subscription** and **Resource group** of your virtual network.
    d) **Connection type**: Select **Site-to-site (IPsec)**.
    e) Navigate to the **Settings tab** of the connection, then select your virtual network gateway.
    f) **Local network gateway**: Select the primary gateway.
    g) **Shared Key (PSK)**: Enter the passphrase configured for the Secure Access network tunnel group in step 2.
    h) **Enable BGP**: Check the box.
    i) **IPsec / IKE policy**: Select **Custom**.
    j) **IKE Phase 1**: The following configuration is recommended.

- **Encryption**: GCMAE256.
- **Integrity/PRF**: SHA256.
- **DH Group**: ECP384.
- For information about cipher parameters supported by Secure Access, see Supported IPsec Parameters. For information about cipher parameters supported by Azure, see Microsoft documentation on Default IPsec/IKE parameters.
- **IPsec SA lifetime in seconds**: <3000. Note that any value less than 300 can cause the CHILD SA Rekey to enter a retry loop while the data plane is still active.
- **DPD timeout in seconds**: 30

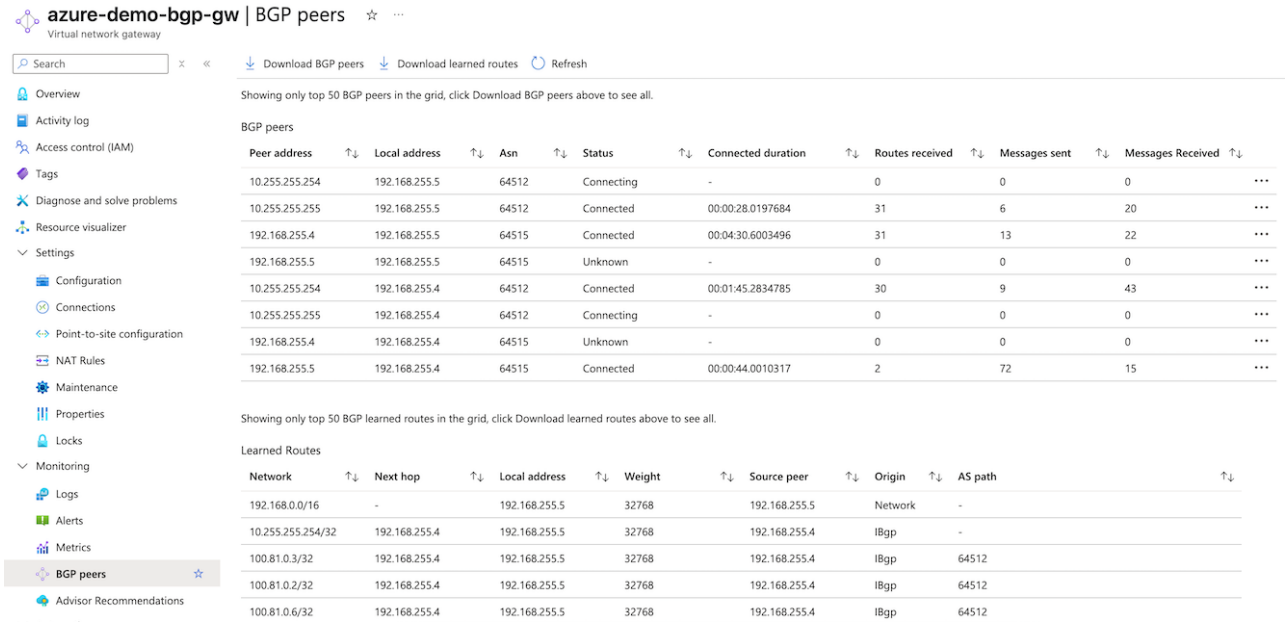


20. Review the configuration, then click **Create**.
    Azure will deploy the S2S connection and update the dashboard when deployment is complete.
21. Repeat step 6 for the secondary local network gateway.

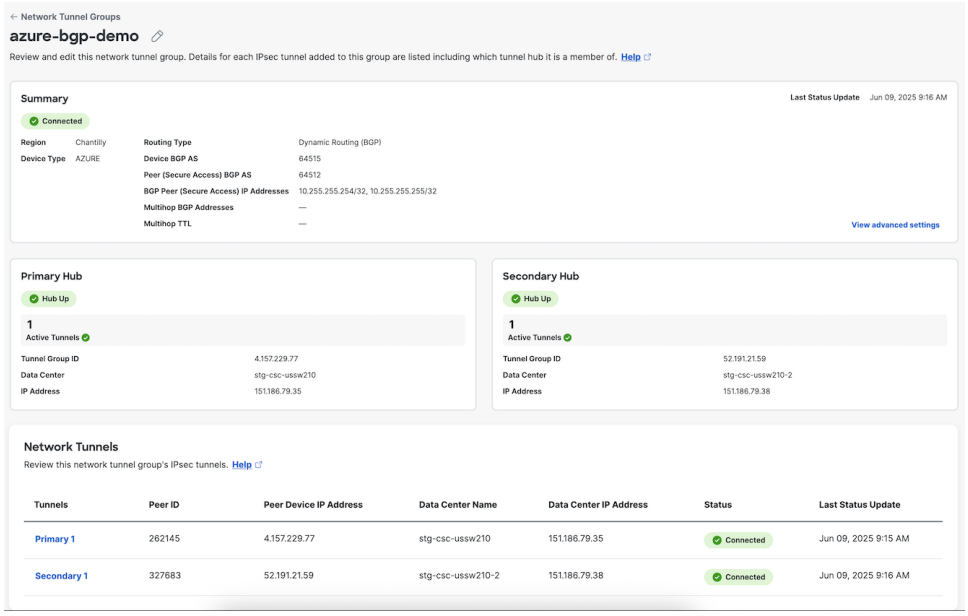


Both S2S VPN tunnels are now established with dynamic routing with BGP between your Azure virtual network gateway and the Secure Access DC.

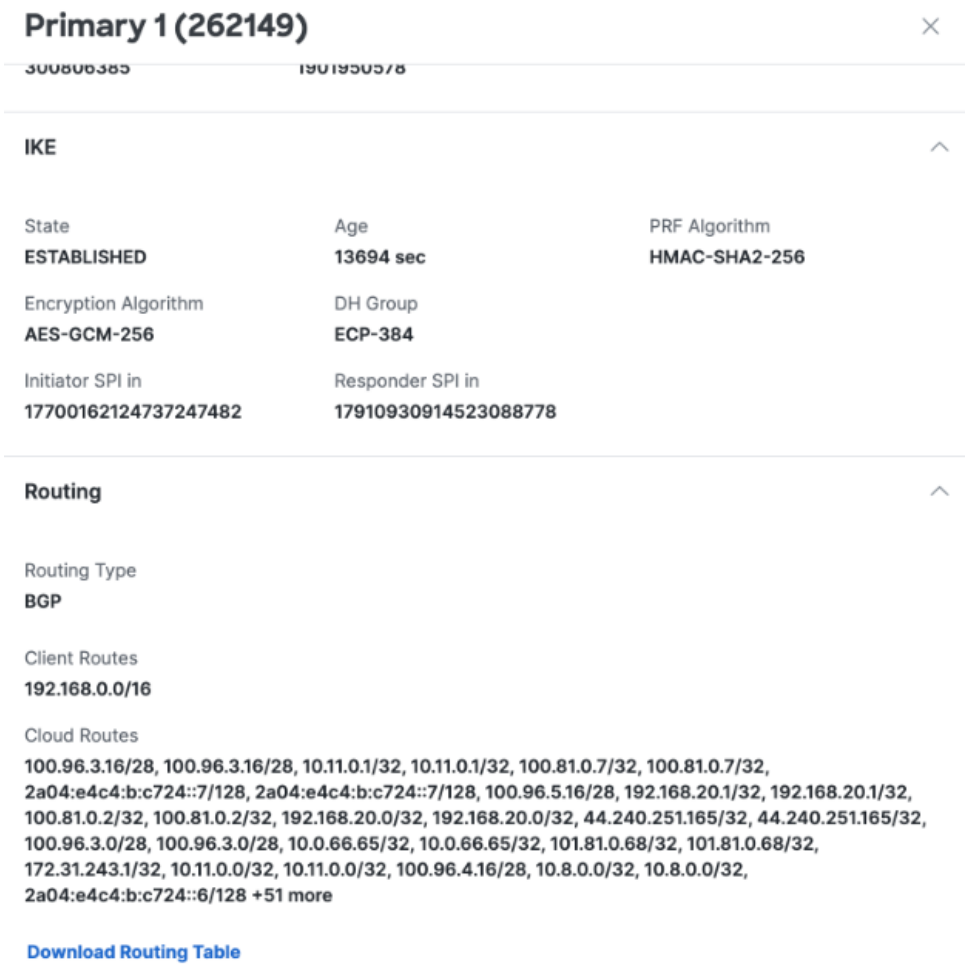
Component 4: Verify tunnel status in Azure and Secure Access.



22. In the Azure admin portal, navigate to **Overview** > **Resource group (click the name of your resource group)**, then click the name of your virtual network gateway.
23. Navigate to **Settings** > **BGP peers** to review the table of **Learned Routes** received by your Azure virtual network gateway and the Secure Access service.
24. In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click the name of the network tunnel group to review the connection status with Azure.



25. Under **Network Tunnels**, click a tunnel name to review **Routing** details. **Client Routes** show routes advertised by Azure to Secure Access via BGP. **Cloud Routes** show routes advertised by Secure Access to Azure via BGP.

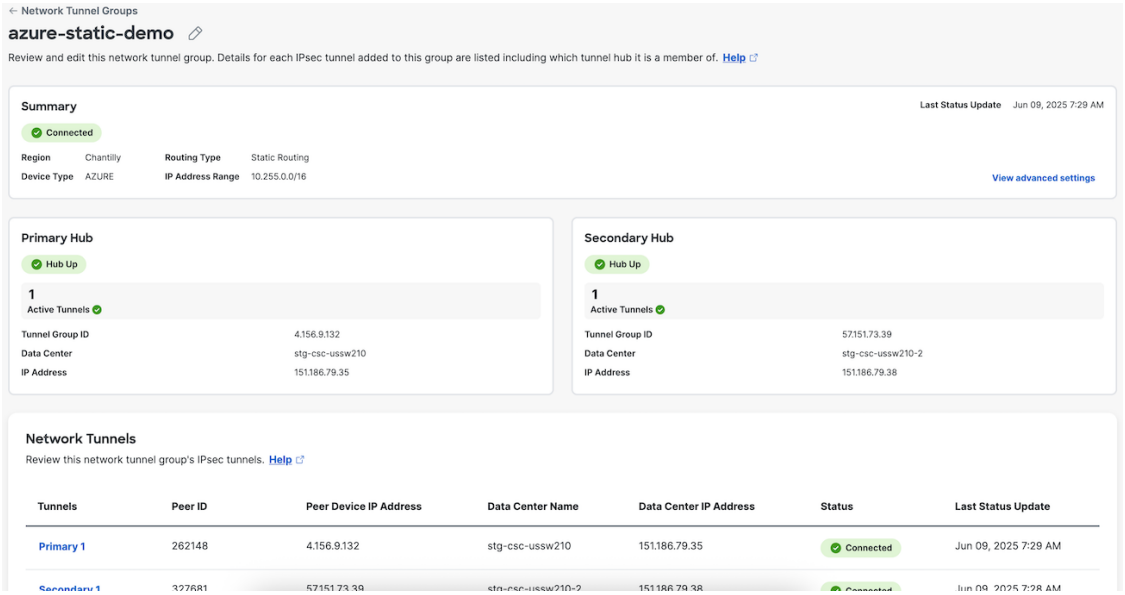


Branch access to resources in your Azure virtual network is now protected by the site-to-site (S2S) IPsec/IKEv2 VPN tunnel with Cisco Secure Access.

What to do next

Verify tunnel status in Secure Access

In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click the name of the network tunnel group to review the connection status with Azure.



Resources in your Azure virtual network are now protected by the site-to-site (S2S) IPsec/IKEv2 VPN tunnel with Cisco Secure Access.

For information about managing and monitoring your network tunnel group, see Manage Network Tunnel Groups.

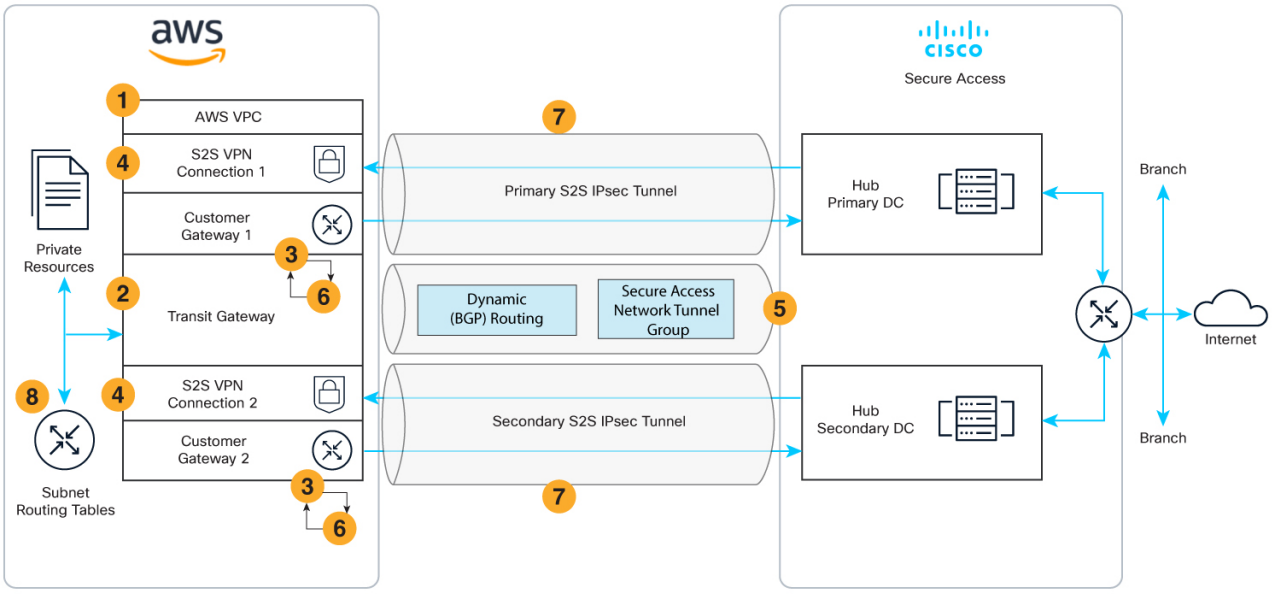
Configure a Site-to-Site VPN tunnel with Amazon Web Services

Understand how to deploy a site-to-site (S2S) VPN tunnel from Amazon Web Services (AWS) to Cisco Secure Access.

Deploy a site-to-site (S2S) VPN tunnel from Amazon Web Services (AWS) to Cisco Secure Access. An AWS S2S VPN in Secure Access will support the following:

- Tunnel redundancy with high availability for branch site connections to your Amazon Virtual Private Cloud (Amazon VPC). For more information, refer to Tunnel throughput, capacity, and scaling and Failover for Branch Connections in Secure Access Data Centers.
- Connection over IPsec (Internet Protocol Security) with authentication negotiated and traffic encrypted by IKEv2 (Internet Key Exchange, version 2). For more information, refer to Supported IPsec Parameters.
- Dynamic (BGP) routing. For more information, refer to Routing Options and Guidelines.

The S2S VPN topology depends on components configured in the following order. Components in the diagram are numbered by order of configuration.



For more detailed instructions, refer to Amazon Virtual Private Cloud Documentation. Please note that AWS may update their documentation without notice.

Limitations

- **Number of Primary Tunnels:** Secure Access supports a maximum of two primary tunnels within an AWS Site-to-Site (S2S) VPN tunnel group. Cisco has not validated configurations involving more than two S2S tunnels from a single AWS transit gateway. Additionally, the Secure Access dashboard does not provide the capability to add IP addresses for more than two tunnels in an AWS network tunnel group.
- **Bandwidth per Tunnel:** Each IPsec tunnel is limited to a maximum bandwidth of 1 Gbps. Given the two-tunnel limit, the total supported throughput for Secure Access in an AWS S2S VPN deployment is 2 Gbps.

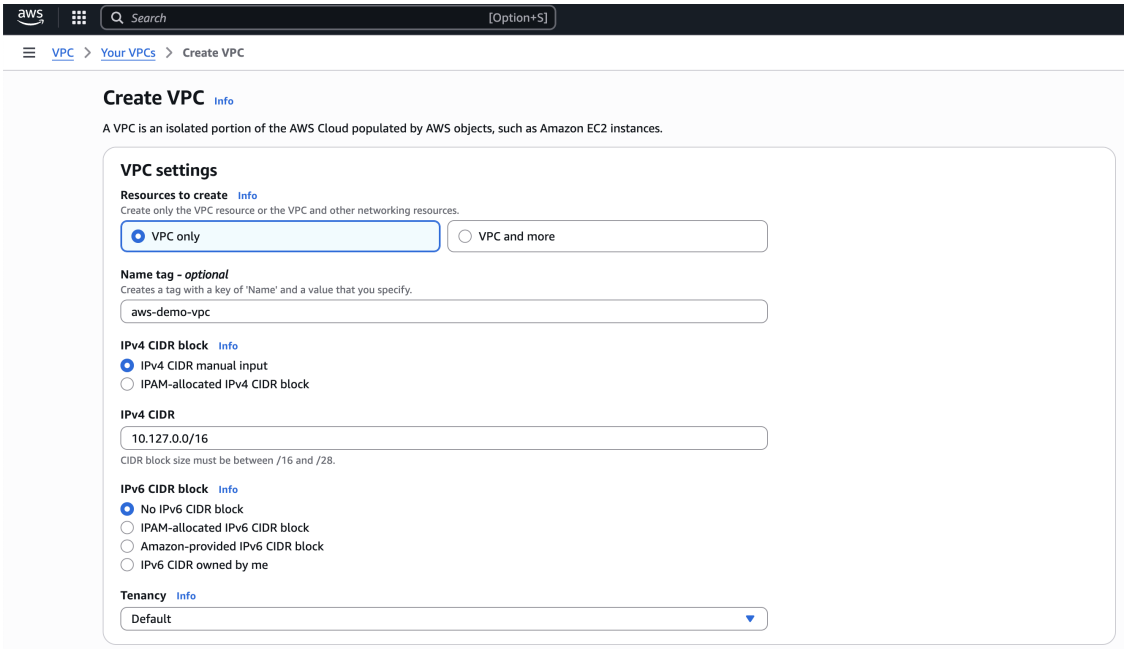
Before you begin

Prerequisites include the following.

- A valid Cisco Secure Access account.
- An AWS account with an active subscription and an Amazon VPC.

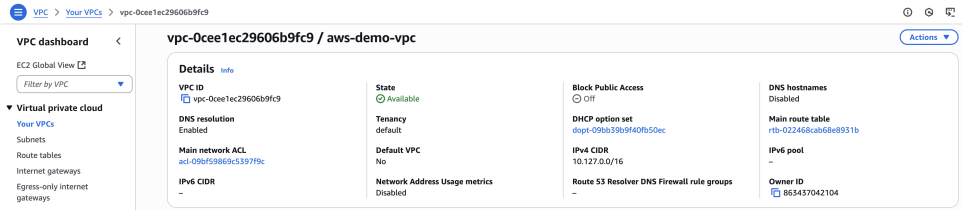
Procedure

Component 1: Create a VPC with two subnets in AWS–In your AWS dashboard, create a VPC with two subnets. Skip this step if you already have a VPC. For more information, refer to Create a VPC



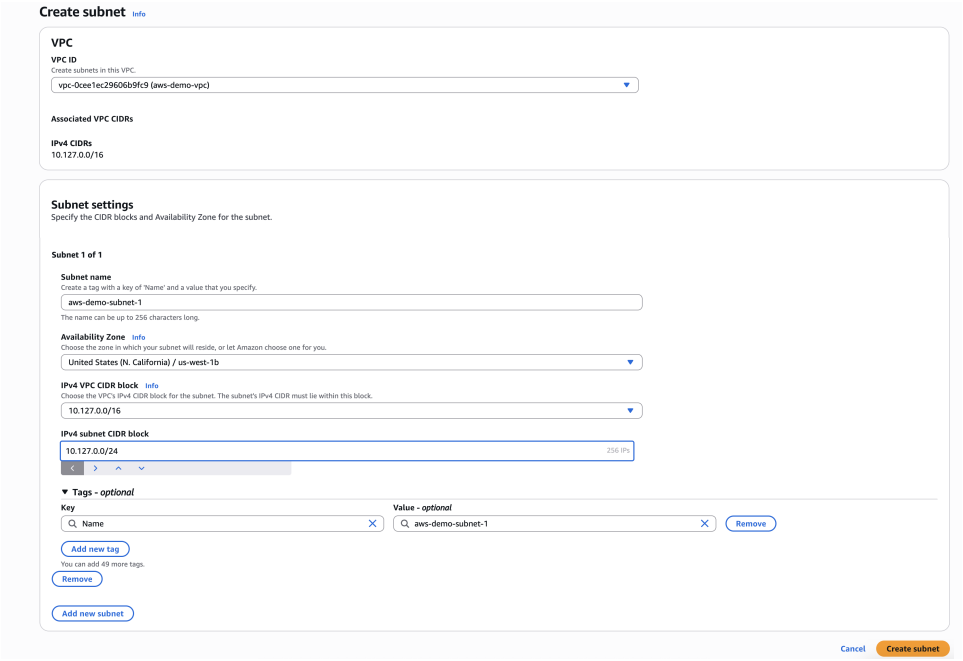
1. Navigate to **VPC dashboard** > **Create VPC**.
2. Resources to create: **VPC only**
3. IPv4 CIDR block: Choose **IPv4 CIDR manual input** and enter an **IPv4 CIDR** for your VPC.
4. Click **Create VPC**.

   The AWS dashboard shows the new VPC details.



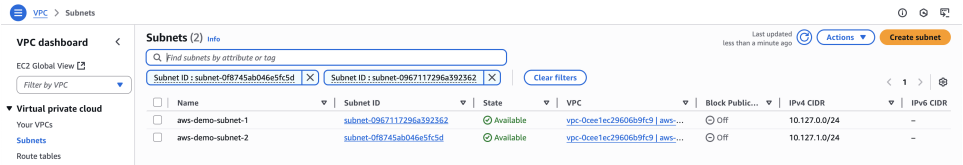
5. Navigate to **VPC dashboard** > **Virtual private cloud** > **Subnets**.
6. Click **Create subnet**.
7. Choose your **VPC ID** or IP address.

   The AWS dashboard shows the **Create subnet** menu.



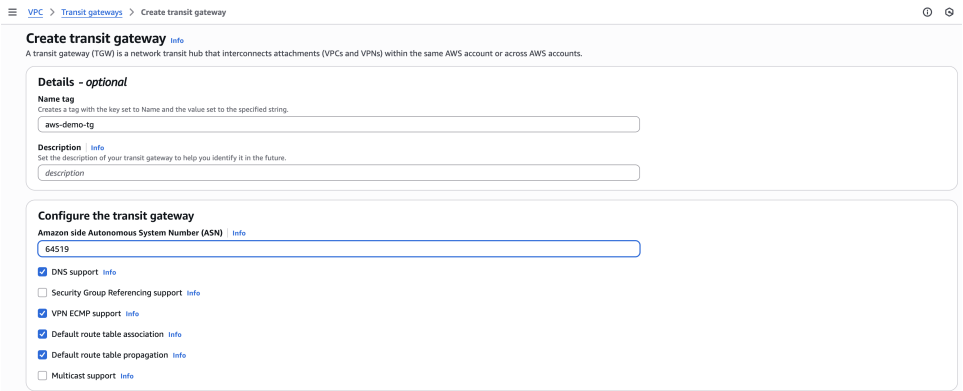
8. Configure subnet 1 of 2.
   a) Enter a **Subnet name** that indicates the VPC and whether this is the first or second subnet.
   b) Choose an **Availability Zone**.
   c) Enter an **IPv4 subnet CIDR block** that is within the VPC CDIR range and does not overlap with the IPv4 range of other subnets in the VPC.
9. Click **Add a subnet**. Repeat the above steps to configure subnet 2 of 2 with a different availability zone for high availability.
10. Click **Create subnet**.

    The AWS dashboard shows the new subnets.



Component 2: Create a Transit Gateway in AWS–Create a transit gateway in AWS with an attachment to your Amazon VPC. For more information, refer to Connect your VPC to other VPCs and networks using a transit gateway, Create a transit gateway using Amazon VPC Transit Gateways, and Create a VPC attachment using Amazon VPC Transit Gateways.

11. Click **Transit gateways** in the left navigation menu of the AWS VPC dashboard.
    The AWS dashboard shows the transit gateway configuration menu.

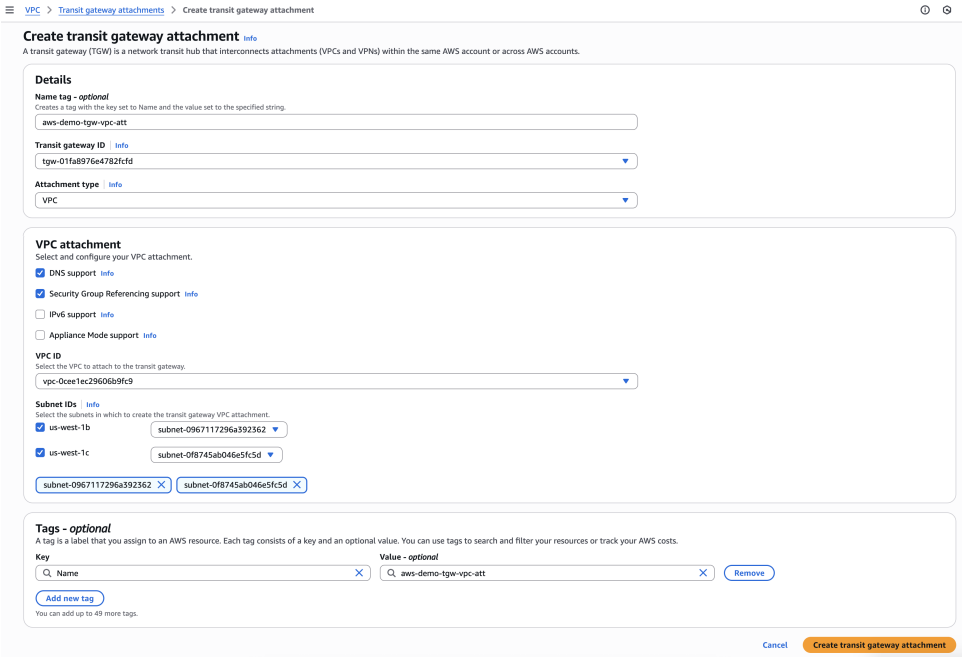


12. Create a transit gateway with an Amazon-side **Autonomous System Number (ASN)**.

> **Note**
>
> The Amazon side ASN is required for dynamic routing supported by Border Gateway Protocol (BGP) sessions. This example uses 64519. The range is from 64512 to 65534 for 16-bit ASNs. We recommend entering an ASN that is not already in use by other transit gateways in your Amazon VPC.

13. Click **Create transit gateway**.

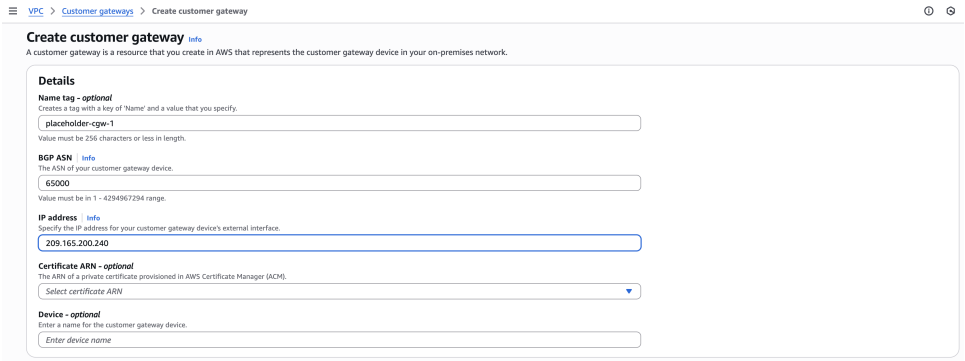
Once the gateway Status is Available, create a transit gateway attachment between the transit gateway and the VPC.



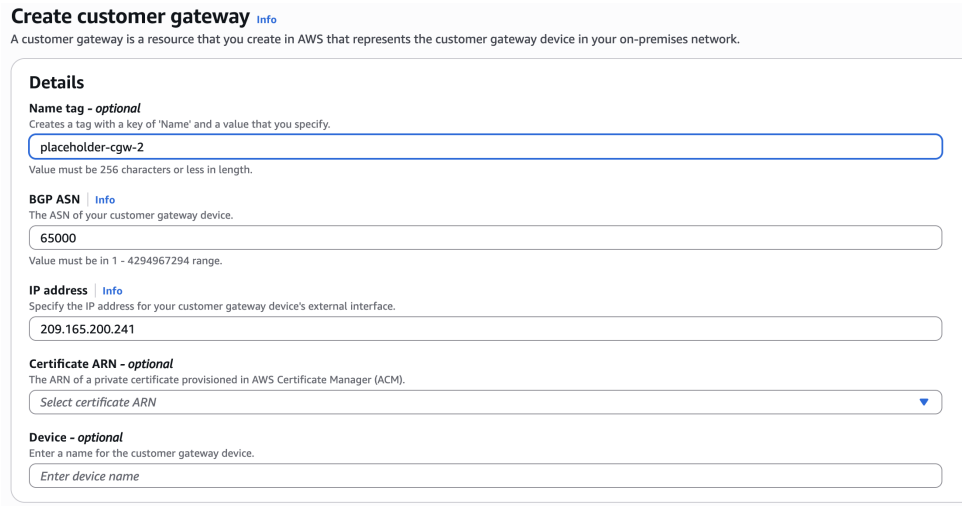
14. Click **Transit gateway attachments** in the left navigation menu of the AWS VPC dashboard.
15. Click **Create transit gateway attachment**.
16. Select the **Transit gateway ID** of the gateway you just created.
17. Select the **VPC ID** of the VPC you created for Component 1.
18. Click **Create transit gateway attachment**.

Component 3: Create two placeholder Customer Gateways in AWS–Create two customer gateways with S2S connections. For more information, refer to Get started with AWS Site-to-Site VPN, Step 1: Create a customer gateway and Step 5: Create a VPN connection.

> **Note**
>
> These gateways will act as temporary placeholders that provide outside IP addresses required by the Secure Access network tunnel group configuration in the next step. The network tunnel group will provide the Secure Access BGP ASN and public IP addresses for the Secure Access Peer IP address DCs that you will use to create two new customer gateways in AWS.



19. In the left navigation menu of the AWS VPC dashboard, navigate to **Virtual private network (VPN)** and click **Customer gateways**.
20. Click **Create customer gateway**.
21. Repeat these steps to create a second customer gateway with a different placeholder IP address. This example uses 209.165.200.241.



Component 4: Create a Site-to-Site VPN connection for each customer gateway

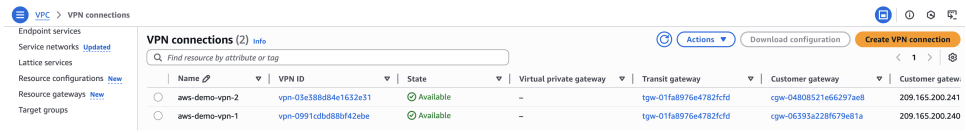
22. In the left navigation menu of the AWS VPC dashboard, navigate to **Virtual private network (VPN)** and click **Site-to-Site VPN** connections.
23. Click **Create VPN connection** and configure the following:
    a) **Target gateway type**: Transit gateway
    b) Select the virtual private gateway that you created earlier.
    c) **Customer gateway**: Existing
    d) Select the first customer gateway that you created earlier.
    e) **Routing options**: Dynamic
    f) **Tunnel 1 options** > **Inside IPv4 CIDR for tunnel 1**: Enter a size /30 IPv4 block from the 169.254.0.0/24 range.

> **Note**
>
> AWS allows inside CIDR addresses in the 169.254.0.0/16 range in which the network address is the first 16 bits, with 65,536 IP addresses in the range 169.254.0.0 to 169.254.255.255. Secure Access utilizes the 169.254.0.0/24 subnet range for BGP peer addresses, refer to Secure Access BGP Configuration.

g) **Tunnel 1 options** > **Pre-shared key for tunnel 1**: Enter a passphrase. You will enter this in the Secure Access network tunnel group in the next step.
h) **Tunnel 1 options** > **Advanced options for tunnel 1**: Edit tunnel 1 options.
i) **Tunnel 1 options** > **DPD timeout action**: Restart.
j) **Tunnel 1 options** > **Startup action**: Start.

24. Repeat these steps for Tunnel 2 options with a different size /30 IPv4 block from the 169.254.0.0/24 range. Refer to the note above about the difference in CIDR range requirements between AWS and Secure Access.
25. Click **Create VPN connection**.
26. Repeat these steps to create a second VPN connection.
    a) Select the second customer gateway that you created earlier.
    b) **Inside IPv4 CIDR for tunnels 1 and 2** should match the inside IP addresses you entered for tunnels 1 and 2 in the first S2S connection.

Confirm that both S2S VPN connections have an available **State**.

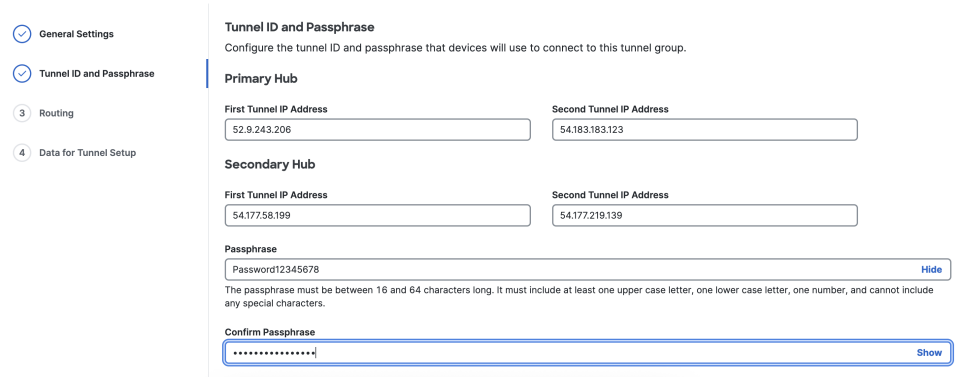


Component 5: Create a network tunnel group in Secure Access–For a more detailed procedure, refer to Add a Network Tunnel Group.

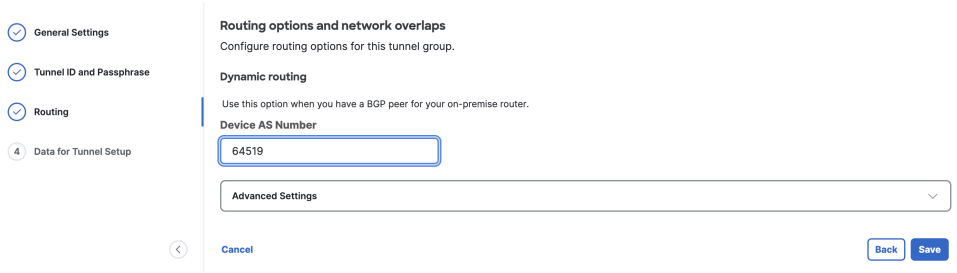
27. **Step 1 - General Settings**: Set **Device Type** to AWS.
28. **Step 2 - Tunnel ID and Passphrase**: Each AWS customer gateway that you created in the previous step will have two tunnels, and each tunnel will have an outside IP address.
    a) **Primary Hub** > **First Tunnel IP Address**: Enter the outside IP address of tunnel 1 for AWS S2S VPN connection 1.

> **Note**
>
> To find this IP address in AWS, navigate to **VPC** > **VPN connections**, click the **VPN ID** of VPN connection 1, then navigate to **Tunnel state** > **Tunnel 1** > **Outside IP address**.

    b) **Primary Hub** > **Second Tunnel IP Address**: Enter the outside IP address of tunnel 2 for AWS S2S VPN connection 1.
    c) **Secondary Hub** > **First Tunnel IP Address**: Enter the outside IP address of tunnel 1 for AWS S2S VPN connection 2.
    d) **Secondary Hub** > **Second Tunnel IP Address**: Enter the outside IP address of tunnel 2 for AWS S2S VPN connection 2.
    e) **Passphrase**: Enter the pre-shared key that you created for the tunnels in AWS.



29. **Step 3 - Routing, Dynamic routing** > **Device AS Number**: Enter the Amazon-side Autonomous System Number (ASN) configured for the Transit Gateway in AWS.



30. **Step 4 - Data for Tunnel Setup**: Copy or download the primary and secondary tunnel IDs, data center (DC) IP addresses, and passphrase (pre-shared key). This is the only time your passphrase will be displayed.

Component 6: Replace the placeholder customer gateways in AWS–Configure two more customer gateways in AWS to connect to the Secure Access DC IPs. These will replace the placeholder customer gateways that you created for Component 3.

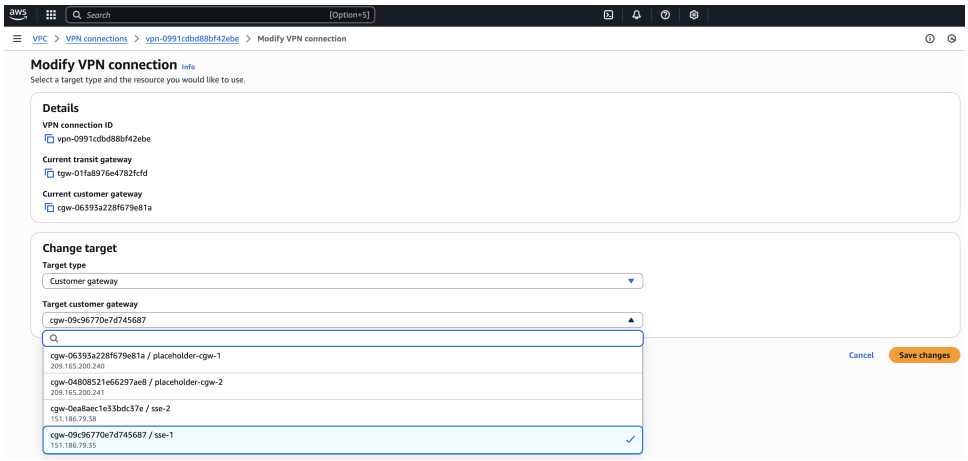
> **Note**
>
> It is not possible to update the placeholder customer gateways. You must create new customer gateways with the DC IPs from Secure Access, then modify the VPN connection in AWS to target the new customer gateways.

Before you begin, you will need this information from Secure Access:

- The DC IP addresses for the primary and secondary tunnel from Component 4. You can also find this information in Secure Access by navigating to **Connect** > **Network Connections** > **Network Tunnel Groups** and clicking the network tunnel group name for details.
- The Peer (Secure Access) BGP AS number for the network tunnel group. Find this information in Secure Access by navigating to **Connect** > **Network Connections** > **Network Tunnel Groups** and clicking the network tunnel group name for details.

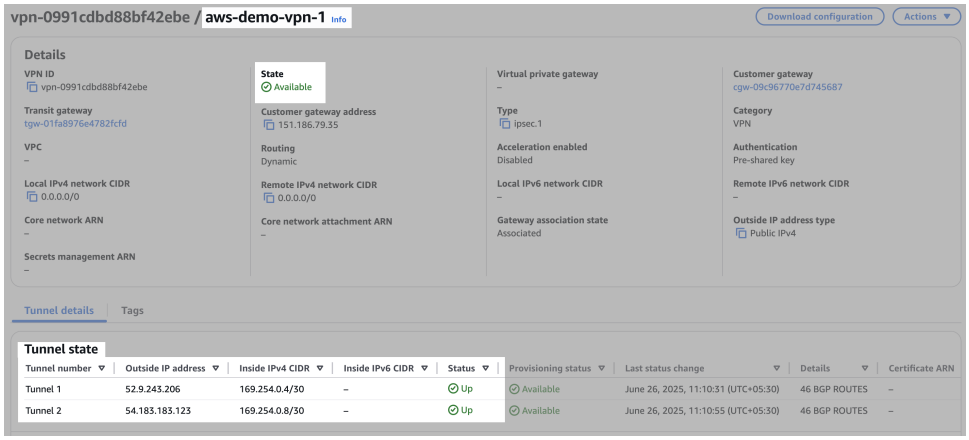
31. Create two customer gateways using the same procedure that you followed for Component 3:
    a) In AWS VPC dashboard, navigate to **Virtual private network (VPN)** and click **Customer gateways**.
    b) Click **Create customer gateway**.
    c) **BGP ASN**: Enter the Peer (Secure Access) BGP AS from the Secure Access network tunnel group.
    d) **IP address**: Enter the DC IP address for the Secure Access primary tunnel.
    e) Click **Create customer gateway**.
    f) Repeat these steps to create a secondary customer gateway with the DC IP address for the Secure Access secondary tunnel.

32. Modify the VPN connection in AWS. For more information, refer to Modify AWS Site-to-Site VPN connection options.
    a) In the left navigation menu of the AWS VPC dashboard, navigate to **Virtual private network (VPN)** and click **Site-to-Site VPN connections**.
    b) Click the **VPN ID** of the first connection. Navigate to **Actions** > **Modify VPN connection**.
    c) Change **Target customer gateway** to the primary tunnel customer gateway created to replace the placeholder gateway.
    d) Click **Save changes**.
    e) Repeat these steps for the second VPN connection and the secondary tunnel customer gateway.
    f) Delete the placeholder customer gateway.

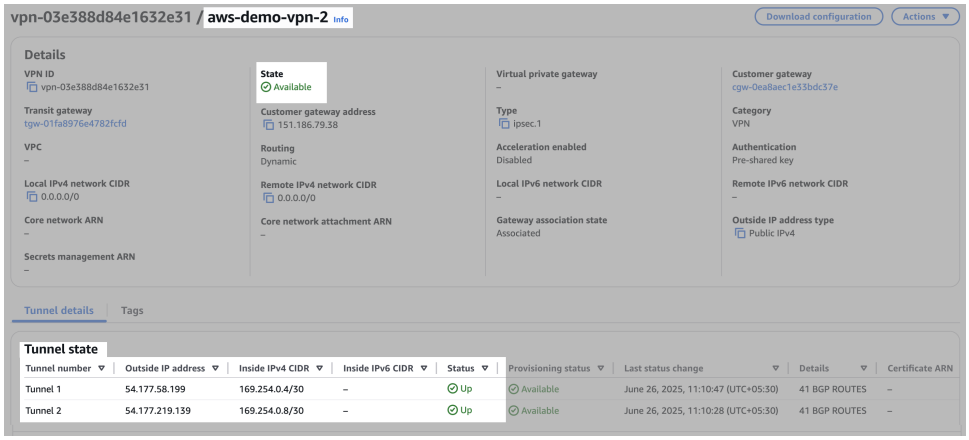


Component 7: Verify tunnel status in AWS and Secure Access–In the left navigation menu of the AWS VPC dashboard, navigate to **Virtual private network (VPN)** and click **Site-to-Site VPN connections**. Click the **VPN ID** of each VPN connection to confirm that the **State** is Available and that the **Status** of both tunnels is Up.

This example shows VPN connection 1 is Available and both tunnels are Up:

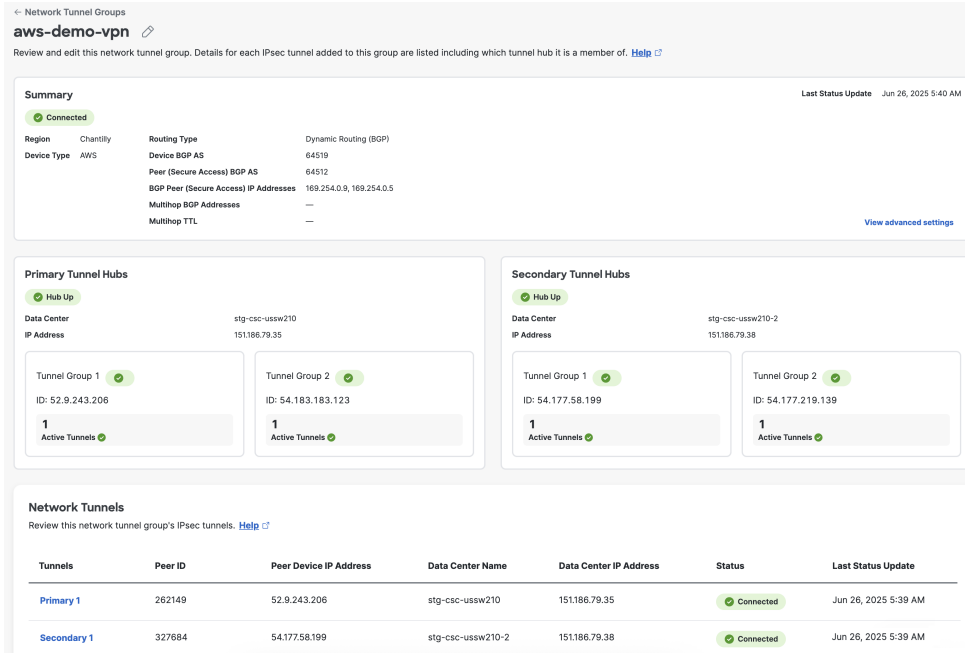


VPN connection 2 is also Available and both tunnels are Up.

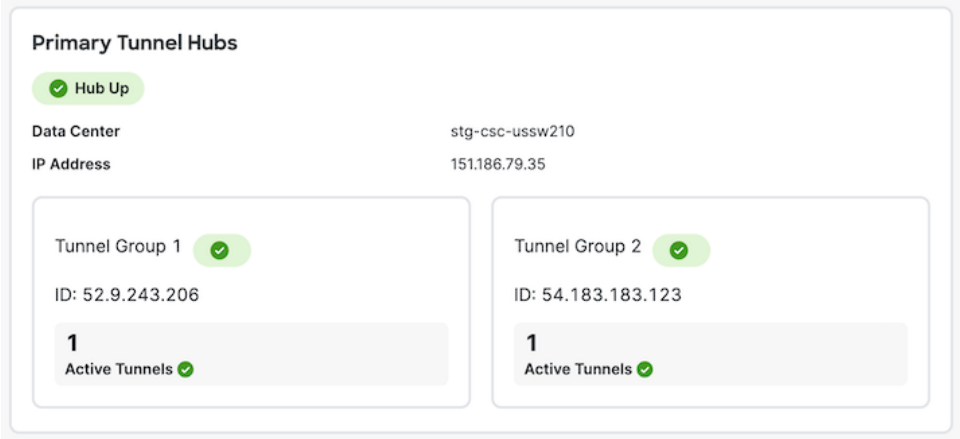


Note that each tunnel has a unique **Outside IP Address**. Tunnel 1 has the same **Inside IPv4 CIDR range** for each VPN connection, and Tunnel 2 has the same **Inside IPv4 CIDR range** for each VPN connection.

33. In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click the name of the network tunnel group to review the connection status with AWS.

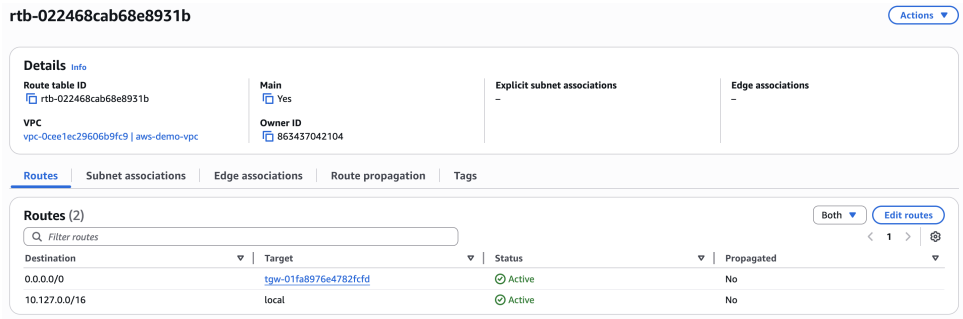


34. Verify the IP address values under **Primary Tunnel Hubs** in Secure Access. The ID of Tunnel Group 1 should match the **Outside IP Address** of VPN connection 1, Tunnel 1 in AWS. The ID of Tunnel Group 2 in Secure Access should match VPN connection 1, Tunnel 2 in AWS.



35. Verify the IP address values under **Secondary Tunnel Hubs** in Secure Access. The tunnel group IDs should match the tunnel addresses of VPN connection 2 in AWS.
    When the tunnel group IDs in the Secure Access primary and secondary tunnel hubs match the tunnel addresses of AWS VPN connections 1 and 2, this confirms that the tunnel connection has been established between AWS and Secure Access DCs.

Component 8: Modify subnet routing tables to send traffic to the AWS Transit Gateway–To send traffic from the AWS VPC to the AWS transit gateway, modify the routing table of each subnet to target the Transit gateway ID. For more information, refer to Change a subnet route table.



36. In AWS, navigate to **VPC dashboard** > **VPC ID** > **Main route table** > **Route table ID** > **Edit routes** > **Add route**.
    a) **Destination**: Enter the value 0.0.0.0/0.
    b) **Target**: Transit Gateway, select your Transit Gateway ID.
    c) Click **Save changes**.

37. In Secure Access, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**.
    a) Click the name of the network tunnel group, then click a tunnel name to review Routing details.
    b) **Client Routes** show routes advertised by Amazon to Secure Access via BGP.
    c) **Cloud Routes** show routes advertised by Secure Access to Amazon via BGP.

This confirms that branch access to resources in your AWS VPC is now protected by the site-to-site (S2S) IPsec/IKEv2 VPN tunnel with Cisco Secure Access.

What to do next

For information about managing and monitoring your network tunnel group, refer to Manage Network Tunnel Groups.

11 DNS and DDNS Servers

Topics:

- Manage DNS and DDNS Servers
- Manage DNS Servers
- Map DNS Servers to Regions
- Manage DDNS Servers
- Map DDNS Servers to Regions

Provides an overview of DNS and DDNS Servers in Cisco Secure Access, including Manage DNS and DDNS Servers, Manage DNS Servers, and Map DNS Servers to Regions. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage DNS and DDNS Servers

Map domain names to IP addresses using DNS and DDNS.

DNS (Domain Name System) is a protocol that translates (resolves) a user-friendly domain name, such as www.cisco.com, to an IP address so that users can access computers, websites, services, or other resources on the internet or private networks.

DDNS (Dynamic DNS) service updates the mappings of domain names to IP addresses to provide accurate IP addresses to DNS clients. When a remote user's network IP address changes, Secure Access can use DDNS to update its system with the new IP address, maintaining seamless connectivity.

See the following topics for more information:

- Manage DNS Servers
- Map DNS Servers to Regions
- Manage DDNS Servers
- Map DDNS Servers to Regions

Manage DNS Servers

Use DNS servers to resolve DNS requests from to internet resources.

You can add DNS servers to resolve DNS requests to internet resources. When adding these DNS servers, DNS Server 1 resolves before DNS Server 2. These DNS Server objects can be applied to RA-VPN IP pools, and selected in private resource definitions for ZTA access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Have the details of DNS servers capable of resolving both IPv4 and Ipv6 is applicable.

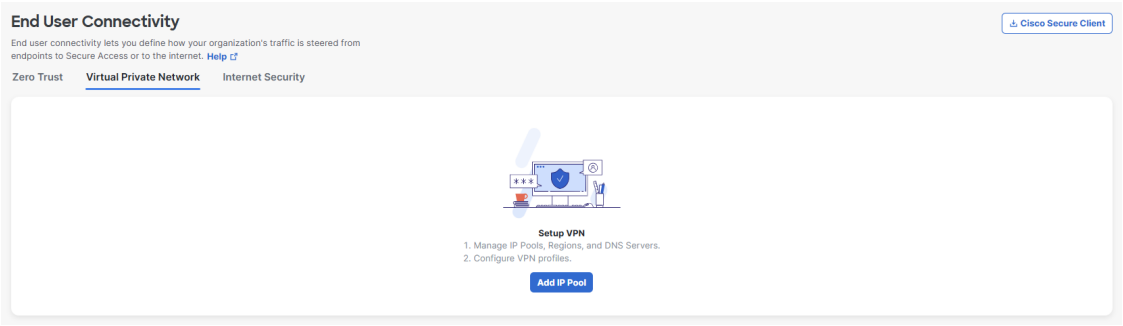
Add a DNS Server

Provides instructions for completing the Add a DNS Server workflow in Cisco Secure Access. Add an IP address or address range for a DNS server.

Add an IP address or address range for a DNS server. Your DNS traffic routes through the DNS servers managed by Secure Access.

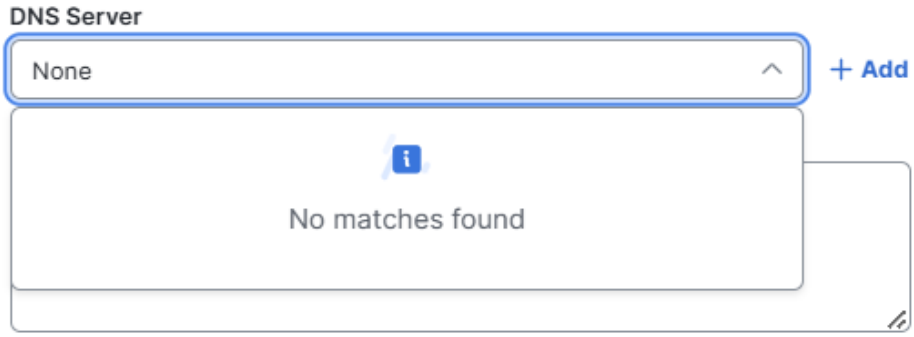
Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**, then click **Add IP Pool**.

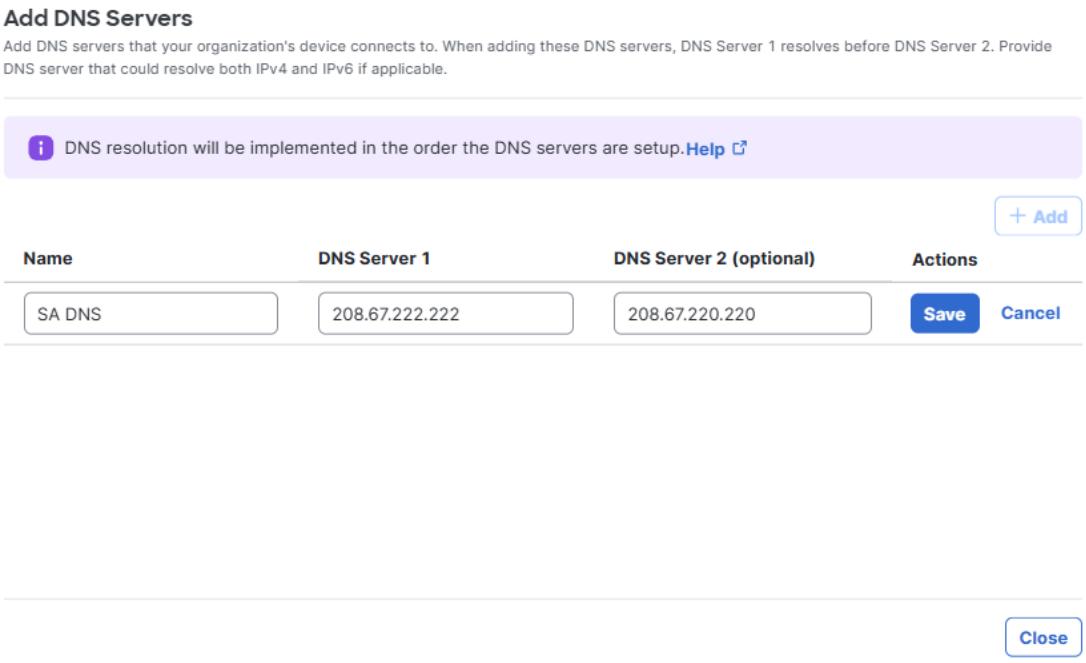


2. Click **Add IP Pool**.
3. Enter the IP pool parameters, including the required **DNS Server**.

   During the initial deployment before any IP pools have been configured, there is no DNS configuration. You must provide a valid DNS server.



4. Click **+ Add** to configure a new DNS server.
   a) Input a **Name**.
   b) **DNS Server 1**: Provide the IP address of the primary DNS server.
   c) **DNS Server 2** (optional): Provide the IP address of the secondary DNS server.



> **Note**
>
> DNS server fields cannot use addresses/networks listed in IP Address Restrictions.

5. Click **Save**, then click **Close**.

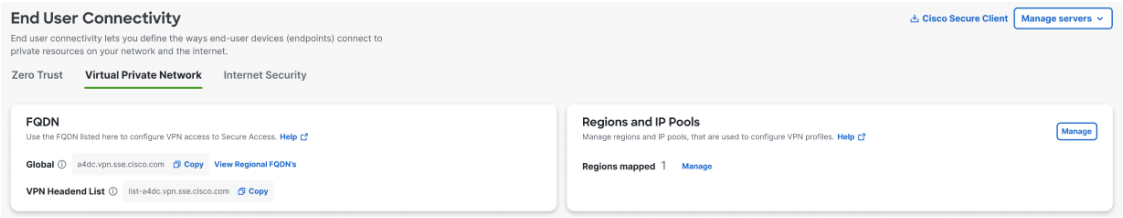
View DNS Servers

Provides instructions for completing the View DNS Servers workflow in Cisco Secure Access. You can view the DNS servers that are configured for your organization.

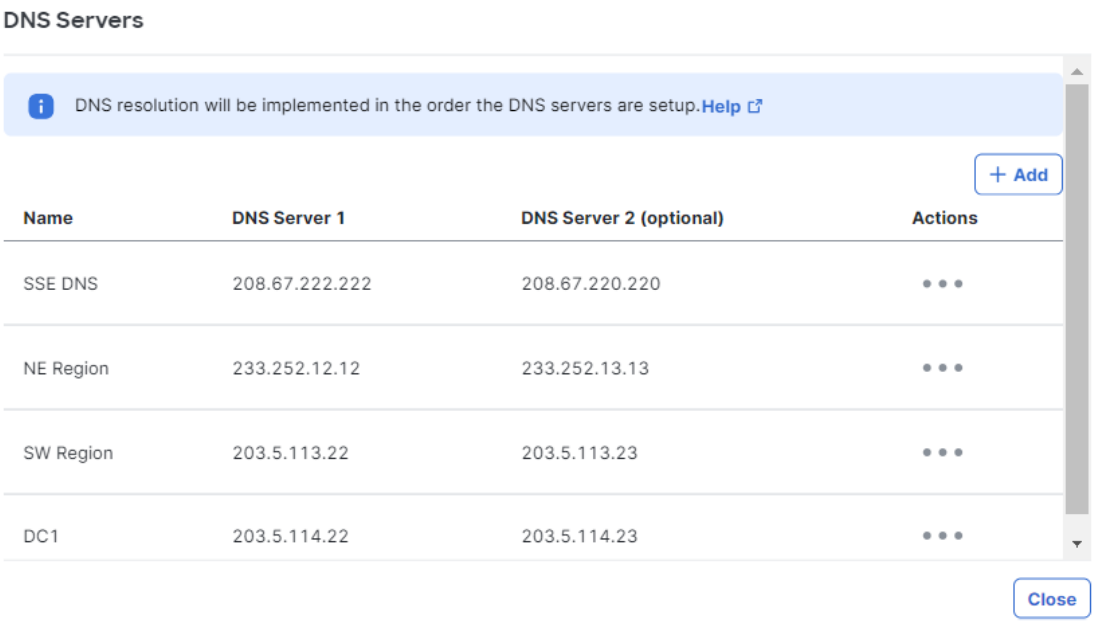
You can view the DNS servers that are configured for your organization. Your DNS traffic routes through the DNS servers managed by Secure Access.

Procedure

1. Navigate to **Connect** > **End User Connectivity**, click **Manage Servers** and choose **DNS Servers**.



2. The list of configured DNS servers is displayed.



3. From the list you can click **Add** to add a new entry, or click the ellipsis (...) to **Edit** or **Delete** a DNS server entry.
4. Click **Close** to dismiss the list.

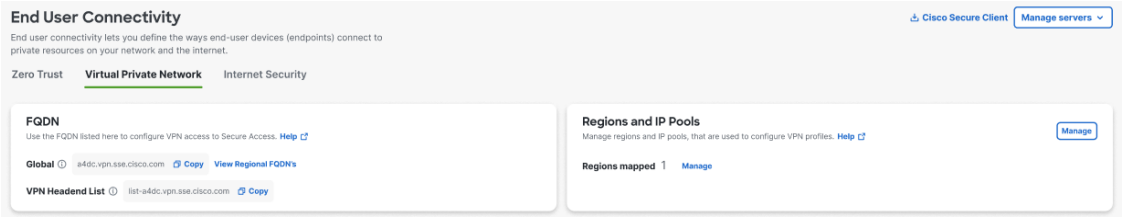
Edit a DNS Server

Provides instructions for completing the Edit a DNS Server workflow in Cisco Secure Access. You can edit the attributes for a DNS server entry.

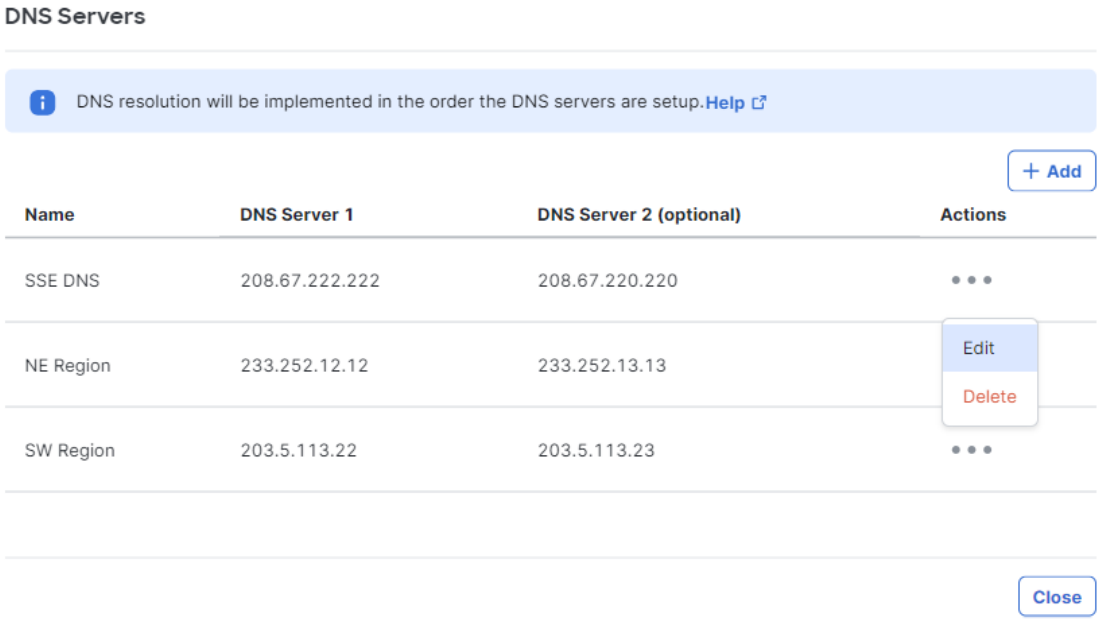
You can edit the attributes for a DNS server entry.

Procedure

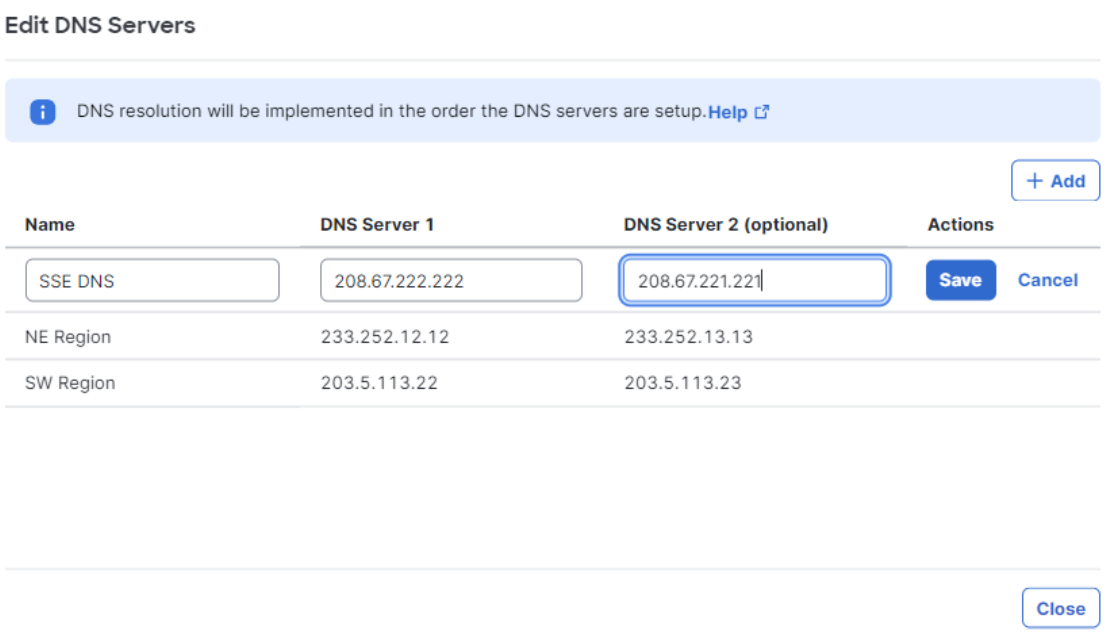
1. Navigate to **Connect** > **End User Connectivity**, click **Manage Servers** and choose **DNS Servers**.



2. Click the ellipsis (...) to **Edit** a DNS server entry.



3. You can modify the label for the DNS server in the **Name** field as well as modify the IP address of the primary and secondary DNS servers as needed for **DNS Server 1** and **DNS Server 2**.



4. Click **Save** and then click **Close**.

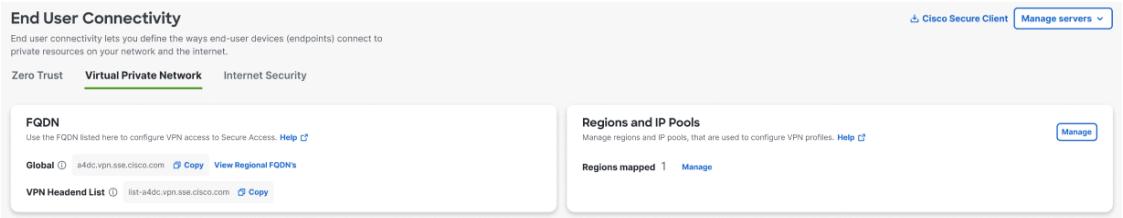
Delete a DNS Server

Provides instructions for completing the Delete a DNS Server workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

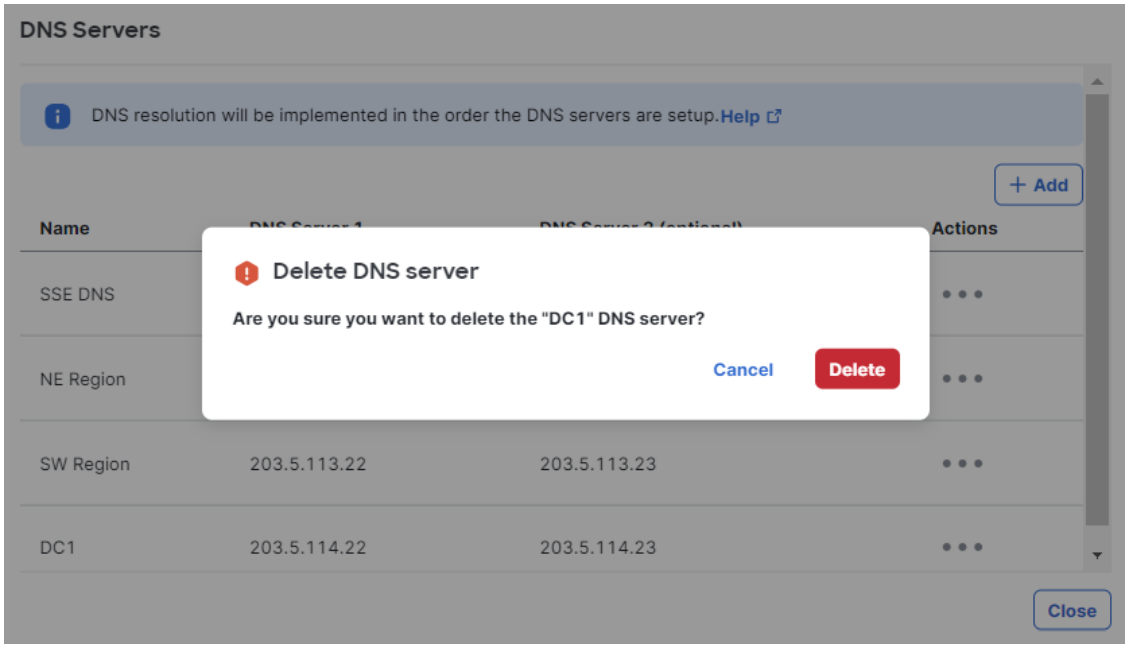
You can delete a DNS server entry.

Procedure

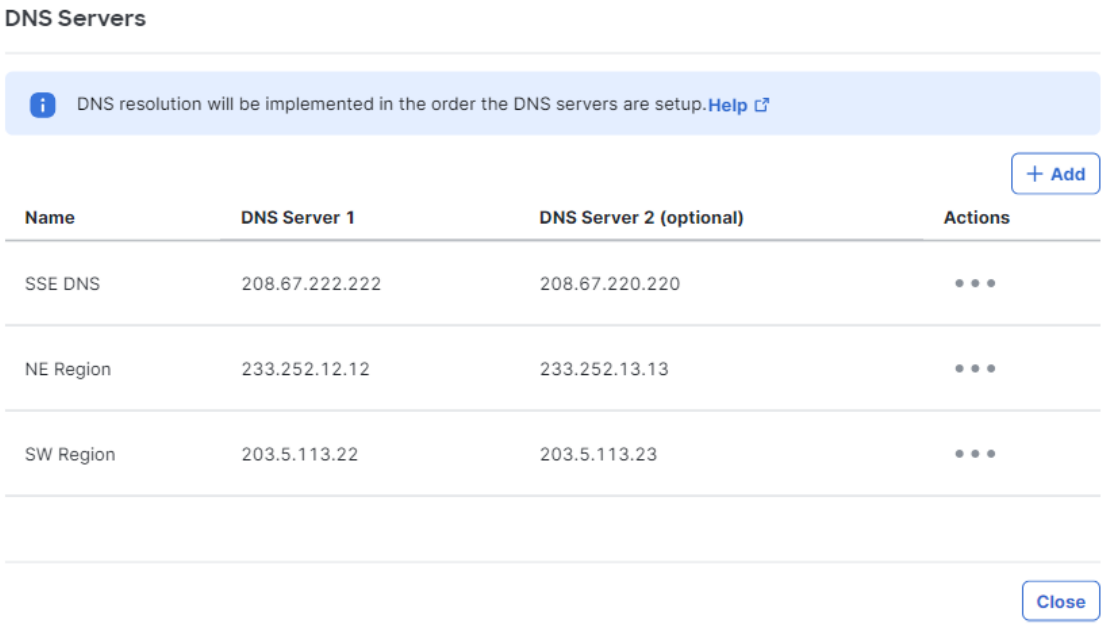
1. Navigate to **Connect** > **End User Connectivity**, click **Manage Servers** and choose **DNS Servers**.



2. Click the ellipsis (...) to **Delete** a DNS server.



3. Review the *Delete DNS server* message and then click **Delete**.
4. Scan the DNS server list to confirm that the DNS server is removed.



5. Click **Close**.

Map DNS Servers to Regions

Understand how to set up a VPN profile to map the DNS servers configured within your network to resolve DNS requests so VPN clients can access network resources when connecting over VPN.

When setting up a VPN profile, you choose the Secure Access region where your data center is located, which determines where the VPN traffic will be routed within the your network. You also choose the DNS servers to resolve DNS requests to internet resources.

Cisco Secure Access allows you to map DNS servers within a VPN profile, essentially directing all your DNS requests through the VPN tunnel to those designated servers, ensuring that your internet traffic is routed through the VPN and utilizing the chosen DNS resolution service.

The following procedure describes how to map DNS servers configured in regions across your Secure Access organization. DNS settings are part of the General settings when setting up VPN profiles, thus this procedure covers only a subset of the VPN profile set up. For more information, see:

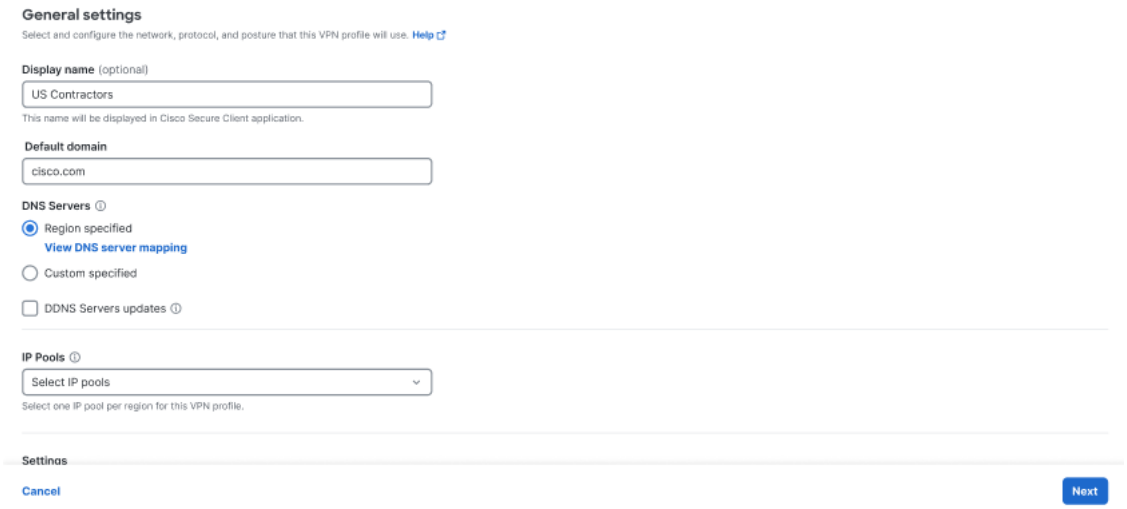
- Add VPN Profiles Step 1 – General Settings for how DNS settings are applied in the VPN profile's general settings.

Before you begin

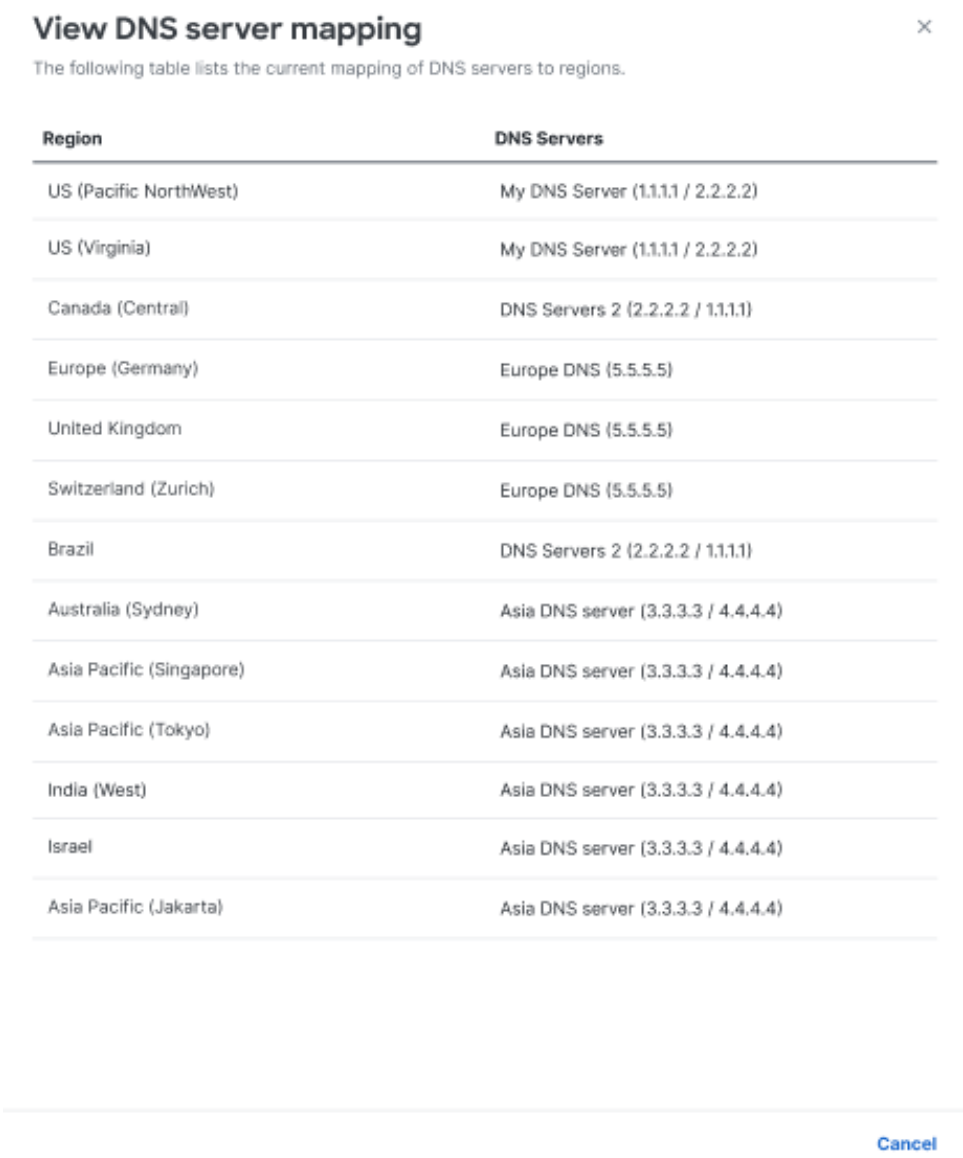
- Full Admin user role. For more information, see Manage Accounts.
- Set up the VPN profile. DNS settings are part of the General settings when setting up VPN profiles. For more information, see Step 1 – General Settings of the VPN profile section.
- When setting up VPN profiles, the **DNS Servers** setting defaults to **Region specified**, meaning that the VPN profile uses the DNS specified for the region. This is the default behavior across all regions.
- (Optional) Change the default to **Custom specified** and map DNS servers to a different server pair for a VPN profile.
- (Optional) Change the default to **Custom specified** selectively for any region, or map all regions to use the same server pair.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **+ VPN Profile**.
3. Enter a meaningful **VPN profile name** for this profile.
4. Enter an optional **Display name** for this profile. This is a customizable and flexible label that is displayed to end-users of the Cisco Secure Client for ease-of-selection when choosing the appropriate profile.
5. Enter the **Default Domain**.
6. Review the **DNS Servers** options.
   a. By default, the **DNS Servers** is set to **Region specified**, meaning that the VPN profile uses the DNS specified for the region.

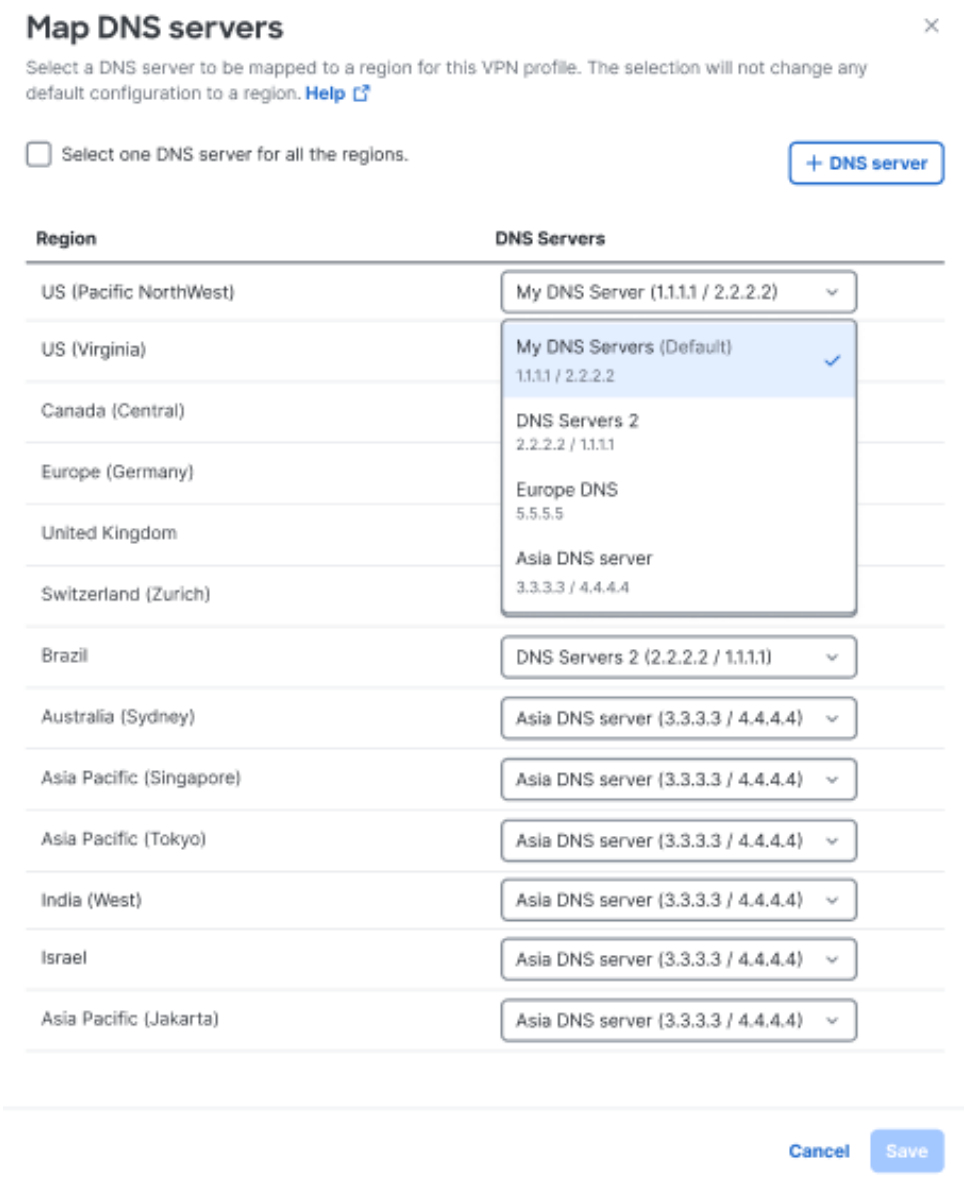


   b. Click **View DNS servers** to see the list of DNS servers mapped to regions.



c. (Optional) To choose a DNS pair other than the default regional DNS, click **Custom specified**, then click **Map DNS servers** to open an configurable view of all available DNS servers for a VPN profile.

d. (Optional) Use the **DNS Servers** drop-downs to map any DNS server changes for a corresponding **Region** . Click **Save** to change the DNS settings, or click **Cancel** to exit.



e. (Optional) To choose one DNS pair for all regions, check **Select one DNS server for all the regions.**

f. (Optional) Select a DNS server pair from the available drop-down list to be applied to all regions. Optionally, click **+ DNS server** to configure a new DNS server option. See Manage DNS Servers for more information.

g. (Optional) Click **Save** to change the DNS settings, or click **Cancel** to exit.

Manage DDNS Servers

Use Dynamic DNS (DDNS) to ensure that changing IP addresses for devices are automatically updated to provide consistent, reliable access to resources.

When end-user devices connect to secure access using the VPNaaS, it is assigned an IP from an IP pool. When the device disconnects and reconnects the VPN, the IP address can change. If the device needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale.

Dynamic DNS (DDNS) provides a mechanism to update DNS RRs whenever the IP address or hostname changes. Add DDNS servers to ensure that changing IP addresses for devices (especially those on dynamic IPs) are automatically updated to provide consistent, reliable access to resources without manual intervention.

When adding these DDNS servers, DDNS Server 1 resolves before DDNS Server 2. Provide DDNS servers that could resolve both IPv4 and IPv6 if applicable. You can also use DDNS for static IP addressing.

Add a DDNS Server Group

Provides instructions for completing the Add a DDNS Server Group workflow in Cisco Secure Access. The following procedure describes how to add a DDNS server group managed by Secure Access.

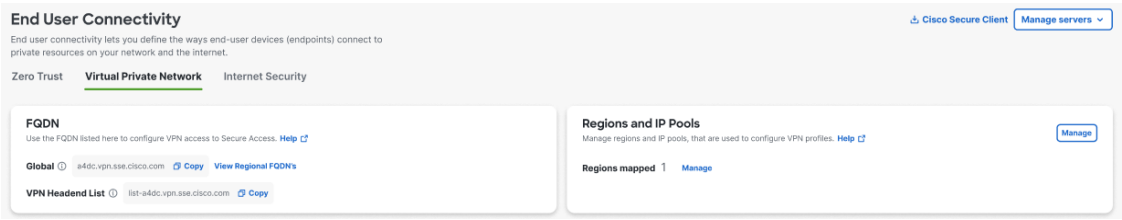
The following procedure describes how to add a DDNS server group managed by Secure Access.

Before you begin

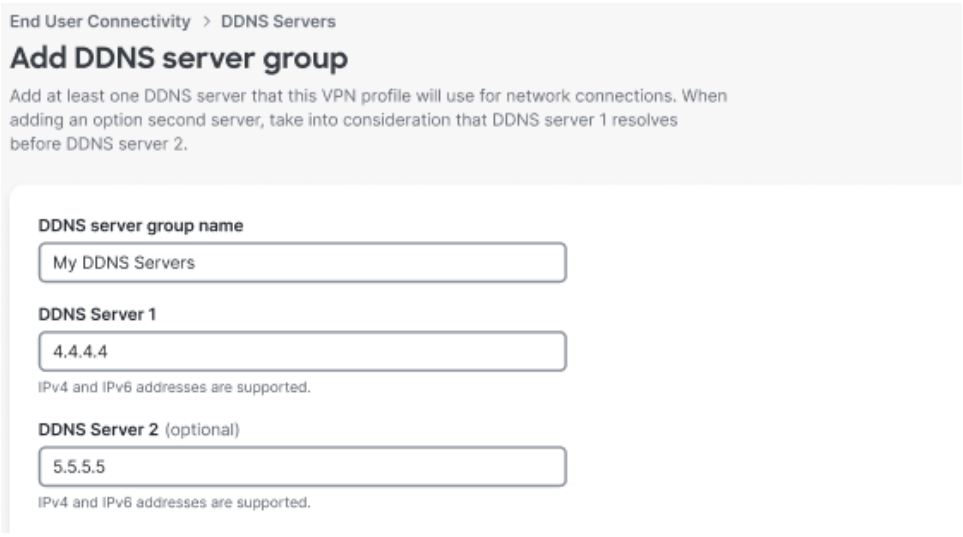
A Full Admin user role is required. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect End User Connectivity** > **Manage Servers** > **DDNS Servers**.

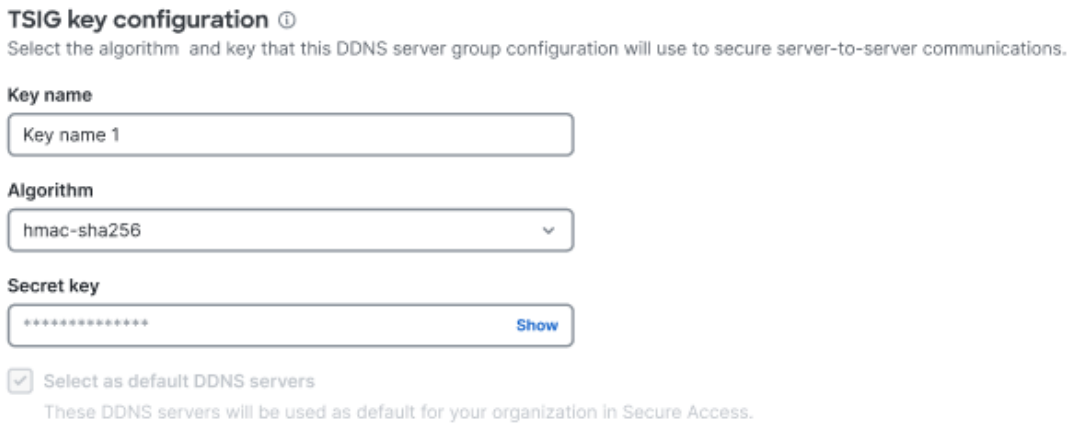


2. Click **+ Add** to configure a new DDNS server.
   a) Input a **DDNS server group name**.
   b) **DDNS Server 1**: Provide the IP address of the primary DDNS server.
   c) **DDNS Server 2** (optional): Provide the IP address of the secondary DDNS server.



> **Note**
>
> DDNS server fields cannot use addresses listed in IP Address Restrictions.

3. **TSIG key configuration**: Select the algorithm and key that the DDNS server group configuration will use to secure server-to-server communications. TSIG (transaction signature) key configuration (defined in RFC 2845) enables the DNS to authenticate updates to a DNS database.
   a) Input a **Key name**.
   b) Select an **Algorithm**.
   c) Input a **Secret key**.



4. Click **Save**.

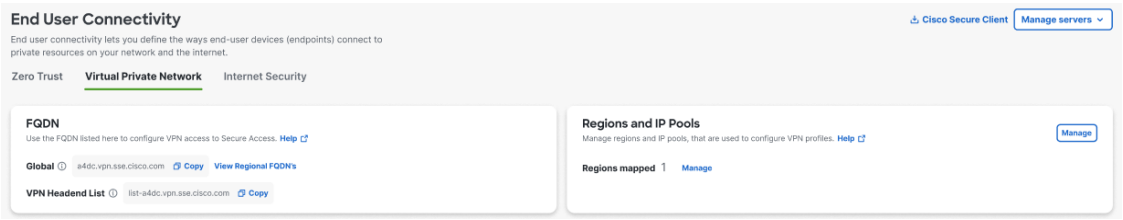
View DDNS Servers

Provides instructions for completing the View DDNS Servers workflow in Cisco Secure Access. You can view the DDNS servers that are configured for your organization.

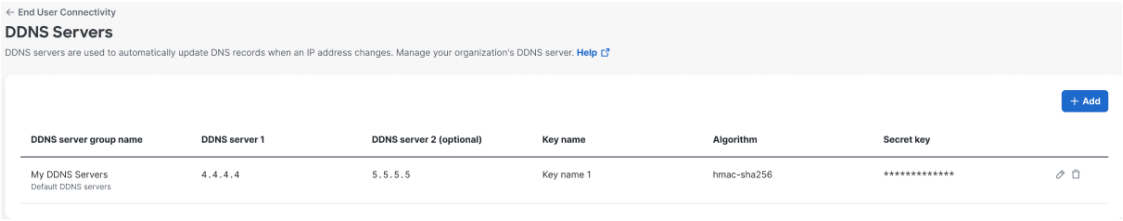
You can view the DDNS servers that are configured for your organization. Your DNS traffic routes through the DDNS servers managed by Secure Access.

Procedure

1. Navigate to **Connect** > **End User Connectivity**, click **Manage Servers** and choose **DDNS Servers**.



2. The list of configured DDNS servers is displayed.



3. From the list you can click **Add** to add a new entry, or click the edit icon to **Edit** or the trash can icon to **Delete** a DDNS server group entry.
4. Click **Close** to dismiss the list.

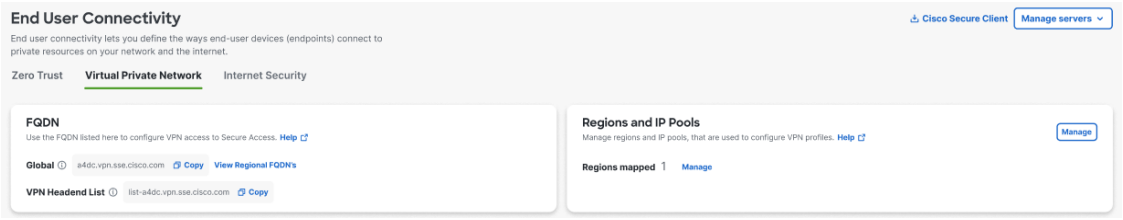
Edit a DDNS Server

Provides instructions for completing the Edit a DDNS Server workflow in Cisco Secure Access. You can edit the attributes for a DDNS server group entry.

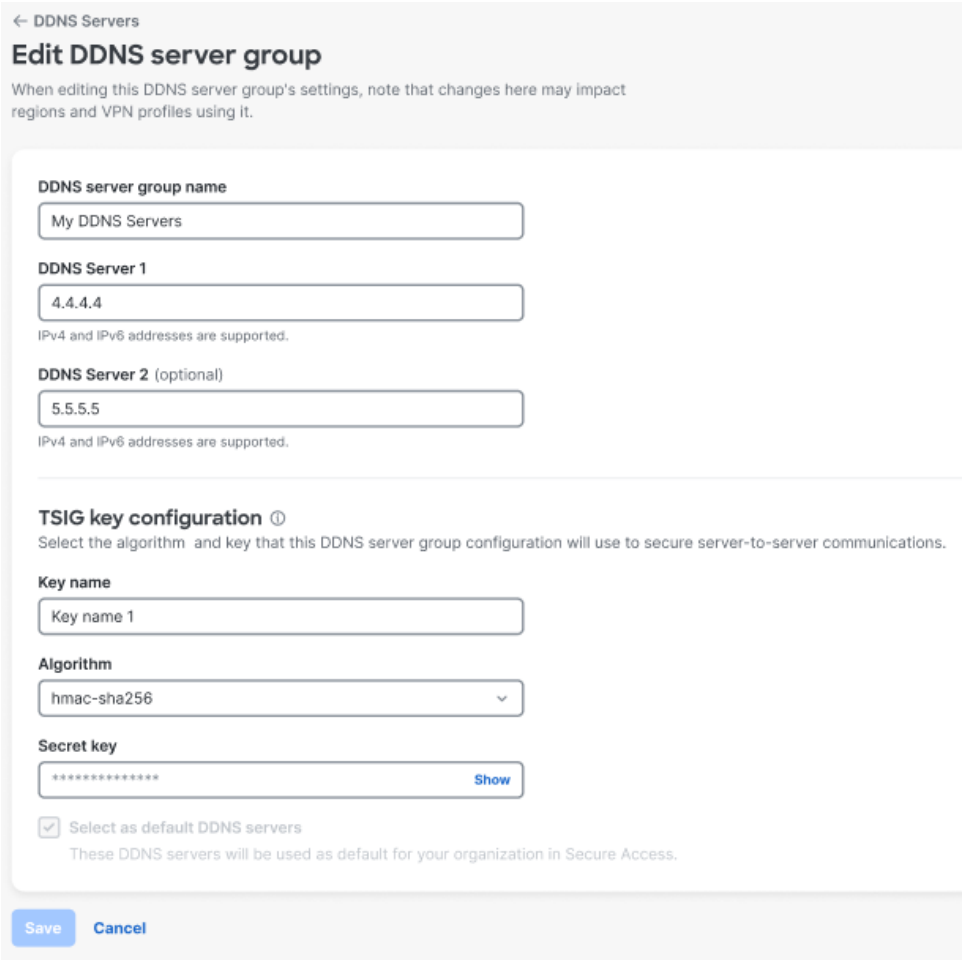
You can edit the attributes for a DDNS server group entry.

Procedure

1. Navigate to **Connect** > **End User Connectivity**, click **Manage Servers** and choose **DDNS Servers**.



2. Click the **Edit** icon for a DDNS server entry.



3. You can modify the label for the DDNS server group in the **DDNS server group name** field as well as modify the IP address of the primary and secondary DDNS servers as needed for **DDNS Server 1** and **DDNS Server 2**.
4. Click **Save**.

Map DDNS Servers to Regions

Understand how to set up a VPN profile to map the DDNS servers configured within your network to resolve DDNS requests so VPN clients can access network resources when connecting over VPN.

When setting up a VPN profile, you choose the Secure Access region where your data center is located, which determines where the VPN traffic will be routed within the your network. You also choose the DNS servers to resolve DNS requests to internet resources. Optionally, you can include DDNS (Dynamic DNS) servers in your VPN profiles to update the mappings of domain names to IP addresses when a remote user's network IP address changes.

Cisco Secure Access allows you to map DNS and DDNS servers within a VPN profile, essentially directing all your DNS requests through the VPN tunnel to those designated servers, ensuring that your internet traffic is routed through the VPN and utilizing the chosen DNS resolution service.

This topic describes how to set up a VPN profile to map the DDNS servers configured within your network to resolve DNS requests and updates so VPN clients can access network resources when connecting over VPN.

The following procedure describes how to map DNS servers configured in regions across your Secure Access organization. DNS settings are part of the General settings when setting up VPN profiles, thus this procedure covers only a subset of the VPN profile set up. For more information, see:

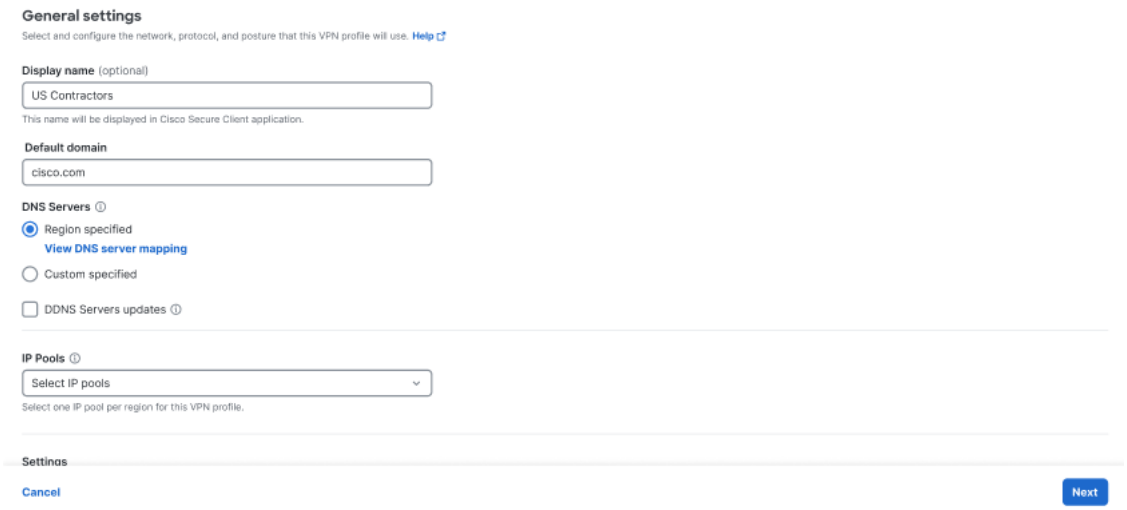
- Add VPN Profiles Step 1 – General Settings for how DNS settings are applied in the VPN profile's general settings.

Before you begin

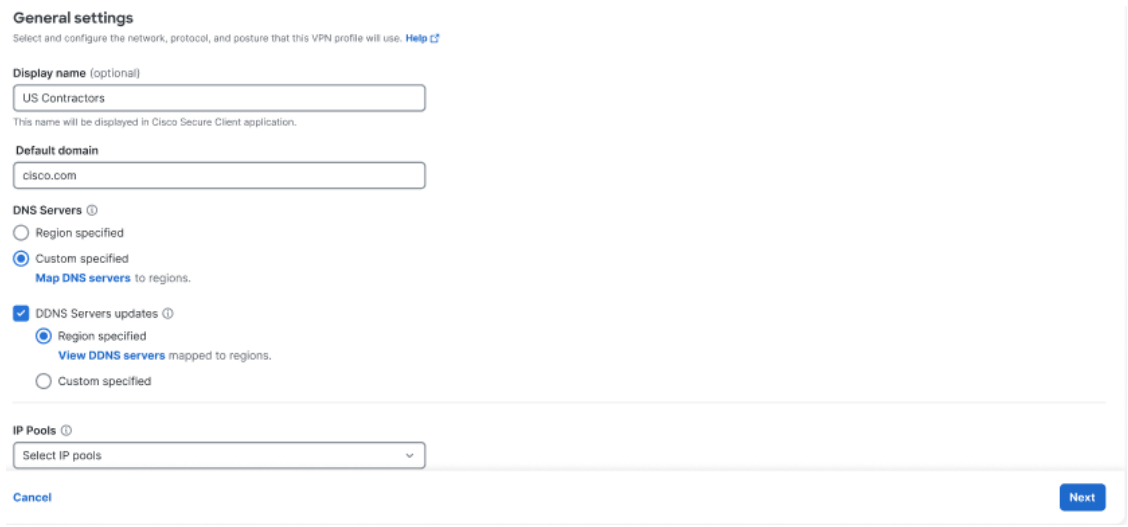
- Full Admin user role. For more information, see Manage Accounts.
- Set up the VPN profile. DNS and DDNS settings are part of the General settings when setting up VPN profiles. For more information, see Step 1 – General Settings of the VPN profile section.
- When setting up VPN profiles, check the **DDNS Servers updates** option to update the mappings of domain names to IP addresses when a remote user's network IP address changes.
- When setting up VPN profiles, the **DDNS Servers** setting defaults to **Region specified**, meaning that the VPN profile uses the DDNS specified for the region. This is the default behavior across all regions.
- (Optional) Change the default to **Custom specified** and map DDNS servers to a different server pair for a VPN profile.
- (Optional) Change the default to **Custom specified** selectively for any region, or map all regions to use the same DDNS server pair.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **+ VPN Profile**.
3. Enter a meaningful **VPN profile name** for this profile.
4. Enter an optional **Display name** for this profile. This is a customizable and flexible label that is displayed to end-users of the Cisco Secure Client for ease-of-selection when choosing the appropriate profile.
5. Enter the **Default Domain**.
6. Review the **DNS Servers** options.
   a. By default, the **DNS Servers** is set to **Region specified**, meaning that the VPN profile uses the DNS specified for the region.



   b. Check **DDNS Servers updates** to include dynamic updates to the mappings of domain names to IP addresses when a remote user's network IP address changes. By default, the **DDNS Servers** is set to **Region specified**, meaning that the VPN profile uses the DDNS specified for the region.

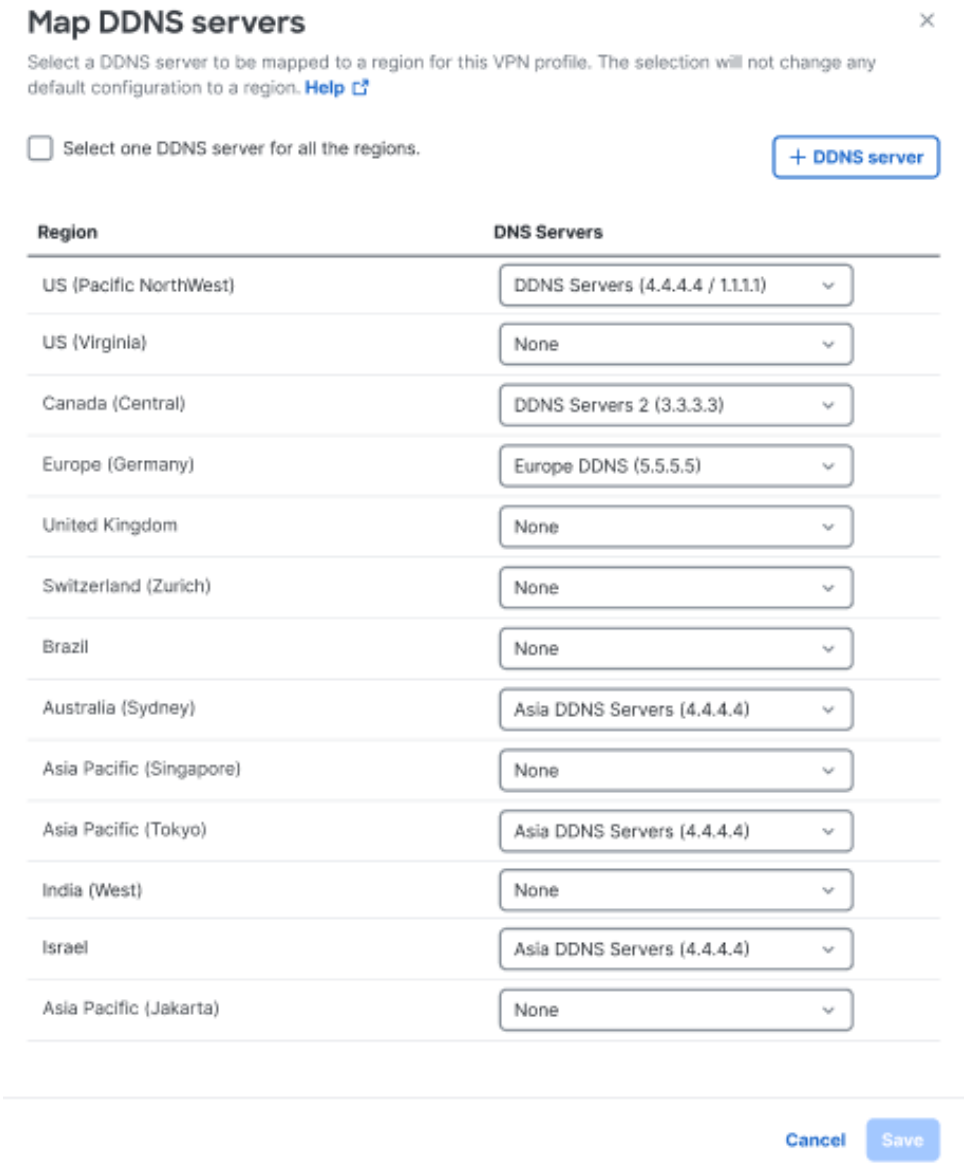


c. Click **View DDNS server mapping** to see the list of DNS servers mapped to regions.



d. (Optional) To choose a DNS pair other than the default regional DNS, click **Custom specified**, then click **Map DDNS servers** to open an configurable view of all available DNS servers for a VPN profile.

e. (Optional) Use the **DDNS Servers** drop-downs to map any DDNS server changes for a corresponding **Region**. Click **Save** to change the DDNS settings, or click **Cancel** to exit.



f. (Optional) To choose one DDNS pair for all regions, check **Select one DDNS server for all the regions.**

g. (Optional) Select a DDNS server pair from the available drop-down list to be applied to all regions. Optionally, click **+ DDNS server** to configure a new DDNS server option. See Manage DNS Servers for more information.



h. (Optional) Click **Save** to change the DDNS settings, or click **Cancel** to exit.

12 Resource Connectors and Connector Groups

Topics:

- Manage Resource Connectors and Connector Groups
- Maintain and Monitor Resource Connectors and Connector Groups
- Schedule Upgrade Windows or Delay for a Connector Group
- Troubleshoot Resource Connectors and Connector Groups

Provides an overview of Resource Connectors and Connector Groups in Cisco Secure Access, including Manage Resource Connectors and Connector Groups and Maintain and Monitor Resource Connectors and Connector Groups. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Resource Connectors and Connector Groups

Resource connectors are lightweight virtual machines installed in your environment that connect traffic from user devices to private resources on your network using zero trust access.

Secure Access resource connectors connect traffic from user devices to private resources on your network using Zero Trust Access.

A resource connector is a lightweight virtual machine that is installed in your environment. We recommend that you deploy resource connectors in groups, for resilience, load balancing, and scalability. Each connector group is associated with a data center, branch office, or security zone, and serves specified private resources in that location. All connectors in a connector group connect traffic to all resources associated with the group.

For additional characteristics of resource connectors and connector groups, see Comparison of Network Connection Methods.

Version Support

You must establish and confirm supported versioning between Secure Access and your third party platforms; whether you use AWS or Azure of VMware, review the Secure Access Resource Connector Release Notes for the latest supported versions, updates, and any relevant enhancements.

Overview: Setting Up Resource Connectors and Connector Groups

1. Define a connector group for each location (data center or network segment such as a branch office or security zone) that has private resources that users need to reach. For more information, see Add Resource Connector Groups.
2. Obtain the resource connector image. You can use the same image for multiple connectors and for connectors in any connector group that uses the same environment. However, always use the most current image version. For more information, see Obtain the Connector Image.
3. Deploy resource connectors in each location associated with a connector group, using a provisioning key that associates each connector with its group.
   - For more information, see Deploy a Connector in AWS.
   - For more information, see Deploy a Connector in Azure.
   - For more information, see Deploy a Connector in VMware.
   - For more information, see Deploy a Connector in Docker.
4. Each deployed connector automatically reaches out to Secure Access after launch; confirm all connectors to ensure that they are legitimate and expected, and to make them ready to connect traffic. For more information, see Add Connectors to a Connector Group.
5. Assign each private resource to a connector group whose connectors are deployed in the same data center, branch office, or security zone as the resource. For more information, see Assign Private Resources to a Connector Group.
6. Test your connectors by accessing a private resource that is enabled for zero trust access from a remote user endpoint device that has Cisco Secure Client and is enrolled for zero trust access.
7. As needed, at any time, add more connectors to provide additional throughput capacity. For more information, see Add Connectors to a Connector Group.
8. As needed, associate additional and newly added private resources to the connector group. For more information, see Assign Private Resources to a Connector Group.

Requirements and Prerequisites for Resource Connectors and Connector Groups

Describes Requirements and Prerequisites for Resource Connectors and Connector Groups in Cisco Secure Access. This guide describes the requirements, prerequisites, and guidelines for deploying resource connectors and connector groups.

This guide describes the requirements, prerequisites, and guidelines for deploying resource connectors and connector groups.

- Guidelines for Connector Groups
- Requirements and Guidelines for Connectors
- Connectivity Requirements
- Capacity Requirements

Guidelines for Connector Groups

Describes Guidelines for Connector Groups in Cisco Secure Access. Generally, we recommend that you deploy one resource connector group for each data center, branch office, or security zone that contains private resources that remote users must reach.

- Generally, we recommend that you deploy one resource connector group for each data center, branch office, or security zone that contains private resources that remote users must reach.
- A single location can have multiple connector groups that send traffic to discrete sets of resources.
- A single connector group that sends traffic to resources in multiple locations is not recommended.
- For configuration guidelines for resource connector groups for private resources residing in multiple locations, see Private Resource Configuration Examples.

When adding connectors to a group:

- Deploy all connectors in a group in the same environment, for example AWS, Microsoft Azure, or VMware.
- For accurate load balancing, the instance type for all connectors in a group must be identical.
- Each connector in a connector group must be able to reach all of the private resources assigned to the connector group.

Connector Group Region

When you create a connector group, choose a Secure Access region that is as close as possible to the location where the private resources that will be associated with the group reside.

Choose the region for your connector groups carefully. You cannot change the region associated with a connector group.

If you need to change the region, you must create a new connector group associated with the new region. Then, deploy connectors in that group and delete the original connector group and its connectors.

Redundancy Across Connector Groups

To provide redundancy across connector groups, deploy multiple connector groups, each associated with the same private resources.

To provide redundancy across regions, associate each redundant connector group with a different region.

After you configure redundancy, Secure Access directs incoming zero trust access user requests to the nearest region that has a connector group associated with that resource.

Requirements and Guidelines for Connectors

Describes Requirements and Guidelines for Connectors in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Supported platforms for connectors: AWS, Microsoft Azure, VMware ESXi, Docker Container.

  - For information about deploying connectors in AWS, see Deploy a Connector in AWS.
  - For information about deploying connectors in Microsoft Azure, see Deploy a Connector in Azure.
  - For information about deploying connectors in VMware, see Deploy a Connector in VMware.
  - For information about deploying connectors in a Docker container, see Deploy a Connector in Docker.
- Connector IP addresses:
  - Connectors support IPv4 addresses. IPv6 is not supported.
  - You cannot use any address reserved for use by Secure Access. For information about addresses reserved for Resource Connectors, see Network Requirements for Secure Access.
  - For maximum connector throughput capacity, DTLS and TLS connections must originate from the same IP address. If the originating IP addresses are different, TLS connections will be used, with a significant reduction in throughput.
- For maximum connector throughput capacity, DTLS is required. Connections are downgraded to TLS if the originating IP addresses for the connections to Secure Access are different or UDP connections are blocked.
- Deploy connectors in the same data center, branch office, or security zone location as the private resources to which they will send traffic.
- Each connector in a connector group must be able to reach all of the private resources assigned to the connector group.
- All connectors must be able to reach the Secure Access cloud. For more information, see Connectivity Requirements.
- Connectors support only a single network interface.

Connectivity Requirements

Describes Connectivity Requirements in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Ensure that Resource connectors can reach the Secure Access destinations. For more information, see Allow Resource Connector Traffic to Secure Access.
- Public-facing IP addresses are not needed.

Capacity Requirements

Describes Capacity Requirements in Cisco Secure Access. The number of connectors that you deploy within a connector group depends on the volume of traffic that you expect.

The number of connectors that you deploy within a connector group depends on the volume of traffic that you expect.

- Estimate the maximum expected volume of traffic to the resources in the data center, branch office, or security zone.
- When you add a connector group, Secure Access suggests a suitable number of connectors to deploy based on the estimated traffic volume you provide. The recommended number of connectors assumes the recommended instance type, 75% CPU usage, and DTLS connectivity, and includes a connector instance for redundancy.
- For connectors that have the recommend instance type, throughput using DTLS is 500 mbps fully loaded (400 at the recommended 75% load). Throughput using TLS is 250 mpbs. If your actual capacity is less than expected, see Troubleshoot Resource Connectors and Connector Groups.
- To determine the number of connectors needed for an existing connector group, see Determine the Number of Connectors Needed in a Connector Group.
- For redundancy, (for example, to avoid service interruptions during connector upgrades), you should deploy at least two connectors in each group.
- For the maximum number of connectors and connector groups per organization, see Limitations and Range Limits.
  - You can deploy up to the maximum number of connectors in a group for load balancing and scalability.
  - You can associate up to the maximum number of connector groups with any region.
  - If you require greater capacity, contact your Cisco representative.

- Your network must be able to support the traffic volume that you specify.

Allow Resource Connector Traffic to Secure Access

Describes Allow Resource Connector Traffic to Secure Access. Your firewall must allow the organization's resource connectors to reach the destinations that are listed on this page.

Your firewall must allow the organization's resource connectors to reach the destinations that are listed on this page. All connections are outbound from your network.

Region-Specific Destinations

Describes Region-Specific Destinations in Cisco Secure Access. Allow traffic to the applicable regional destination FQDNs or addresses on UDP/443 (DTLS) and TCP/443 (TLS).

Allow traffic to the applicable regional destination FQDNs or addresses on **UDP/443 (DTLS)** and **TCP/443 (TLS)**.

Continent	Region	FQDN	Resolves To
Africa	Africa (South Africa)	*.afs1.acgw.sse.cisco.com	151.186.161.0/24
Asia	Asia Pacific (Hong Kong)	*.ape1.acgw.sse.cisco.com	151.186.169.0/24
	Asia Pacific (Jakarta)	*.apse3.acgw.sse.cisco.com	151.186.205.0/24
	Asia Pacific (Osaka)	*.apne3.acgw.sse.cisco.com	151.186.170.0/24
			151.186.121.0/24
	Asia Pacific (Singapore)	*.apse1.acgw.sse.cisco.com	151.186.195.0/24
	Asia Pacific (Seoul)	*.apne2.acgw.sse.cisco.com	163.129.130.0/24
	Asia Pacific (Tokyo)	*.apne1.acgw.sse.cisco.com	151.186.193.0/24
			151.186.117.0/24
	India (South)	*.aps2.acgw.sse.cisco.com	151.186.166.0/24
	India (West)	*.aps1.acgw.sse.cisco.com	151.186.194.0/24
			163.129.198.0/24
			163.129.194.0/24
	Israel (Tel Aviv)	*.ilc1.acgw.sse.cisco.com	151.186.203.0/24
	Middle East (Saudi Arabia)	*.mec2.acgw.sse.cisco.com	151.186.109.0/24
			151.186.126.0/24
	Middle East (UAE)	*.mec1.acgw.sse.cisco.com	151.186.171.0/24
Australia	Sydney	*.apse2.acgw.sse.cisco.com	151.186.196.0/24
Europe	Germany	*.euc1.acgw.sse.cisco.com	151.186.197.0/24
	Milan	*.eus1.acgw.sse.cisco.com	163.129.129.0/24
	France (Paris)	*.euw3.acgw.sse.cisco.com	151.186.164.0/24
	Spain	*.eus2.acgw.sse.cisco.com	151.186.163.0/24
	Stockholm	*.eun1.acgw.sse.cisco.com	151.186.162.0/24

Continent	Region	FQDN	Resolves To
	Switzerland (Zurich)	*.euc2.acgw.sse.cisco.com	151.186.207.0/24
	United Kingdom	*.euw2.acgw.sse.cisco.com	151.186.198.0/24
			163.129.222.0/24
			163.129.234.0/24
North America	Canada (Central)	*.cac1.acgw.sse.cisco.com	151.186.206.0/24
	Canada (West)	*.caw1.acgw.sse.cisco.com	151.186.167.0/24
	LATAM (Mexico)	*.mxc1.acgw.sse.cisco.com	163.129.128.0/24
	US (Central)	*.usc1.acgw.sse.cisco.com	163.129.226.0/24
			163.129.203.0/24
	US (Midwest)	*.use2.acgw.sse.cisco.com	151.186.160.0/24
	US (Pacific Northwest)	*.usw2.acgw.sse.cisco.com	151.186.192.0/24
	US (Virginia)	*.use1.acgw.sse.cisco.com	151.186.199.0/24
South America	Brazil	*.sae1.acgw.sse.cisco.com	151.186.168.0/24

Destinations For All Regions

Describes Destinations For All Regions in Cisco Secure Access. Resource Connectors need access to regional Fully Qualified Domain Name (FQDN) destinations because they establish secure outbound connections to the nearest regional Secure Access data center's resource connector gateway.

Cisco Secure Access Requirements

Resource Connectors need access to regional Fully Qualified Domain Name (FQDN) destinations because they establish secure outbound connections to the nearest regional Secure Access data center's resource connector gateway. Resource Connectors are deployed in groups within the same region as the private resources they serve.

Allow outbound traffic to the destinations that apply to your Resource Connector deployment method. Destinations marked with an asterisk (*) are required only for the setup-script deployment method.

Table 13: Required Resource Connector Destinations by Deployment Method

FQDN	Resolves To	Port and Protocol
us.repo.acgw.sse.cisco.com	**44.219.201.178 3.216.0.64 52.25.242.148 52.43.27.33**	TCP/443
me.repo.acgw.sse.cisco.com	**51.17.119.174 51.16.220.207 157.241.89.41 15.184.106.65**	TCP/443
eu.repo.acgw.sse.cisco.com	**3.69.139.181 3.65.114.4 13.43.63.69 18.132.151.163**	TCP/443
ap.repo.acgw.sse.cisco.com	**13.114.55.164 57.181.78.26 52.64.179.81 52.65.178.47**	TCP/443
us.controller.acgw.sse.cisco.com	**54.188.111.4 35.165.184.17 54.152.122.37 3.211.159.37**	TCP/443

FQDN	Resolves To	Port and Protocol
eu.controller.acgw.sse.cisco.com	**35.156.127.26 52.57.119.242 18.135.181.212 18.135.254.39**	TCP/443
ap.controller.acgw.sse.cisco.com	**3.105.121.195 13.211.184.71 54.199.90.120 18.178.227.126**	TCP/443
api.sse.cisco.com	**146.112.59.20**	TCP/443
prod.acme.sse.cisco.com		TCP/443
ssepki.cryptosvcs.cisco.com		TCP/80
ssepki-prd.pureca.cryptosvcs.cisco.com	**52.200.248.37 3.225.142.190 3.218.255.115**	TCP/80
index.docker.io*		TCP/443
docker.io*		TCP/443
auth.docker.io*		TCP/443
cdn.auth0.com*		TCP/443
login.docker.com*		TCP/443
hub.docker.com*		TCP/443
registry-1.docker.io*		TCP/443
production.cloudflare.docker.com*		TCP/443
docker-images-prodr2.cloudflarestorage.com*		TCP/443
tuf-repo-cdn.sigstore.dev*		TCP/443

FQDN	Resolves To	Port and Protocol
github.com*		TCP/443
release-assets.githubusercontent.com*		TCP/443
208.67.222.222	208.67.222.222	TCP/53 , UDP/53

Note

Required only to allow resolution of **github.com** during setup and deployment of the resource connector in the Docker container.

Note

Required only to allow resolution of **release-assets.githubusercontent.com** during setup and deployment of the resource connector in the Docker container.

Note

The Resource Connector uses the Cisco OpenDNS resolver (208.67.222.222) as a fallback mechanism. This is optional and is only utilized if your configured DNS server becomes non-functional. If you do not wish to use this fallback, it is not required for standard operations.

Note

***** Required only when deploying the Resource Connector by using the Connector Docker Image setup-script method. If you deploy from the signed package obtained through **Download Connector Image for Docker**, you do not need to add these destinations to the Connector host's allow list.

Note

Ubuntu repository endpoints may resolve to additional regional mirrors; for example, ubuntu-mirror-*.canonical.com or other Canonical infrastructure. These endpoints are dynamic and may vary by region. Firewall policies should account for this behavior.

Docker RC Requirements

Docker RC refers to running a resource connector as a docker container, which allows the resource connector to be launched and managed within a docker environment. This provides flexibility and ease of deployment across various infrastructures.

Resource Connectors access outbound destinations by resolving destination FQDNs (Fully Qualified Domain Names) via configured DNS servers. The connector then forwards traffic to the resolved IP addresses of private resources. Allowing outbound access to the following Ubuntu-specific destinations is necessary for OS package repositories during the installation process and acquiring lists of known domains.

Note

Docker RC environments do not support fully restricted egress unless internal package mirrors are provided. In restricted environments, internal mirrors must be used to replace external Ubuntu repositories required for installation and updates.

Allow outbound access to the following destinations for Docker RC environments:

FQDN	Resolves to	Port and Protocol
esm.ubuntu.com		TCP/443
us.archive.ubuntu.com		TCP/80
archive.ubuntu.com		TCP/80
security.ubuntu.com		TCP/80
ubuntu-mirror-1.ps6.canonical.com		TCP/80
ubuntu-mirror-2.ps6.canonical.com		TCP/80
ubuntu-mirror-3.ps6.canonical.com		TCP/80
ubuntu-mirror-1.ps5.canonical.com		TCP/80
ubuntu-mirror-2.ps5.canonical.com		TCP/80
ubuntu-mirror-3.ps5.canonical.com		TCP/80

Add Resource Connector Groups

Provides instructions for completing the Add Resource Connector Groups workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

We recommend that you deploy resource connectors in groups, for scalability, load balancing, and redundancy. Each connector group is associated with a set of private resources in a particular data center, branch office, or security zone, and any connector in the group can connect traffic to any private resource in the group.

First, add a resource connector group. Then deploy the associated resource connectors using the provisioning key that is generated when you create the connector group.

Secure Access uses the default DNS server that you configured during connector deployment to resolve destinations for private resources. If the private resources in your organization are on various domains and the destinations are resolved by different DNS servers, you can specify these domains and DNS servers for the connector group in Secure Access.

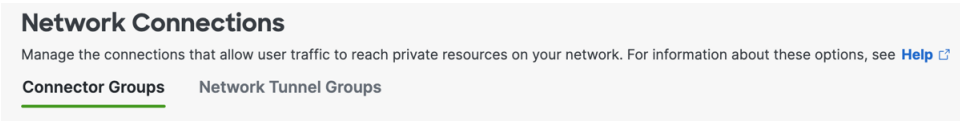
Configure the properties of the Connector Group and optionally add DNS Servers and domains to resolve traffic for private resources.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Meet the requirements to deploy resource connectors. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.
- Determine the volume of traffic your connector group must accommodate. For more information, see Determine the Number of Connectors Needed in a Connector Group.
- (Optional) To add domains and DNS servers for a connector group, you must deploy the resource connectors in the connector group with Cisco Secure Access Connector software image version **2.0.33-xxxxx** or newer.

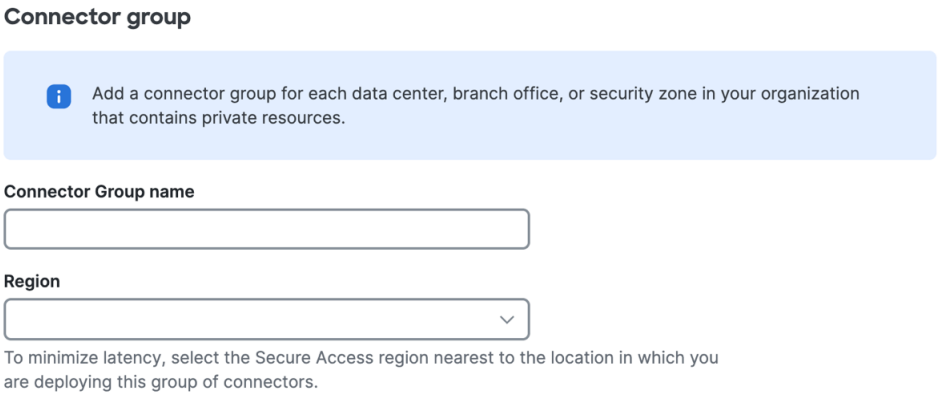
Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.



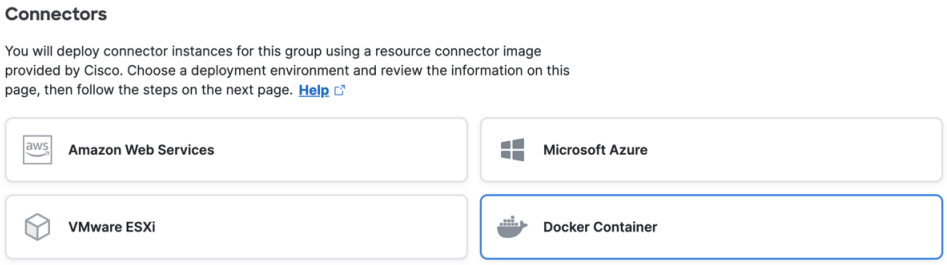
2. Click **Add a Connector Group**.
3. For **Connector group**, enter a name for the connector group and choose a **Region**.

   We recommend that you indicate the data center, branch office, or security zone location in the name. Choose the **Region** (Secure Access cloud instance) closest to the data center location where you are creating this connector group. Choose the region carefully. You cannot change this later.



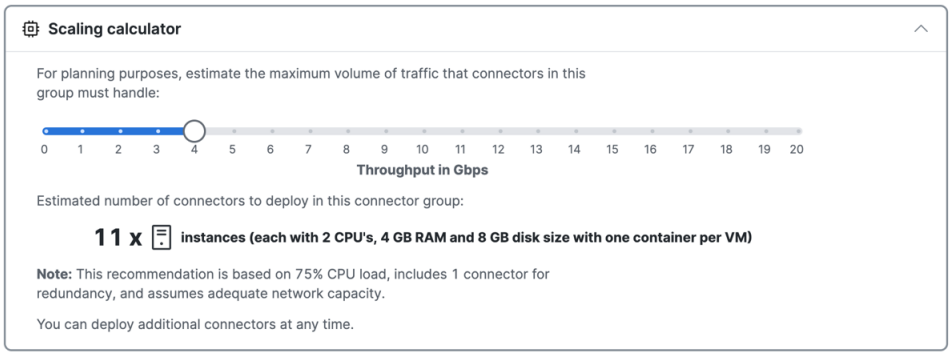
4. Click **Next**.
5. For **Connectors**, select the environment where you will deploy the resource connectors.

This section provides the information about the capacity of the connectors in the group. We recommend that you make a note of the number of connectors that Secure Access recommends.



a) To determine the number of connectors to deploy in this group, choose the estimated maximum throughput capacity that the connectors in the group must handle.

The estimated number of connectors that Secure Access recommends includes instances required for redundancy. For more information, see connector and capacity requirements in Requirements and Prerequisites for Resource Connectors and Connector Groups.

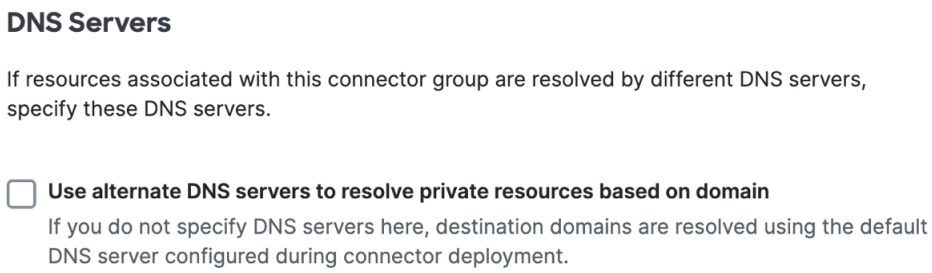


b) Click **Next**.

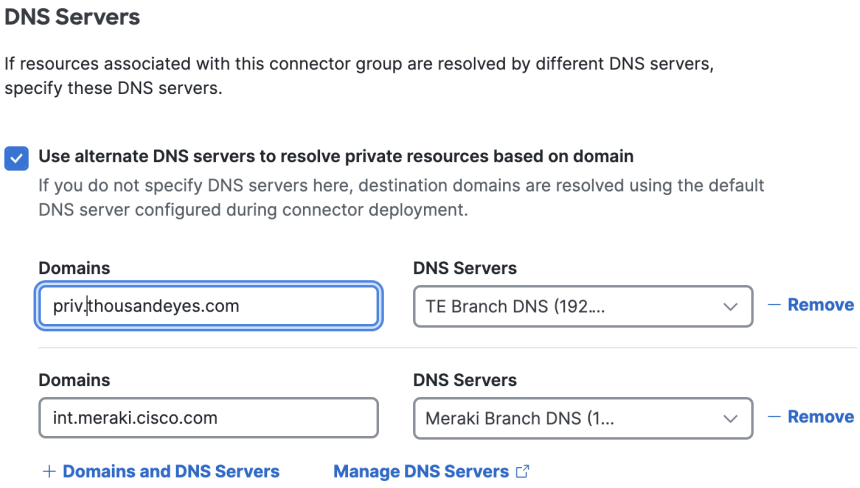
6. For **DNS Servers**, check **Use alternate DNS servers to resolve private resources based on domain**.
   - You can add up to five DNS servers and domains with a total of 50 unique domains.
     - For each addition, you can select the same DNS Server but add unique domains only.
   - When you select a DNS server, Secure Access adds the primary DNS server and if configured, the secondary DNS server.
   - You can add a maximum of ten unique domains with a DNS server. When you add multiple domains, separate the domains with a comma.
   - You must add at least one domain with a DNS server.
   - Secure Access does not support wildcards with domains.
   - Secure Access supports valid domains only.

Resource connectors do not support multicast DNS (mDNS) and the use of `nslookup` to resolve internal domains configured with ***.local**.

If a DNS server associated with a resource connector has DNS entries configured with ***.local**, the resource connector is unable to resolve these local domains. DNS resolution of local domains with the ***.local** extension rely on mDNS.



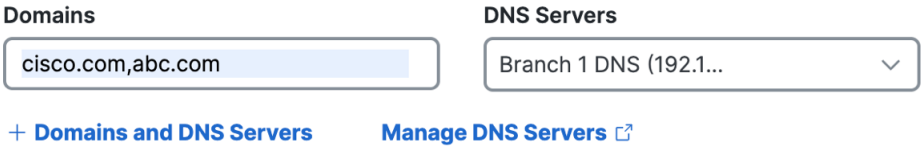
a) For **Domains**, enter a single domain or a comma-separated list of domains.



b) For **DNS Servers**, select a configured DNS server.

The selected DNS servers includes the primary DNS server and if available, the secondary DNS server. For more information, see Manage DNS Servers.

c) (Optional) To add more domains and DNS servers, click **+Domains and DNS Servers**,



7. Click **Save**.

What to do next

1. Deploy connectors for the group. For more information, see Add Connectors to a Connector Group.
2. Assign private resources to the group. For more information, see Assign Private Resources to a Connector Group.

Add Connectors to a Connector Group

Describes Add Connectors to a Connector Group in Cisco Secure Access. A resource connector is associated with a connector group.

A resource connector is associated with a connector group. A connector group helps manage the connectors in your cloud environments.

You can use the pre-configured connector images to deploy resource connectors in your data centers. During deployment, associate each connector with a group using the connector group's provisioning key.

If you need additional throughput capacity to handle the volume of traffic that a connector group must handle, add connectors to the group. You can add resource connectors to a group at any time.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Meet the requirements for connectors. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.
- Add a connector group for traffic to the data center, branch office, or security zone. For more information, see Add Resource Connector Groups.
- Determine the number of resource connectors to deploy in the group.
  - For more information, see Capacity Requirements.
  - For more information, see Determine the Number of Connectors Needed in a Connector Group.

Procedure

- Step 1 - Deploy Secure Access Resource Connectors
- Step 2 - Confirm Connectors
- Step 3 - Assign Private Resources to Connector Groups

Step 1 – Deploy Secure Access Resource Connectors

Provides instructions for completing the Step 1 - Deploy Secure Access Resource Connectors workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Obtain the connector image. For more information, see Obtain the Connector Image. You can download the image once, then use it for multiple connectors in multiple groups.

   All connectors in a group must use the same environment, for example AWS, Microsoft Azure, or VMware. However, before deploying, ensure that you have the latest image version.

2. Copy the provisioning key for the connector group where you are deploying connectors. You must have this key when deploying connector instances. For more information, see Provisioning Keys for Resource Connectors.
3. Deploy connector instances in your environment.
   - For information about VMware, see Deploy a Connector in VMware
   - For information about AWS, see Deploy a Connector in AWS.
   - For information about Microsoft Azure, see Deploy a Connector in Azure.
   - For more information, see Deploy a Connector in Docker.

Step 2 – Confirm Connectors

Provides instructions for completing the Step 2 – Confirm Connectors workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After the resource connector instances launch, they automatically connect to Secure Access.

Before you can use the resource connectors, you must confirm the resource connectors in Secure Access, which validates that the connector is legitimate.

A resource connector that has not been confirmed in Secure Access is either in the **announced** or **reachable** state. You can use the Secure Access Resource Connector and Connector Groups API to view the status of a resource connector in the **announced** or **reachable** state.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. In Secure Access, navigate to **Connect** > **Network Connections**, and then click **Connector Groups**.
2. Expand **Confirm Connectors**.

   If necessary, wait up to 15 minutes for deployed connectors to launch and communicate to Secure Access.
3. Review the list of deployed connectors to ensure that all are expected and valid.

   The **Origin IP Address** of the connector may indicate where the connector is located, which helps determine if the connector is valid.

   If there are connectors in the list that you are unsure about, you can revoke or disable them.

   - You can confirm connectors that are disabled. Disabled connectors remain in the inactive state.
   - You can not confirm revoked connectors. Revoking a connector invalidates the current provisioning key and generates a new key. You will need to use the new key for subsequent connectors that you deploy. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.
4. To confirm all connectors in the list, click **Confirm Connectors**.

Step 3 – Assign Private Resources to Connector Group

Describes Step 3 – Assign Private Resources to Connector Group in Cisco Secure Access. Connectors send user traffic to the private resources assigned to the connector group, which the connectors belong to.

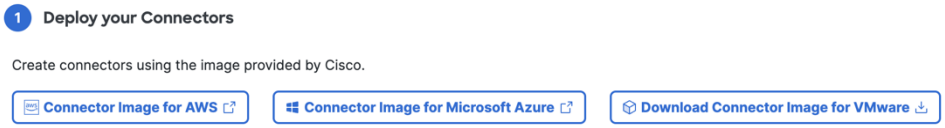
Connectors send user traffic to the private resources assigned to the connector group, which the connectors belong to. For more information, see Assign Private Resources to a Connector Group.

If you see issues with a newly deployed connector, see Connector diagnostics (CLI) and Connector Troubleshooting Tools.

Obtain the Connector Image

Describes Obtain the Connector Image in Cisco Secure Access. The Cisco Secure Access Resource Connector images are available to download.

The Cisco Secure Access Resource Connector images are available to download. On Secure Access, you can download the VMware resource connector image, or follow the marketplace links for Microsoft Azure or AWS to the connector virtual machine images.



A connector image is not specific to any connector group. You can download a connector image once and use it for any number of connectors in any connector group.

Requirements

- Before using a previous download, always verify that your downloaded version is the latest version.
- All connectors in a group must be deployed in the same environment, for example: AWS, Azure, or VMware.

Get the Connector Image for AWS

Provides instructions for completing the Get the Connector Image for AWS workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Get the Secure Access Resource Connector image for AWS.

For more information, see Get the Connector Image on the AWS Marketplace.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.
2. Click **Connector Image for AWS** to follow the link to the AWS Marketplace, or in your browser, navigate to the AWS Marketplace at `https://aws.amazon.com/marketplace/pp/prodview-oonzvpdnti7jm`.

   Follow the steps to download the image.

Get the Connector Image for Microsoft Azure

Provides instructions for completing the Get the Connector Image for Microsoft Azure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Get the Secure Access Resource Connector image for Azure.

For more information, see Get the Connector Image on the Microsoft Azure Marketplace.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.
2. Click **Connector Image for Microsoft Azure**.

Follow the link to the Microsoft Azure Marketplace, or in your browser, navigate to the Microsoft Azure Marketplace at **https://portal.azure.com/#view/Microsoft_Azure_Marketplace/GalleryItemDetailsBlade/id/cisco.cisco-resource-connector**.

Download the Connector Image for VMware

Provides instructions for completing the Download the Connector Image for VMware workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Get the Secure Access Resource Connector image for VMware.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.
2. If you see a **Next Steps** section at the top of the page, click **Deploy Your Connectors**.
   a) Check the Environment column in the table to ensure that you download the correct image for the connector group.
   b) Click **Download Connector Image for VMware**.
3. If you do not see a **Next Steps** section, or if no connector groups are listed under **Deploy Your Connectors**, scroll down to the **Connector Groups** section.
   a) Click the ellipsis button at the end of any connector group and choose **View Provisioning Key**.



   b) Click **Download Connector Image for VMware**.
   c) (Optional) If you need the provisioning key for this connector group now, copy the provisioning key.

   For more information, see Provisioning Keys for Resource Connectors.

Get the Connector Image for Docker

Provides instructions for completing the Get the Connector Image for Docker workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Get the Secure Access Resource Connector image for Docker.

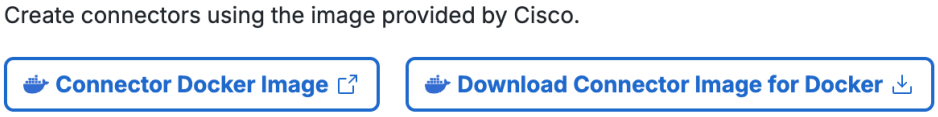
For more information, see Deploy a Connector in Docker.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.
2. Navigate to **Next Steps** > **Deploy your Connectors**.



3. Choose how you want to obtain and deploy the Connector image:
   - Click **connector Docker Image** to use the existing setup-script deployment method. This method downloads the container image from DockerHub.

     If you selected Connector Docker Image, follow *Set Up the Resource Connector and Container*.
   - Click **Download Connector Image for Docker** to download the signed resource-connector-v<VERSION>.tar.gz package directly from Cisco Secure Access. This method does not require DockerHub access.

     If you selected **Download Connector Image for Docker**, follow *Deploy from a Directly Downloaded Connector Image* and begin with *Extract the Connector image package.*

Provisioning Keys for Resource Connectors

Describes Provisioning Keys for Resource Connectors in Cisco Secure Access and explains Important Information about Provisioning Keys. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

A connector group has a provisioning key. A provisioning key associates each connector with a connector group. When you deploy a connector in your environment, you must specify the provisioning key for the connector group where the connector belongs.

Important Information about Provisioning Keys

- When you create a connector group, a provisioning key is automatically generated for the group.
- Provisioning keys are used only when deploying a new connector.
- Provisioning keys expire after 14 days.
  - This expiration does not affect existing deployed connectors.
  - You cannot use an expired key to create a new connector. Instead, generate a new provisioning key using the **Regenerate** button. Regenerating a provisioning key does not affect existing connectors. For more information, see Add Connectors to a Connector Group.
- If you want to prevent a key from being used to create additional connectors, for example if you suspect that a bad actor has somehow obtained the key, regenerate the key. You must use the current key to deploy additional connectors. Regenerating a provisioning key invalidates the existing key but does not affect existing connectors. For more information, see Add Connectors to a Connector Group.
- If you revoke a connector, this also revokes and regenerates the current provisioning key for the connector's connector group. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.
- Provisioning keys appear on the **Admin** > **API Keys** page. You can not manage the provisioning keys from the API Keys page. These keys have a name like `Connector Provisioning Key - GroupName` along with a timestamp.

Copy the Provisioning Key for a Connector Group

Provides instructions for completing the Copy the Provisioning Key for a Connector Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Copy the provisioning key for a connector group, and then use the provisioning key when you deploy a resource connector.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Understand and address the resource connector requirements. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.

Procedure

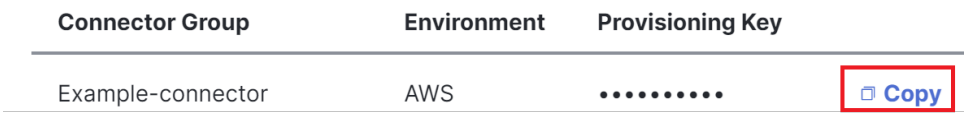
1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.
2. Navigate to the list of connector groups.
   a. If you see a **Next Steps** section at the top of the page, click **Deploy Your Connectors**.

      Choose the connector group where you will add connectors.

   b. If the connector group that you want is not listed on **Next Steps**, then navigate to **Connector Groups**. Click the ellipsis (**...**) on the connector group item, and then choose **View Provisioning Key**.



3. Click **Copy**, to get the provisioning key associated with the connector group.



   a. If the Copy button is dimmed, click **Regenerate** in the same table row and wait a moment while the new key generates, then click **Copy**.

Deploy a Connector in VMware

Describes Deploy a Connector in VMware in Cisco Secure Access. A resource connector is a lightweight service deployed in a virtual machine in your cloud environment.

A resource connector is a lightweight service deployed in a virtual machine in your cloud environment. A resource connector manages the network communications to a configured private resource. Cisco Secure Access provides a pre-configured resource connector image for VMware ESXi.

This guide describes the steps to deploy an OVA file package that includes the Secure Access virtual appliance image for resource connectors running on VMware ESXi. You can deploy the Secure Access OVF template to create your resource connector instances on VMware vSphere or vCenter.

Prerequisites

Meet the requirements for deploying a resource connector on VMware ESXi.

- **vSphere version**–7.0.2 or 8.0.3.
- **CPU**–a 2-core CPU.
- **Memory**–4GB.
- **Disk space**–40GB.
- We recommended that you use an NTP server on your own network. If you use an NTP server on the internet, you must allow traffic to that address on UDP port 123.

For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.

Deployment Guidelines

- Secure Access does not support deploying resource connectors on standalone VMware ESXi hosts. You can only create your resource connectors on VMware vSphere or vCenter.
- Secure Access does not recommend the use of VMware virtual machine snapshots with resource connectors. VMware snapshots of resource connectors may not include the most recent certificate for your resource connector, which may disrupt the connectivity to the resource connector.

UEFI Secure Boot Environment for Resource Connector Images

The Secure Access Resource Connector images for VMware support UEFI Secure Boot, which provides a trusted boot environment for the connector instance.

- You can deploy Resource Connector images with UEFI Secure Boot on these architectures:
  - Intel x86_64
  - AMD64
- We recommend that you deploy your Resource Connector instances with the UEFI Secure Boot environment.

Add a Connector Group

- Add a connector group in the region nearest to the geographical location where you will deploy these connectors, and choose **VMware ESXi** connectors.
- All connectors in a group must use the same virtual environment, for example VMware, otherwise registration fails.

Obtain the Connector Image

You can download the image once and use it for any number of connectors in any connector group. If you have a previously downloaded image, ensure that the image you deploy is the latest version.

- For more information, see Obtain the Connector Image.
- Copy the provisioning key for the connector group where you will deploy the connectors. For more information, see Provisioning Keys for Resource Connectors.

Disk Encryption

Disk encryption is recommended for your connectors. You configure disk encryption during connector deployment, but you should complete any prerequisites before deploying the image. For more information, see the VMware documentation.

SSH Key Generation

To troubleshoot a resource connector, Secure Access requires an SSH key pair. Use the SSH key pair to log in to your resource connector instance. The username is **acadmin**.

- (Recommended) Generate an SSH key pair using a standard tool such as **ssh-keygen**. When you configure the resource connector, add your public key.
- Supported SSH public key types are `ssh-rsa` and `ssh-ed25519`.
- For keys of type `ssh-rsa`, we recommend the key length of 2048 bits or 4096 bits.
- Save your SSH key in your location environment.

> **Note**
>
> You can not set up the SSH login after you deploy the connector.

Save Your Private SSH Key

After you generate an SSH key pair required for access to the resource connector, you must save your SSH key in your environment.

Cisco cannot recover your SSH key and you will lose remote access and the capability to manage the resource connector.

What's Next

Perform the following tasks once per connector instance. You can use the Cisco Secure Access Resource Connector image to create multiple connector instances. You must deploy each connector instance independently.

Important

Do not clone the connector instances.

- Step 1 – Extract the Connector Image for VMware Tar File
- Step 2 – Verify the Integrity of the Image
- Step 3 – Deploy the OVF Template
- Step 4 – Power on Connector Instances
- Step 5 – Confirm Connectors

Step 1 – Extract the Connector Image for VMware Tar File

Provides instructions for completing the Step 1 – Extract the Connector Image for VMware Tar File workflow in Cisco Secure Access. Extract the contents of the Connector Image for VMware tar file.

Procedure

Extract the contents of the **Connector Image for VMware** tar file.

What to do next

```
tar -xvf resource-connector-v1.0.9ova.tar
```

The VMware connector image tar file includes:

- an .ova template containing the Secure Access virtual machines
- a signature file
- a Cisco public key to validate the signature
- a README file

Step 2 – Verify the Integrity of the Image

Describes Step 2 - Verify the Integrity of the Image in Cisco Secure Access. Validate the signature and verify the checksum of the signing key.

Validate the signature and verify the checksum of the signing key.

Validate the Signature

Provides instructions for completing the Validate the Signature workflow in Cisco Secure Access. Verify the authenticity of the image's signature and ensure that the image hasn't been corrupted.

Verify the authenticity of the image's signature and ensure that the image hasn't been corrupted.

Procedure

Run the `openssl dgst` command with the `-sha512` flag.

What to do next

```
openssl dgst -sha512 -verify resource-connector-v0.2.10-240116.pubkey -signature
 resource-connector-v0.2.10-240116.sign resource-connector-v0.2.10-240116.ova
```

On successful signature validation, you should see the message:

```
Verified OK.
```

Verify the Checksum of the Signing Key

Provides instructions for completing the Verify the Checksum of the Signing Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The image download includes a `.pubkey` file. To enhance security and ensure the authenticity of this signing key, you can verify its checksum using the `shasum` command.

Procedure

Run the `shasum` command and provide the name of the `.pubkey` file that is included in your downloaded tar file.

What to do next

```
shasum -a 256 resource-connector-v0.2.10-240116.pubkey
```

The hash generated by this command should match this string:

```
148e2dffa6aa12a4dc6c7cd66d4726ac2c8ef372f28597056ad4e86614da6201
```

Step 3 – Deploy the OVF Template

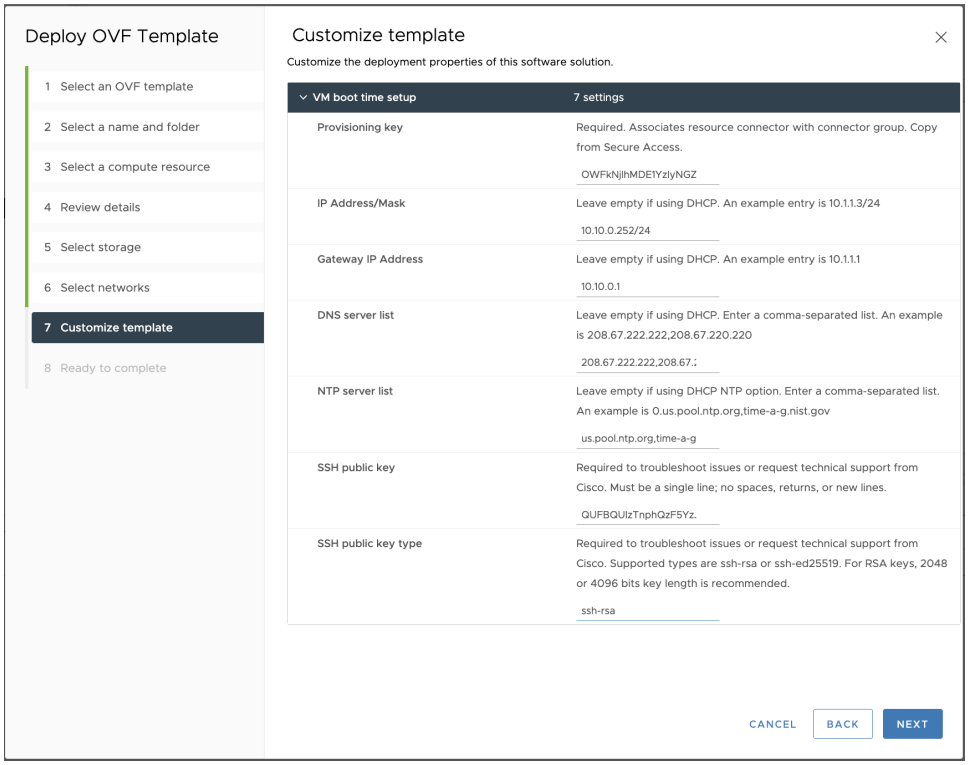
Provides instructions for completing the Step 3 - Deploy the OVF Template workflow in Cisco Secure Access. These instructions are for vSphere, but you can also use vCenter.

These instructions are for vSphere, but you can also use vCenter.

Procedure

1. Sign in to your VMware vSphere client.
2. Click the **File** tab.
3. Click **Deploy OVF Template** and choose the extracted `.ova` template.

   You can use a local copy of the file or a copy of the file stored in your library.



4. Complete the deployment for your environment.

> **Note**
>
> You can not make changes later. If necessary, deploy a new connector.

   a. For **Select Networks**, choose only a single network.

   b. (Recommended) Enable disk encryption.

   c. On **Customize Template**:

   - For **Provisioning key**, add your provisioning key. The provisioning key is required.
   - For **SSH public key**, enter your public key only. Do not include the key type.

     The key must be entered as a single line, without spaces, carriage returns, or new lines.
   - For **SSH public key type**, enter the key type. The key type is case-sensitive.
     - SSH access is required in order to troubleshoot any issues and provide information to Cisco Support.
     - If you don't add the SSH key when you deploy the template, you can not add it later.
   - For **NTP server list**, we recommend that you use an NTP server on your own network.

If you use an internet NTP server, allow traffic through your firewall to the NTP server's address on UDP port 123.

- All other settings on the **Customize Template** page are optional.

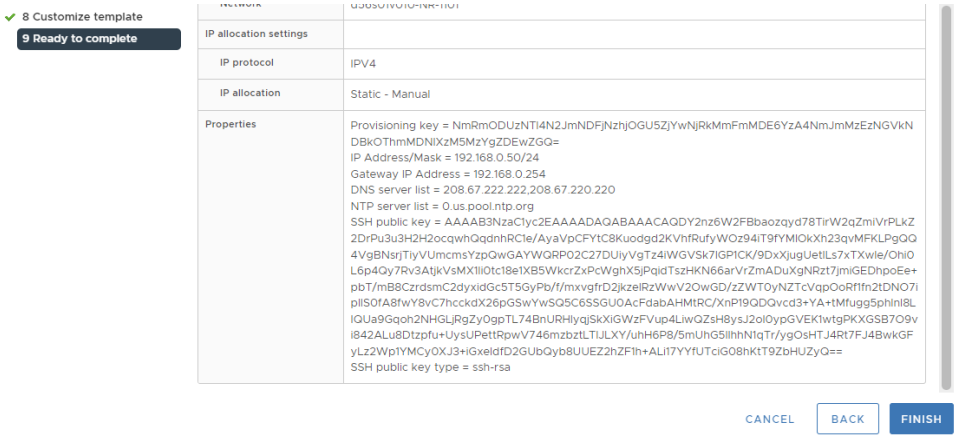
Important

Information you provide on the Customize Template page is not validated during configuration. Verify your entries carefully. If there are errors, your only option is to delete and redeploy the connector.

d. On **Ready to Complete**, review your configurations.

If you entered an SSH key on the **Customize Template** page, verify that the entire key, and only the key, appears on the line and meets the formatting requirements.

For example:



5. Repeat this procedure to deploy additional connectors as needed.

Step 4 – Power on Connector Instances

Provides instructions for completing the Step 4 – Power on Connector Instances workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

After deploying, power on each connector instance. Connectors automatically connect to Secure Access.

Step 5 – Confirm Connectors

Provides instructions for completing the Step 5 – Confirm Connectors workflow in Cisco Secure Access. To complete the connector configuration, you must confirm each connector instance.

To complete the connector configuration, you must confirm each connector instance.

Procedure

You must confirm each connector instance to complete the connector configuration. For more information, see Add Connectors to a Connector Group: Confirm Connectors.

If you do not see the connector in your deployed connectors list, see Troubleshoot Resource Connectors and Connector Groups.

Deploy a Connector in AWS

Describes Deploy a Connector in AWS in Cisco Secure Access. A resource connector is a lightweight service deployed in a virtual machine in your cloud environment.

A resource connector is a lightweight service deployed in a virtual machine in your cloud environment. A resource connector manages the network communications to a configured private resource. Cisco Secure Access provides a pre-configured resource connector image for Amazon Web Services (AWS). This guide describes the steps to deploy an Amazon Machine Image (AMI) to create your resource connector instances.

Prerequisites

Gather the required information, and understand and meet the Requirements and Prerequisites for Resource Connectors and Connector Groups.

- An AWS account.
- Supported architectures:
  - Intel x86_64
  - AMD64
- Required instance type for deployments in production environments: C5.xlarge
- Create the connector group in the region nearest to the geographical location where you will deploy these connectors.
- All connectors in a group must use the same environment, for example: AWS.
- Obtain the connector image from the AWS marketplace. For more information, see Get Connector Images on the AWS Marketplace
- Copy the provisioning key for the specific connector group where you will deploy these connectors. For more information, see Provisioning Keys for Resource Connectors.
- Disk encryption is recommended for your connectors. You configure this during connector deployment, but you should complete any prerequisites before deploying the image. For more information, see the AWS documentation.

UEFI Secure Boot Environment for Resource Connector Images

The Secure Access Resource Connector images for AWS support UEFI Secure Boot, which provides a trusted boot environment for the connector instance.

Important

If you choose an AWS instance type that is not recommended by Cisco Secure Access, we can not guarantee that your Resource Connector instance can boot in AWS. Review the AWS documentation to verify whether your instance type supports UEFI Secure Boot.

- You can deploy Resource Connector images with UEFI Secure Boot on these architectures:
  - Intel x86_64
  - AMD64
- We recommend that you redeploy your Resource Connector instances with the UEFI Secure Boot environment.

Save Your Private SSH Key

After you generate an SSH key pair required for access to the resource connector, you must save your SSH key in your environment.

Cisco cannot recover your SSH key and you will lose remote access and the capability to manage the resource connector.

What's Next

Perform the following tasks once per connector instance. You can use the Cisco Secure Access Resource Connector image to create multiple connector instances. You must deploy each connector instance independently.

Important

Do not clone the connector instances.

- Step 1 – Launch an Amazon Machine Image for each Connector Instance
- Step 2 – Configure the Connector
- Step 3 – Launch the Connector Instance

Get Connector Images on the AWS Marketplace

Provides instructions for completing the Get Connector Images on the AWS Marketplace workflow in Cisco Secure Access. Navigate to the AWS Marketplace at https://aws.amazon.com/marketplace/pp/prodview-oonzvpdnti7jm and sign in with your AWS account.

Procedure

1. Navigate to the AWS Marketplace at `https://aws.amazon.com/marketplace/pp/prodview-oonzvpdnti7jm` and sign in with your AWS account.
2. Choose the Secure Access Resource Connector image for your cloud environment.

Step 1 – Launch an Amazon Machine Image for the Connector Instance

Provides instructions for completing the Step 1 – Launch an Amazon Machine Image for the Connector Instance workflow in Cisco Secure Access. Launch an Amazon machine image for each connector instance.

Launch an Amazon machine image for each connector instance.

Procedure

1. Navigate to the AWS Marketplace at `https://aws.amazon.com/marketplace/pp/prodview-oonzvpdnti7jm` and sign in with your AWS account.
2. Review the AMI product overview, pricing, usage, and support.
3. Click **Continue to Subscribe**.
4. Review the **Terms and Conditions** and then click **Accept Terms**.
5. Click **Continue to Configuration** after accepting End User License Agreement (EULA).
6. Choose **Fulfillment Option (AMI)**, **Software Version (latest)** and **Region**.
7. Continue to **Launch**.
8. For the **Launch** action, choose **Launch through EC2** to launch the configuration through the Amazon EC2 console, and then click **Launch**.

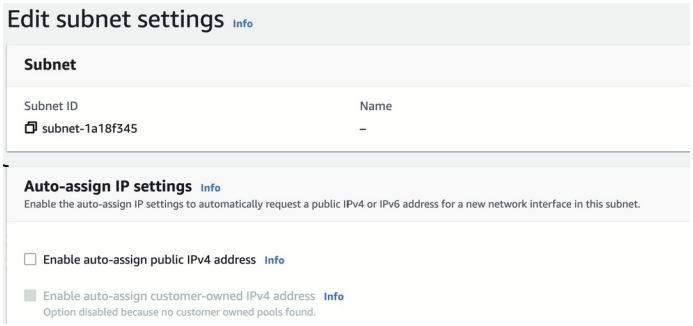
> **Note**
>
> The **Launch from website** option is not supported.

Step 2 – Configure the Connector

Provides instructions for completing the Step 2 - Configure the Connector workflow in Cisco Secure Access. Navigate to the launched Amazon EC2 console to configure the connector instance.

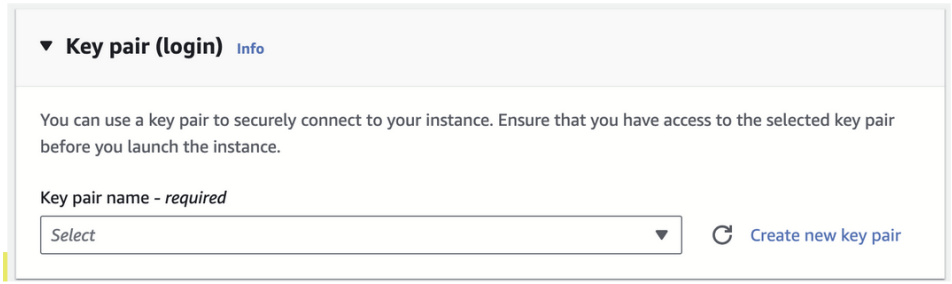
Procedure

1. Navigate to the launched Amazon EC2 console to configure the connector instance.
2. Enable **Auto-Assign Public IP**.



   This ensures that a Datagram Transport Layer Security (DTLS) connection uses the same IP address as Transport Layer Security (TLS) connections, which is required for optimal throughput.

3. Set the SSH key pair to enable access to the connector instance, and then save your SSH key to your local system. Use the **acadmin** username.



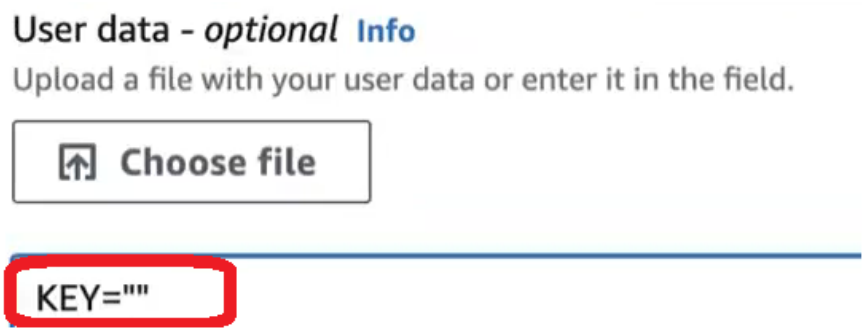
   SSH access is required in order to troubleshoot an issue or get information about the connector to provide to Secure Access support. You can SSH to the connector after the instance launches.

   Important

   You can not enable SSH access after the connector deploys on AWS.

4. Associate the connector with the connector group.
   a. Navigate to **Advanced Details**, scroll to the **User Data - optional** area.

b. In the text box, type **KEY=" "** and paste the provisioning key that you copied from the connector group in Secure Access between the quotation marks, with no spaces anywhere in the text box. For more information about creating connector provisioning keys, see Provisioning Keys for Resource Connectors.



5. Specify the number of connector instances to create based on the calculations you used for required throughput when you added the connector group.

   For redundancy, you should deploy at least two connector instances for each group.

Step 3 – Launch the Connector Instance

Provides instructions for completing the Step 3 – Launch the Connector Instance workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

---

1. Launch the instance.

   Once the resource connector VM is up, you can connect to your instance using SSH.

   The resource connector establishes a network tunnel to the private resource.

2. After you launch the instance, the connector syncs automatically with Secure Access.

   - You must confirm each connector instance to complete the connector configuration. For more information, see Add Connectors to a Connector Group: Confirm Connectors.
   - If you do not see the connector in your deployed connectors list, see Troubleshoot Resource Connectors and Connector Groups.

Deploy a Connector in Azure

Describes Deploy a Connector in Azure in Cisco Secure Access. A resource connector is a lightweight service deployed in a virtual machine in your cloud environment.

A resource connector is a lightweight service deployed in a virtual machine in your cloud environment. Resource connectors manage the network communications to a configured private resource. Cisco Secure Access provides a pre-configured resource connector image for Azure.

Follow the steps in this guide to deploy the Cisco Secure Access resource connector image on Azure and create your resource connector instances.

Prerequisites

Gather the required information and meet the requirements to deploy resource connectors on Azure. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.

- A user account on Azure.
- Create the connector group in the region nearest to the geographical location where you will deploy these connectors. For more information, see Add Resource Connector Groups.
- All connectors in a group must use the same environment, for example: Azure.
- Obtain the connector image from the Microsoft Azure Marketplace. For more information, see Get Connector Images on the Azure Marketplace.
- Copy the provisioning key for the specific connector group where you will deploy these connectors. For more information, see Provisioning Keys for Resource Connectors.
- Disk encryption is recommended for your connectors. You configure this during connector deployment, but you should complete any prerequisites before deploying the image. For more information, see the Azure documentation.

UEFI Secure Boot Environment for Resource Connector Images

The Secure Access Resource Connector images for Azure support UEFI Secure Boot, which provides a trusted boot environment for the connector instance.

We recommend that you deploy your Resource Connector instances with the UEFI Secure Boot environment.

Deployment Requirements

- You can deploy Resource Connector images in Azure on **x64** architectures.
- For production environments, we recommend these instance types:
  - F4s Standard
  - F4s Standard v2
  - F8s Standard v2
  - Standard_D4as_v5 (4 vCPU, 16 GiB)

Save Your Private SSH Key

After you generate an SSH key pair required for access to the resource connector, you must save your SSH key in your environment.

Cisco cannot recover your SSH key and you will lose remote access and the capability to manage the resource connector.

What's Next

Perform the following tasks once per connector instance. You can use the Cisco Secure Access Resource Connector image to create multiple connector instances. You must deploy each connector instance independently.

Important

Do not clone the connector instances.

- Step 1 – Get Connector Images on Microsoft Azure Marketplace
- Step 2 – Configure the Resource Connector Virtual Machine
- Step 3 – Connect to Resource Connector Instance

Step 1 – Get Connector Images on Microsoft Azure Marketplace

Provides instructions for completing the Step 1 – Get Connector Images on Microsoft Azure Marketplace workflow in Cisco Secure Access. Sign in to Azure and then navigate to the Microsoft Azure Marketplace.

Procedure

1. Sign in to Azure and then navigate to the Microsoft Azure Marketplace.

   https://portal.azure.com/#view/Microsoft_Azure_Marketplace/GalleryItemDetailsBlade/id/cisco.cisco-resource-connector.

   > **Note**
   >
   > You can reach the Microsoft Azure Marketplace and Cisco Secure Access Resource Connector images from Secure Access. Navigate to **Connect** > **Network Connections** > **Connector Groups** and then click **Connector Image for Microsoft Azure**

2. Select the **Cisco Secure Access Resource Connector BYOL** plan, and then click **Create** to configure the resource connector virtual machine.

Step 2 – Configure the Resource Connector Virtual Machine

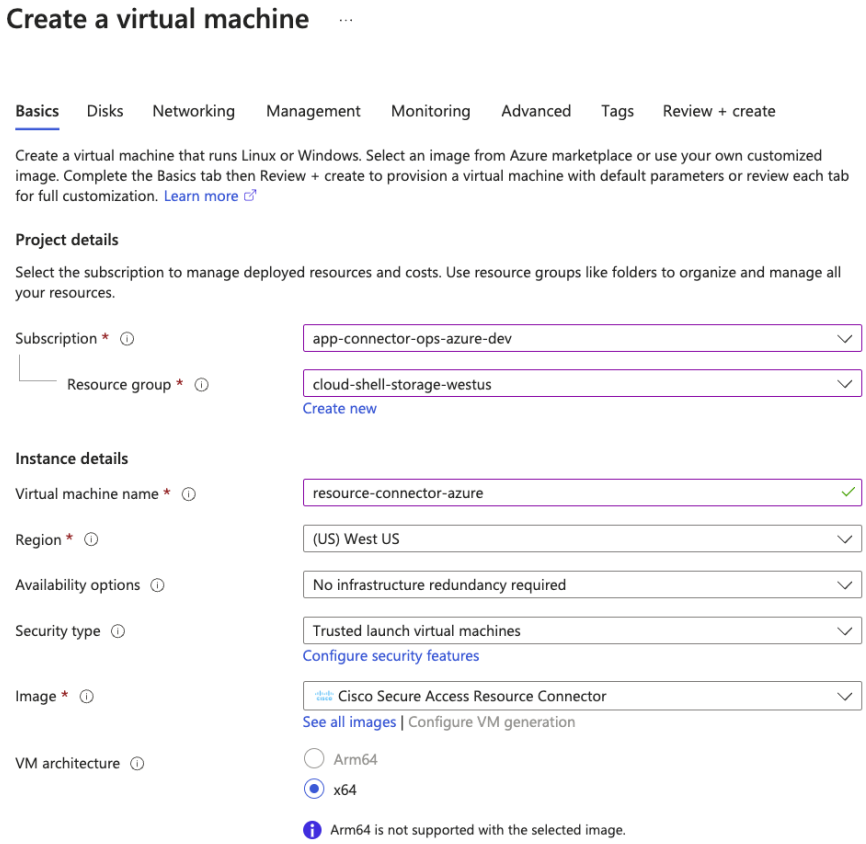
Provides instructions for completing the Step 2 – Configure the Resource Connector Virtual Machine workflow in Cisco Secure Access. Create a resource connector virtual machine on Azure.

Create a resource connector virtual machine on Azure.

Procedure

1. On **Create a virtual machine**, click the **Basics** tab.

> **Note**
>
> For **Disks**, **Management**, **Monitoring**, and **Tags**, you can modify the settings for you cloud environment or keep the default selections.



2. Navigate to **Project details**.
   a) Choose your **Subscription** and **Resource Group**.
3. Navigate to **Instance details**.
   a) For **Virtual machine name**, enter a name for the virtual machine.
   b) For **Region**, choose the region where the private resource is deployed in your cloud environment.
   c) For **Security type**, use the default setting: **Trusted launch virtual machines**.

      The **Trusted launch virtual machines** default setting selects the **Enable secure boot** option.

   d) For **VM architecture**, choose the **x64** architecture for the virtual machine.
   e) For **Size**, choose **Recommended by image publisher** types.

   > **Note**
   >
   > You do not have to configure the image. **Image** is preselected.

4. Navigate to **Administrator account**.

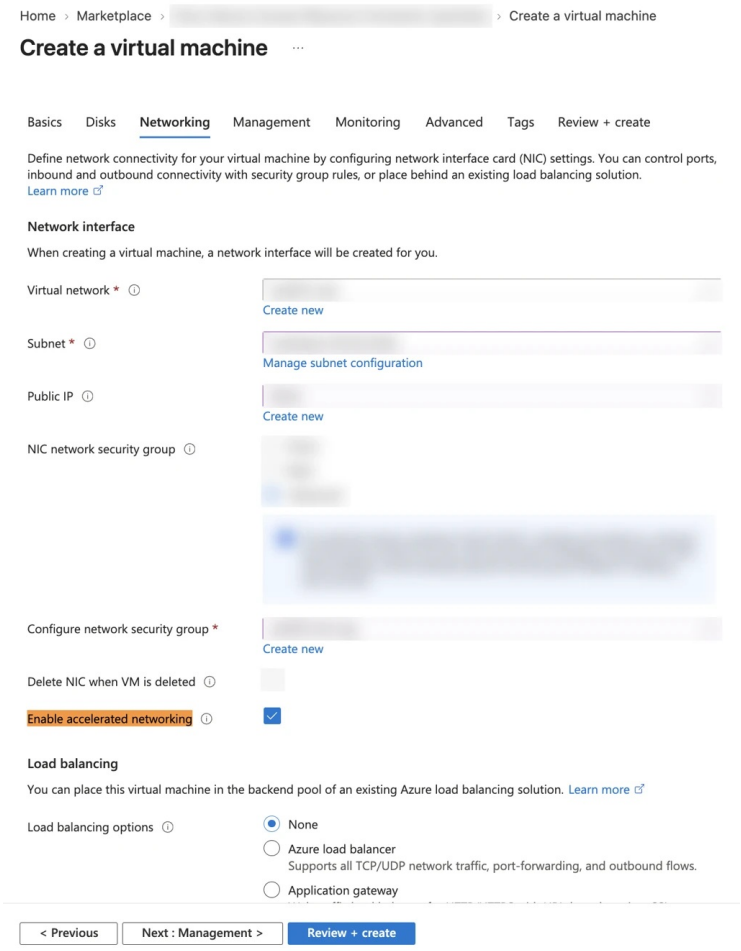
a) For **Authentication type**, choose **SSH public key**.
b) For **Username**, use the default setting: **azureuser**. The **azureuser** username is an internal account that does not have login access. You must deploy the VM with the username **azureuser**.

> **Note**
>
> You can only log into the resource connector instance with the username **acadmin**.

Choose an existing SSH key pair or generate an SSH key pair to enable access to the connector instance. Save your SSH key to your local system.

SSH access to the resource connector VM is required in order to troubleshoot an issue or get information about the connector to provide to Support.

5. Click the **Networking** tab and check the **Enable accelerated networking** checkbox. This supports the Standard_D4as_v5 instance type.



Note: Enable **Accelerated Networking** on the connector VM's network interface. In the Azure portal, select **Enable accelerated networking** on the **Networking** tab when you create the VM. Accelerated Networking improves network throughput and reduces CPU load on the connector.

To enable it on an existing connector VM use the following steps:

a. Stop the VM so that its status is **Stopped**. Restarting the VM is not enough.

b. Open the VM's network interface, then enable **Accelerated networking.**

c. Start the VM. You can confirm the setting with the Azure CLI: `az network nic show -g -n --query enableAcceleratedNetworking`. The output is `true` when Accelerated Networking is enabled.

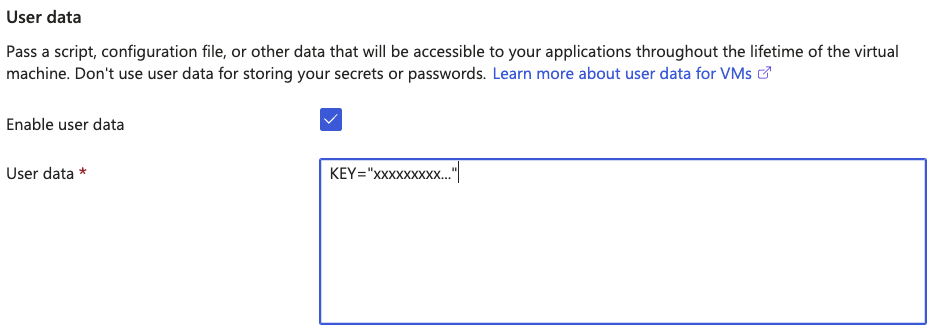
6. Click the **Advanced** tab.

a) Check **Enable user data**.

b) For **User data**, in the text box, type **KEY=" "** and paste the provisioning key that you copied from the connector group in Secure Access between the quotation marks, with no spaces anywhere in the text box.

> **Note**
>
> If you do not see a **User data** field when creating the VM, then you are in the newer create-VM experience Azure provides, which hides this field. At the top of the **Create a virtual machine** page, select **" Previous experience"** and revert the creation window to the classic experience to restore the **Enable user data / User data** option, then continue with the steps below.

For more information about creating connector provisioning keys, see Provisioning Keys for Resource Connectors.



7. Navigate to the **Review + create** tab, and then click **Create**.

The system deploys the instance of the resource connector in the virtual machine.

8. (Optional) Compare the ID of the deployed virtual machine on Azure with the **Connector ID** for the resource connector on Secure Access.

a) On Azure, navigate to **Home** > **Virtual Machines** and then click the name of a virtual machine. From a virtual machine, navigate to **Overview**, and then click **JSON View**.

The **JSON View** displays the properties of the deployed resource connector instance. The value of the **vmId** property is the ID of the virtual machine.

```
"properties": {
    "hardwareProfile": {
        "vmSize": "Standard_F4s_v2"
    },
    "provisioningState": "Succeeded",
    "vmId": "b9c3a487-9fad-4707-b832-2826e7351b38",
```

b) On Secure Access, navigate to **Connect** > **Network Connections** > **Connector Groups**.

Locate the resource connector by the **Connector ID**. Verify that the **Connector ID** for the deployed resource connector matches the ID of your virtual machine on Azure.



Step 3 – Connect to the Resource Connector Instance

Provides instructions for completing the Step 3 - Connect to the Resource Connector Instance workflow in Cisco Secure Access. Once the resource connector VM is up, you can connect to your instance using SSH.

Once the resource connector VM is up, you can connect to your instance using SSH.

The resource connector establishes a network tunnel to the private resource.

The resource connector syncs automatically with Secure Access.

- You must confirm each connector instance to complete the connector configuration. For more information, see Add Connectors to a Connector Group: Confirm Connectors.
- If you do not see the connector in your deployed connectors list, see Troubleshoot Resource Connectors and Connector Groups.

Procedure

Log into the resource connector instance using SSH with the **acadmin** username.

Deploy a Connector in Docker

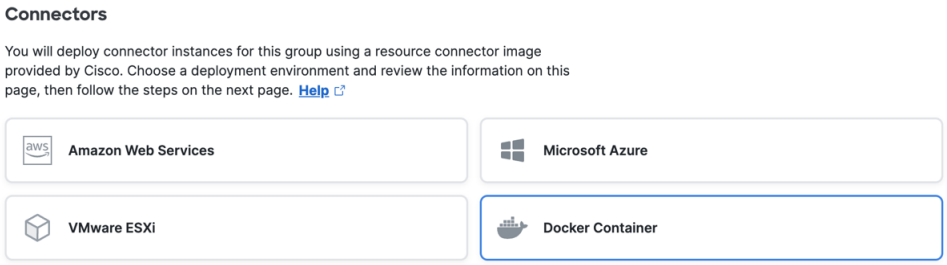
Describes Deploy a Connector in Docker in Cisco Secure Access. Cisco Secure Access supports several methods to deploy Resource Connectors in on-premises or cloud environments.

Cisco Secure Access supports several methods to deploy Resource Connectors in on-premises or cloud environments. A Resource Connector is a lightweight service that manages the network communications for a private resource. The private resource is configured and managed by the organization.

This guide describes how to deploy a Resource Connector in a Docker container using the Secure Access Docker container image.

Prerequisites

- Create a Resource Connector Group with the **Docker Container** type. For more information, see Add Resource Connector Groups.



- Copy the provisioning key for the resource connector group where you are deploying the connectors. You must have the provisioning key for the resource connector group when deploying the connector instances. For more information, see Provisioning Keys for Resource Connectors.

Deployment Guidelines

- Dedicate a virtual machine (VM) or bare metal host for the resource connector.
- You can launch only one Resource Connector instance for each VM or bare metal environment.
- The VM or bare metal environment must have a single network interface. Secure Access does not support multiple network interfaces.
- Secure Access does not recommend the use of VMware virtual machine snapshots with resource connectors.

  VMware snapshots of resource connectors may not include the most recent certificate for your resource connector, which may disrupt the connectivity to the resource connector.

Host or VM Requirements

- **CPU**–At least two vCPUs.
- **Memory**–4GB.
- **Disk space**–16GB.
- **Network**–A single network interface on the host or VM.

Supported Host Operating Systems

Secure Access supports a deployment of one of these operating systems on the host machine:

- Ubuntu Server LTS 22.04 x64
- Ubuntu Server LTS 24.04 x64
- Red Hat Enterprise Linux (RHEL v9)

Important

When you install the supported OS on the host machine, do not install Docker on the host. The Secure Access setup script (**setup_connector.sh**) installs Docker and the resource connector software packages. For more information about the Secure Access setup script, see Set Up the Resource Connector and Container.

What's Next

1. Set Up the Resource Connector and Container–Run the set up script for the resource connector.
2. Launch the Resource Connector in the Docker Container–Launch the Docker container that runs the instance of the resource connector.

Set Up the Resource Connector and Container

Provides instructions for completing the Set Up the Resource Connector and Container workflow in Cisco Secure Access. To begin, get the Secure Access Resource Connector setup script (setup_connector.sh).

> **Note**
>
> On the host, Secure Access supports running one Docker container.

To begin, get the Secure Access Resource Connector setup script (`setup_connector.sh`). Then, set the permissions on the script and run the script.

The `setup_connector.sh` script downloads the scripts and configuration files that are required to set up and run the resource connector in the Docker container. The `setup_connector.sh` script saves the scripts and configuration files in the `/opt/connector/install` directory.

Procedure

1. Log into the host or VM with a user that has sudo permissions.
2. Run `curl` to get the Secure Access Resource Connector setup script (`setup_connector.sh`).

```
curl -o setup_connector.sh
https://us.repo.acgw.sse.cisco.com/scripts/latest/setup_connector.sh
```

3. Set the permissions on the script.

```
chmod +x setup_connector.sh
```

4. Run the `setup_connector.sh` script.

```
sudo ./setup_connector.sh
```

What to do next

For information about error conditions that may occur when you set up of the resource connector, see Troubleshoot Container Deployments - Setup Failures.

Launch the Resource Connector in the Docker Container

Provides instructions for completing the Launch the Resource Connector in the Docker Container workflow in Cisco Secure Access. Run the connector.sh script to deploy the resource connector in the Docker container and start and stop the resource connector.

Run the **connector.sh** script to deploy the resource connector in the Docker container and start and stop the resource connector.

The **connector.sh** script sets up a service in the `/etc/service/connector_svc` directory. If the Docker container stops, the **connector.sh** service relaunches the container with the resource connector automatically.

Important

You can launch one instance of a resource connector only in a host or VM.

Procedure

1. Log into the host or VM with a user that has sudo permissions.
2. Construct a descriptive name for the resource connector. You will use the name of the resource connector to launch the connector in the Docker container.

   We recommend that you use the name of the resource connector group as part of the connector's name.

   For example:

```
<name of the resource connector group>-<label for the resource connector>
```

   The `--name <connector_name>` option in the launch script accepts a sequence of 1-32 alphanumeric and hyphen (**-**) characters.

   Secure Access appends the ID of the connector onto the value that you provide for `connector_name`.

3. Run the **connector.sh** script with the specified options.

```
sudo /opt/connector/install/connector.sh launch --name <connector_name> --key
 <provisioning_key>
```

   a) For `connector_name`, provide the name of the resource connector.
   b) For `provisioning_key`, provide the value of the provisioning key that you generated for the resource connector group.

      For more information, see Copy the Provisioning Key for a Connector Group.

4. Sign in to Secure Access and confirm that the resource connector deployed. The resource connector that is deployed in the Docker container should provision and then display in Secure Access. For more information, see Step 2: Confirm Connectors.

What to do next

Important

If you provide an incorrect provisioning key for the resource connector group, the Docker container will start, but the resource connector will not be able to provision and register with Secure Access. If this occurs, we recommend that you delete the Docker container and deploy the connector again.

Troubleshoot Container Deployments

Describes Troubleshoot Container Deployments in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Setup Failures on page 429
- Check the Container's Status–Verify the status of the container.
- Get the Version of the Docker Container Image–Get the version of the running container image.
- Stop the Container–Stop the container.
- Restart the Container–Restart the container.
- Delete the Container–Remove the container.
- Run Diagnostic and Techsupport Scripts–Run the **diagnostic** and **techsupport** scripts to gather information about the deployed container.

Setup Failures

Describes Setup Failures in Cisco Secure Access. If error conditions occur when you set up the connector with Docker, verify that you can access the destinations to download and install the required software packages and files.

- If error conditions occur when you set up the connector with Docker, verify that you can access the destinations to download and install the required software packages and files.
- Before you run the connector setup script, you may have to authenticate with Docker.

Connectivity or Execution Errors

You may come across one of the following errors, or a similarly phrased error:

- `Failed to fetch...`

- `Could not connect to...`
- `Network is unreachabe.` or `Connection timed out.`

This may be caused by insufficient access to outbound destinations, a faulty package installation, required security updates, or a setup dependency that has been updated since you initially executed the installation script.

We strongly recommend running the `setup_connector.sh` script again or confirming that your environment allows **all** traffic to the designated destinations mentioned in Destinations For All Regions on page 399 and Region-Specific Destinations on page 398.

Rate Limit with Docker Pull

The `setup_connector.sh` script runs `docker pull` without authentication to download the connector image from Docker Hub, which is rate limited. If you encounter a rate limit error when you run `setup_connector.sh`, Docker returns this error message:

```
You have reached your pull rate limit. You may increase the limit by
authenticating and upgrading …
```

When the Docker rate limit error occurs, we recommend that you authenticate with Docker, and then run the `setup_connector.sh` script again. To authenticate with Docker, run:

```
sudo docker login
```

Connectivity Issues

The `setup_connector.sh` script installs the required host packages and downloads the scripts to manage the connector.

Ensure that the host has connectivity to these destinations and can download the required scripts and files:

- **https://github.com** –Access to this site is required only for downloading the Sigstore **cosign** binary during the connector setup. Secure Access uses **cosign** to verify the container image. You do not need access to the GitHub site when you run the connector, only for the setup of the connector in the container.
- **https://us.repo.acgw.sse.cisco.com**
- **Docker Hub**–For more information, see Allow Resource Connector Traffic to Secure Access.
- **Supported OS packages**–Configure the host or VM correctly to install the supported OS packages, repo mirror, or locally mounted DVD image.

Check the Container's Status

Provides instructions for completing the Check the Container's Status workflow in Cisco Secure Access. Log into the host machine with a user account that has sudo access.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the Docker `ps` command to show the status of all containers.

```
sudo docker ps -a
```

Get the Version of the Docker Container Image

Provides instructions for completing the Get the Version of the Docker Container Image workflow in Cisco Secure Access. Log into the host machine with a user account that has sudo access.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the Docker `ps` command to list the running Docker containers and format the output with the value of `.Image`.

```
sudo docker ps --format '{{.Image}}'
```

Stop the Container

Provides instructions for completing the Stop the Container workflow in Cisco Secure Access. Log into the host machine with a user account that has sudo access.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the `connector.sh` script with the `stop` command to stop the container.

```
sudo /opt/connector/install/connector.sh stop
```

Restart the Container

Provides instructions for completing the Restart the Container workflow in Cisco Secure Access. Log into the host machine with a user account that has sudo access.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the `connector.sh` script with the `start` command to restart the container.

```
sudo /opt/connector/install/connector.sh start
```

Delete the Container

Provides instructions for completing the Delete the Container workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Delete the container and persistent datastore.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the `connector.sh` script with the `stop` command and `--destroy` flag to delete the container and persistent datastore.

```
sudo /opt/connector/install/connector.sh stop --destroy
```

What to do next

Sign into Secure Access and remove the Resource Connector. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.

Run Diagnostic and Techsupport Scripts

Provides instructions for completing the Run Diagnostic and Techsupport Scripts workflow in Cisco Secure Access. The diagnostic script runs a series of ping and DNS tests on the local IP address, gateway, Secure Access APIs, and headend IP addresses.

The **diagnostic** script runs a series of ping and DNS tests on the local IP address, gateway, Secure Access APIs, and headend IP addresses. The script also checks connectivity on HTTPS ports to various Secure Access endpoints, along with system artifacts created through the connector instance provisioning process.

The **techsupport** script displays the following information:

- Version of the resource connector software.
- VPN tunnel state and related information.
- System monitoring metrics, such as disk and memory statistics.
- Information snapshot of the connector host, from DNS to Network interface details, iptables, routes, sysctl system settings, and monitoring information.
- Recent periodic resource connector software logs.

Run the **diagnostic** or **techsupport** scripts to troubleshoot the resource connector in the container.

Procedure

1. Log into the host machine with a user account that has sudo access.
2. Run the diagnostic and troubleshooting scripts.
   - For the **diagnostic** script, run:

     ```
     /opt/connector/data/bin/diagnostic
     ```

   - For the **techsupport** script, run:

     ```
     sudo /opt/connector/data/bin/techsupport
     ```

Determine the Number of Connectors Needed in a Connector Group

Provides instructions for completing the Determine the Number of Connectors Needed in a Connector Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The number of connectors needed in a group depends on the throughput capacity that your organization needs. You can expand throughput capacity at any time by adding connectors to a connector group.

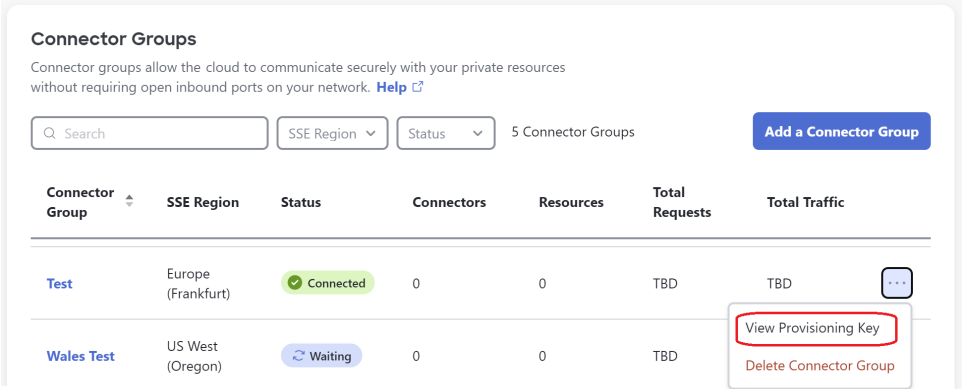
Use the following procedure to determine how many connectors to deploy in a connector group, based on the volume of traffic that you expect the connector group to handle.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Review the important information about calculating the capacity. For more information, see Capacity Requirements.

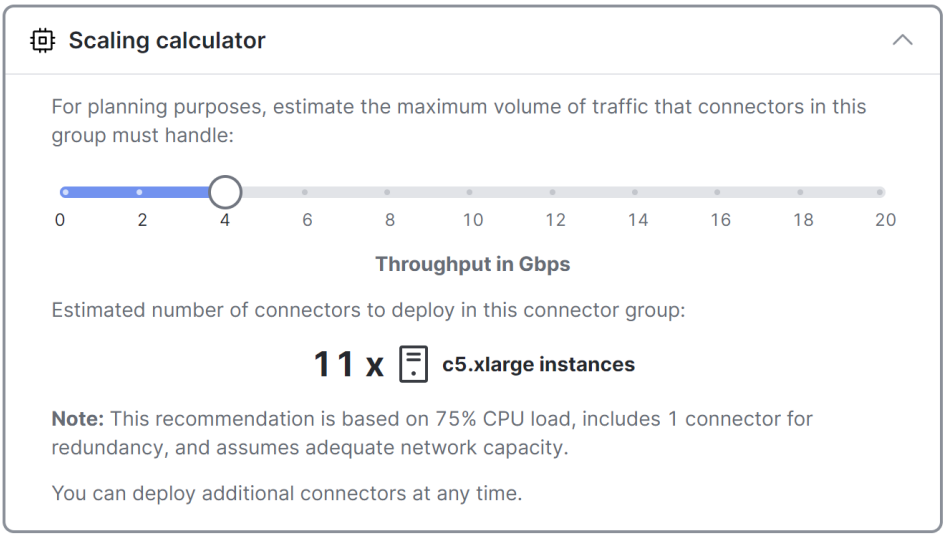
Procedure

1. Navigate to **Connect** > **Network Connections**, and then click **Connector Groups**.
2. If you see **Next Steps** at the top of the page, scroll down to the **Connector Groups** section.
3. In the row for the relevant connector group, click the ellipsis for the connector group and choose **View Provisioning Key**.



4. Look at the **Scaling calculator** section.

   For example, for AWS, the information might look like this:



Assign Private Resources to a Connector Group

Describes Assign Private Resources to a Connector Group in Cisco Secure Access. Resource Connectors send user traffic to the private resources assigned to a connector group.

Resource Connectors send user traffic to the private resources assigned to a connector group. You can view the resources already assigned to a connector group. For more information, see View a Connector Group's Connectors and Assigned Resources.

Guidelines for Assigning a Private Resource to a Connector Group

Describes Guidelines for Assigning a Private Resource to a Connector Group in Cisco Secure Access. All resources should be located in the same data center, branch office, or security zone as the connectors in the group.

- All resources should be located in the same data center, branch office, or security zone as the connectors in the group.
- If an application is hosted across multiple locations, you can assign the private resource to multiple connector groups, and Secure Access will send traffic to the connector group that is geographically nearest to the location from which the end-user device is connected, based on IP address.
- You can assign resources to a group at any time.

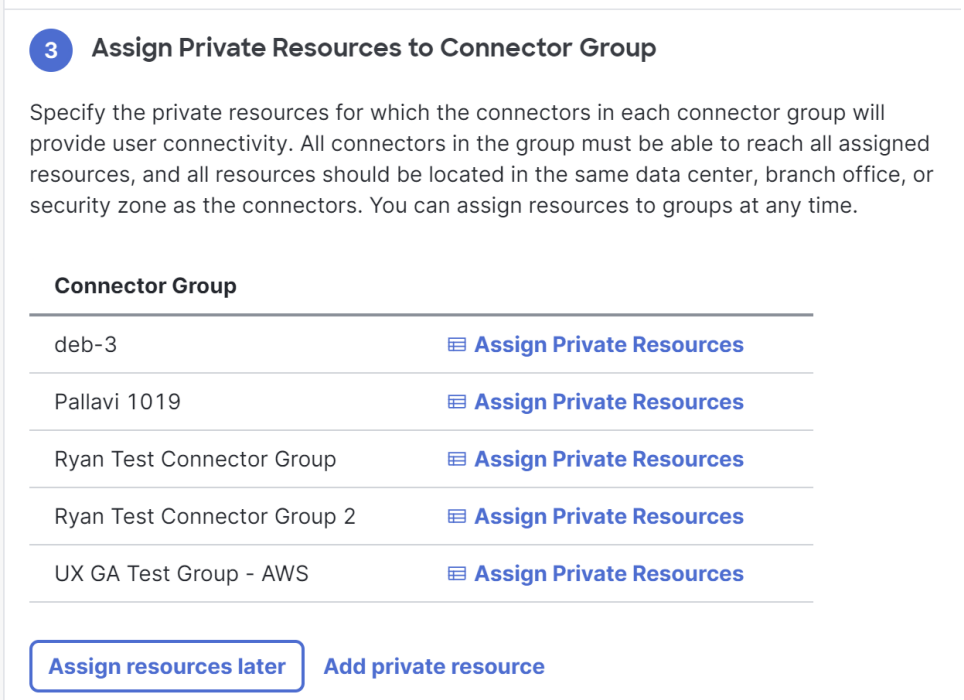
Assign a Private Resource to a Connector Group

Provides instructions for completing the Assign a Private Resource to a Connector Group workflow in Cisco Secure Access. Assign each private resource to the connector group in the same data center, branch office, or security zone that contains the private resource.

Assign each private resource to the connector group in the same data center, branch office, or security zone that contains the private resource.

Procedure

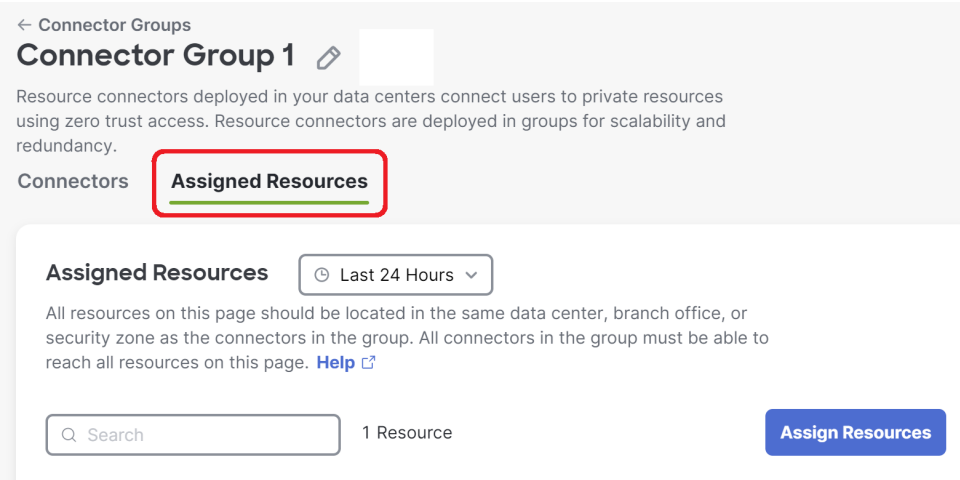
1. Navigate to **Connect** > **Network Connections**.
2. If you see **Next Steps** at the top of the page:
   a. Click **Assign Private Resources to Connector Group** :



   b. Look in the list for the connector group that you want to assign resources to.

      If you don't see the group you want, go to the next step.

   c. For the connector group you want to add connectors to, click **Assign Private Resources**.
3. If you don't see a "Next Steps" section or an "Assign Private Resources to Connector Groups" subsection:
   a. Scroll down the page to the **Connector Groups** section.
   b. In the table, click the name of the connector group.
   c. Click the **Assigned Resources** tab.



d. Click **Assign Resources**.

4. Assign resources.
5. Click **Save**.

View a Connector Group's Connectors and Assigned Resources

Provides instructions for completing the View a Connector Group's Connectors and Assigned Resources workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View the connectors and private resources that are assigned to a connector group.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Connect** > **Network Connections**.
2. Click **Connector Groups**.
3. If you see **Next Steps** at the top of the page, scroll down to the **Connector Groups** section.
4. In the row for the relevant connector group, click the name of the connector group.
5. Click the **Connectors** or **Associated Resources** tab.

Edit a Resource Connector Group

Provides instructions for completing the Edit a Resource Connector Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you deploy a Cisco Secure Access connector group, you can modify the name of the connector group, add alternate DNS servers with domains, or edit the DNS servers and domains that you configured for the resource connector.

Secure Access uses the default DNS server that you configured during connector deployment to resolve destinations for private resources. If the private resources in your organization are on various domains and the destinations are resolved by different DNS servers, you can specify these domains and DNS servers for the connector group in Secure Access.

Configure the properties of the Connector Group, optionally add DNS Servers and domains to resolve traffic for private resources, and edit configured DNS servers and domains.

Important

If you delete a DNS server in Secure Access that is configured on a resource connector group, then new instances of the connectors in the resource connector group can not communicate with Secure Access. We recommend that you first remove a DNS server and domains on the resource connector group before you delete the DNS server from Secure Access. For more information, see Manage DNS Servers.

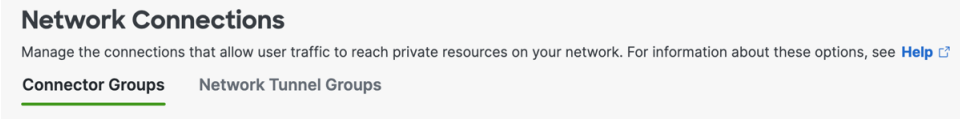
During initialization, resource connectors use the default DNS server to resolve the fully-qualified domain name (FQDN) of a private resource. By associating domains with DNS servers, you override this behavior and allow alternate DNS servers to resolve the domains for private resources.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- (Optional) To add domains and DNS servers for a connector group, you must deploy the resource connectors in the connector group with Cisco Secure Access Connector software image version **2.0.33-xxxxx** or newer.

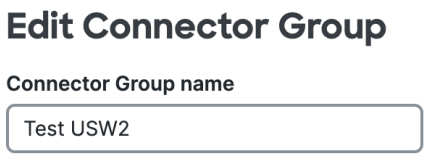
Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.

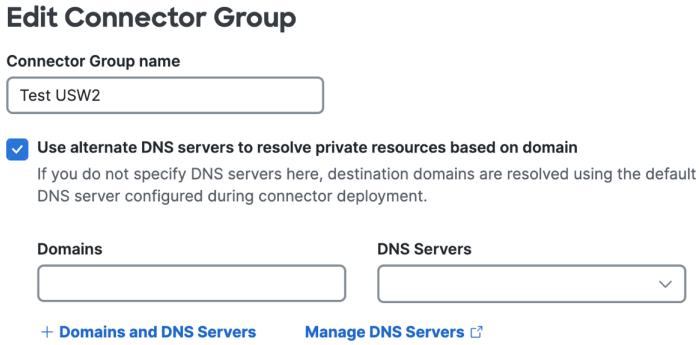


2. Navigate to the Connector Group table, click on the name of a Connector Group, and then click **Edit**.
3. For **Connector Group name**, enter a descriptive name for the connector group.

   We recommend that you indicate the data center, branch office, or security zone location in the name.

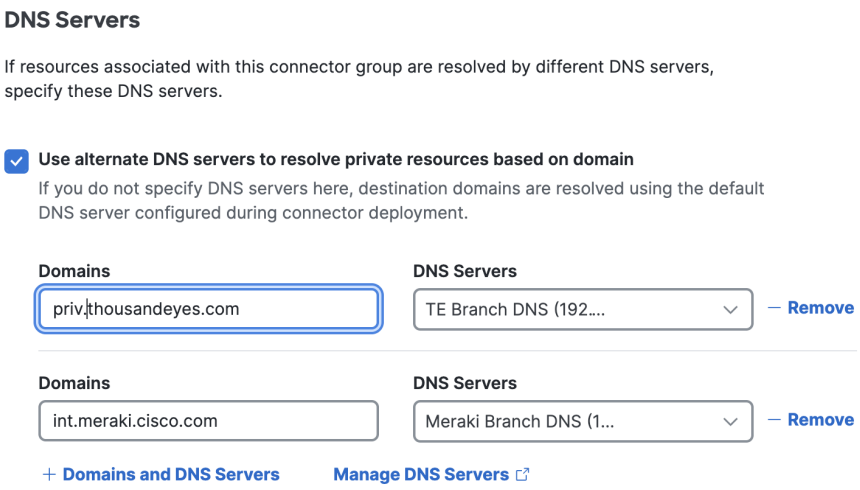


4. Check **Use alternate DNS servers to resolve private resources based on domain**.



   a) For **Domains**, enter a single domain or a comma-separated list of domains.
      - You can add up to five DNS servers and domains with a total of 50 unique domains.
        - For each addition, you can select the same DNS Server but add unique domains only.

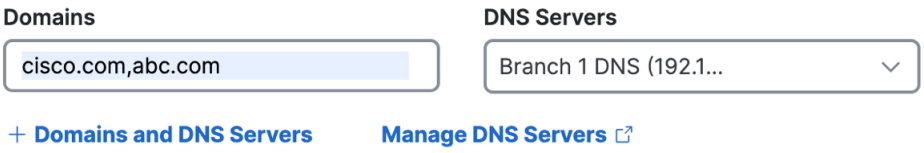
- When you select a DNS server, Secure Access adds the primary DNS server and if configured, the secondary DNS server.
- You can add a maximum of ten unique domains with a DNS server. When you add multiple domains, separate the domains with a comma.
- You must add at least one domain with a DNS server.
- Secure Access does not support wildcards with domains.
- Secure Access supports valid domains only.



b) For **DNS Servers**, select a configured DNS server.

The selected DNS servers includes the primary DNS server and if available, the secondary DNS server. For more information, see Manage DNS Servers.

c) (Optional) To add more domains and DNS servers, click **+ Domains and DNS Servers**, and then repeat steps 5-6.



d) (Optional) To remove a set of **Domains** and **DNS Servers**, click **Remove**.

5. (Optional) To remove all configured DNS servers and domains, uncheck the **Use alternate DNS servers to resolve private resources based on domain** option.
6. Click **Save**.

Disable, Revoke, or Delete Resource Connectors and Groups

Describes Disable, Revoke, or Delete Resource Connectors and Groups in Cisco Secure Access and explains About Disabling a Resource Connector, About Revoking a Resource Connector, and About Deleting a Resource Connector. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can disable, delete, or revoke connectors. You can also disable or delete connector groups.

The differences between these actions are described on this page.

For more information, see Disable, Revoke, or Delete a Connector.

About Disabling a Resource Connector

Disabling a resource connector stops Secure Access from sending traffic through that connector unless and until you enable it again.

Other connectors in the group that are not disabled will continue to send traffic to private resources in the connector group.

Disabled connectors continue to be automatically updated.

About Revoking a Resource Connector

Revoke a connector if, for example, you suspect that it is rogue or has been compromised.

Revoking a connector will:

- Prevent the connector from connecting to Secure Access and providing connections to private resources. Existing connections through the connector instance will be dropped, and affected users must re-initiate connections to resources. Other existing connectors are not affected.
- Invalidate the current provisioning key for the connector group and generate a new key. The provisioning key is used only during connector creation, so existing connectors are not affected. When you add connectors to the connector group in the future, you can no longer use the old key.

Revoking a connector does not delete deployed connector instances. To delete a connector instance, see the documentation for your virtual environment.

About Deleting a Resource Connector

Connectors that have not connected to Secure Access will be automatically deleted after a period of time.

If you delete a connector:

Existing connections through the connector instance will be dropped, and affected users must re-initiate connections to resources.

Performance may be affected, since fewer connectors are available to handle traffic.

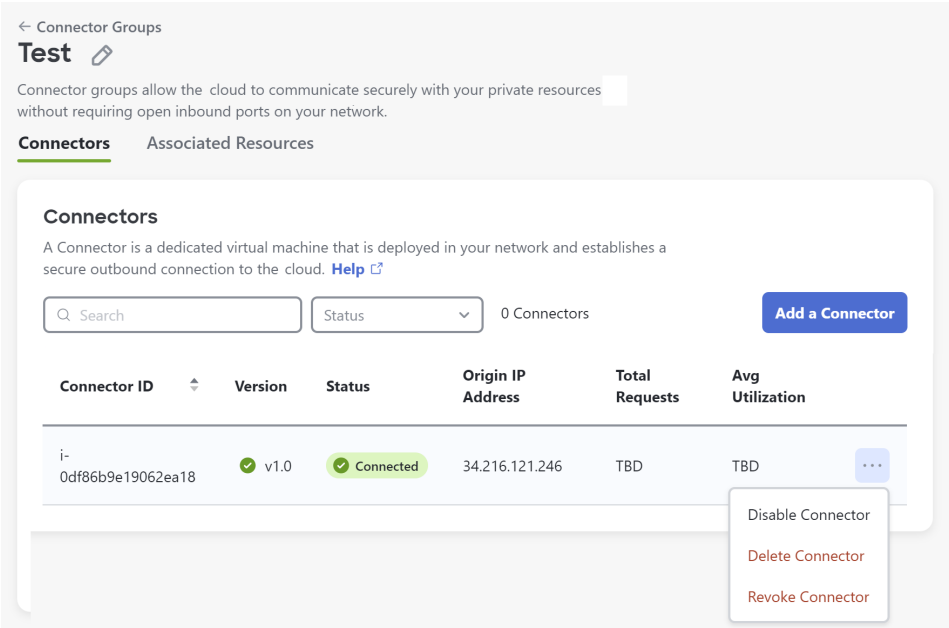
Deleting connectors does not delete deployed connector instances. To delete connector instances, see the documentation for your virtual environment.

Disable, Revoke, or Delete a Connector

Describes Disable, Revoke, or Delete a Connector in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To disable, revoke, or delete connectors:

1. Navigate to **Connect > Network Connections**.
2. Click **Connector Groups**.
3. If you see **Next Steps** at the top of the page, scroll down to the **Connector Groups** section.
4. Click the name of the relevant connector group.
5. Click the **Connectors** tab.
6. If you are deleting or revoking a connector, and you have not yet deleted the connector instance deployed in your data center, make a note of the Connector ID that you will delete or revoke.
7. In the table row for the applicable connector, click the ellipsis button […] and choose an option.



8. Read the confirmation dialog carefully and respond.
9. If you deleted or revoked a connector, delete the corresponding connector instance deployed in your data center.

   To delete a connector instance, see the documentation for your virtual environment.

Disable or Delete a Resource Connector Group

Describes Disable or Delete a Resource Connector Group in Cisco Secure Access. Disabling or deleting a connector group may impact users who are currently connected to a resource, as well as future connectivity.

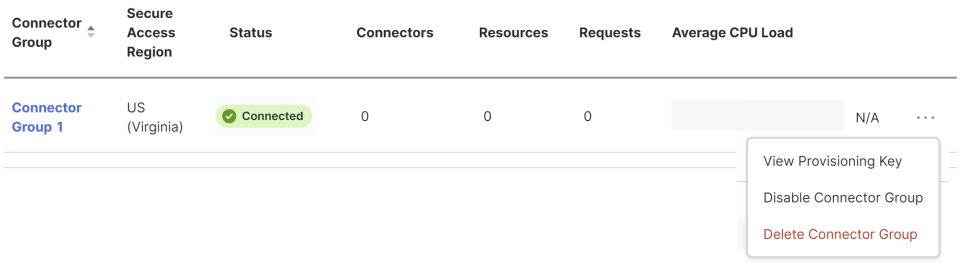
Disabling or deleting a connector group may impact users who are currently connected to a resource, as well as future connectivity.

If you delete a connector group, all connectors belonging to the group become permanently unusable. Deleting a connector group cannot be undone.

Proceed with caution.

To disable or delete a connector group:

1. Navigate to **Connect > Network Connections**.
2. Click **Connector Groups**.
3. If you see **Next Steps** at the top of the page, scroll down to the **Connector Groups** section.
4. In the table, locate the connector group to modify.
5. If you are deleting a connector group, and you have not yet deleted the associated connector instances deployed on your network, identify the connectors associated with the group so you know which connectors to delete:
   a. Click the name of the connector group in the list.
   b. Make a note of the Connector IDs in the table on the Connectors tab.
   c. Navigate back to the list of connector groups.
6. Click the ellipsis button [...] at the end of the table row for the relevant group and choose an option:



7. Follow instructions on the screen.
8. If you deleted a connector group, delete all connector instances deployed in your data center that are associated with this group. To delete a connector instance, see the documentation for your virtual environment.

Maintain and Monitor Resource Connectors and Connector Groups

Understand how to prevent, identify, and address issues with resource connectors and connector groups.

Maintain and monitor resource connectors and groups to prevent, identify, and address issues.

About Resource Connector Software Updates

Secure Access manages the updates of the Secure Access software on the connectors in your organization using over-the-air (OTA) updates.

If the connector software has not reached last date of support (LDOS), Secure Access upgrades the connector automatically.

To avoid impacting the private resources supported by the connector, Secure Access updates only one connector in a group at a time. Secure Access checks for software updates daily on each resource connector deployed in the organization.

About Connector OS Updates

Secure Access does not upgrade the operating system (OS) on the resource connectors deployed in your environment automatically.

An organization must deploy new resource connectors with the latest version of the OS in the connector image and delete the connectors with the outdated connector image.

- When security vulnerabilities are reported to Cisco, Secure Access publishes an updated connector image.

  For information about OS vulnerabilities addressed in a specific connector image, see Secure Access Release Notes for Resource Connectors.

- New versions of the connector image will have the latest operating system version. Secure Access may also periodically issue connectors with the latest operating system even if there are no other changes.

About Last Date of Support for Connector Images

Secure Access supports a connector software version for up to six months. After six months, Secure Access sets the status of the connector software to last day of support (LDOS).

Secure Access supports a connector OS for up to one year. After one year, Secure Access sets the status of the connector OS to LDOS.

To ensure that Secure Access continues to support the connectors in the organization, deploy a new connector in the environment:

1. Obtain the new connector image. For more information, see Obtain the Connector Image.
2. Deploy the new connector image provided by Cisco. For more information, see Add Connectors to a Connector Group.

3. Delete the connector image in Secure Access. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.

Comparison of Connector Software Upgrades and OS Upgrades

For VM-based resource connectors:

Secure Access delivers software upgrades automatically as long as the connector software is not at LDOS.

However, there is no automatic upgrade mechanism for the OS. When the OS reaches LDOS, the organization must manually upgrade. Delete the resource connector and then deploy a new resource connector instance with the latest OS.

Importantly, connectors running on unsupported OS versions will not receive software updates. Ongoing monitoring is required to ensure both software and OS remain supported.

For container-based resource connectors:

Secure Access delivers software upgrades automatically as long as the connector software is not at LDOS.

Both the connector software and the container OS software are upgraded together as part of the automatic upgrade.

Organizations are required to manage and update the host OS independently. Ongoing monitoring is required to ensure both the connector and container software remain supported.

Managing Certificate Renewals on the Connector

Secure Access updates the certificate for a resource connector automatically. However, if a resource connector is shutdown during the two week period prior to the expiration of the connector's certificate, Secure Access cannot renew the connector's certificate.

Once the certificate expires on the connector, you must redeploy the connector. For more information, see Monitor Connector Status.

Monitor Connector Group Status

Describes Monitor Connector Group Status in Cisco Secure Access. Check the Connectivity section on the Overview page for status and health of your connector groups.

Check Connector Group Status on the Overview Page

Check the **Connectivity** section on the **Overview** page for status and health of your connector groups. Click a status tile to see the connector groups that are experiencing the problem.

Status	Status Message	Recommendations
Disconnected	Click the **Disconnected** tile to see which connector groups have this problem, then click a connector group to see which connectors are problematic.	For more information, see Troubleshoot Resource Connectors and Connector Groups
Warning	This indicates that users have failed to reach resources in at least one connector group. Click the **Warning** tile to see which connector groups have this problem, then click a connector group to see which connectors are problematic.	For more information, see Troubleshoot Resource Connectors and Connector Groups

Status	Status Message	Recommendations
Overloaded CPU	Click the **Warning** tile to see which connector groups have CPU loads over 70%.	If this situation continues, increase connector group capacity as needed by deploying additional connectors in the group. For more information, see Add Connectors to a Connector Group.

Check Connector Group Status on the Connector Groups Page

On the connector group listing page, scroll down to the table of connector groups and check the Status column. If any of the connectors in a group have connectivity issues that affect end user connectivity to resources, Secure Access displays a warning. Click a connector group to see the connectors that are showing warnings. For more information, see Monitor Connector Status.

Status	Description	Action Required
Connected	At least one connector in the group is connecting user traffic to private resources, and the connectors are not overloaded.	None
Overloaded	The running average CPU load of all connectors in the group is above the recommended threshold (70% usage.)	Deploy additional connectors in the group. Be sure to use the current provisioning key shown for the connector. For more information, see Add Connectors to a Connector Group.
Disabled	The connector group or all connectors in a group have been intentionally disabled by an administrator and are not forwarding traffic to resources.	If you want to re-enable connectors or connector groups, click the ellipsis menu at the end of the applicable table row.
Unestablished	The connector group is not yet fully set up.	Add at least one connector and one private resource to the group. For more information, see Add Connectors to a Connector Group and Assign Private Resources to a Connector Group as applicable.
Disconnected	All connectors in the group are disconnected. The connector group is not forwarding any traffic to private resources.	For more information, see Troubleshoot Resource Connectors and Connector Groups.

View Connector Groups in Secure Access

Provides instructions for completing the View Connector Groups in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View the name, Secure Access region, status, number of connectors, number of resources, number of requests, and average CPU load for the resource connector groups in the organization.

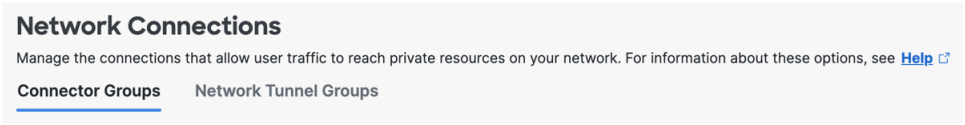
Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

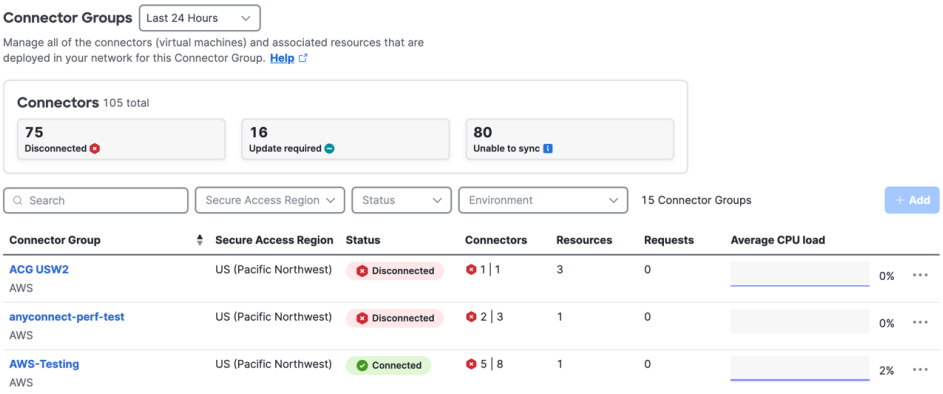
Procedure

Navigate to **Connect** > **Network Connections**, and then click **Connector Groups**.

Secure Access displays the details about each connector group in the organization.



- **Connector Group**–The unique identifier of the connector group.
- **Secure Access Region**–The label for the Secure Access region where the connectors in the connector group are deployed.
- **Status**–The basic diagnostic information about the connector group.
- **Connectors**–The number of resource connectors in the connector group.
- **Resources**–The number of resources supported by the connector group.
- **Requests**–The number of requests sent to the connectors in the connector group.
- **Average CPU Load**–The graph of the average CPU load on the connector group.



View Connectors in Secure Access

View the status, notification details, and CPU load for the resource connectors deployed in the organization.

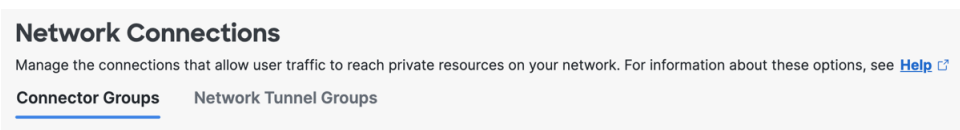
View the status and notification details for the resource connectors deployed in the organization.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

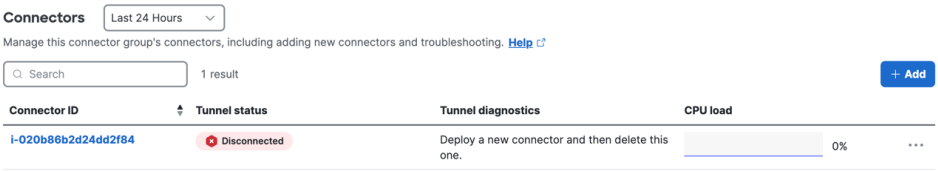
1. Navigate to **Connect** > **Network Connections**.



2. On **Connector Groups**, navigate to the **Connector Groups** table and then click on the name of a connector group.



3. On **Connectors**, navigate to the **Connectors** table.
   - **Connector ID**–The unique identifier of the connector.
   - **Tunnel status**–The descriptive label for the status of the connector tunnel.
   - **Tunnel diagnostics**–The basic diagnostic information about the connector.
   - **CPU load**–The graph of the CPU load on the connector.



Monitor Connector Status

Describes Monitor Connector Status in Cisco Secure Access. Secure Access provides notifications about the status of the resource connectors deployed in the organization.

Secure Access provides notifications about the status of the resource connectors deployed in the organization.

A connector's status consists of various states and a notification for each state. The value of the notification depends on the conditions detected on the resource connector.

A resource connector that has not been confirmed in Secure Access is either in the **announced** or **reachable** state. You can use the Secure Access Resource Connector and Connector Groups API to view the status of a resource connector in the **announced** or **reachable** state. For more information about confirming the deployment of a resource connector in Secure Access, see Step 2 - Confirm Connectors.

Tunnel Status

For each resource connector, Secure Access provides the state and information about the connectivity on the connector tunnel.

Status Label	Status Description	Example Status Message	Action Required
Connected	The connector is sending user traffic to private resources as expected.	Connected Last update on Oct 8, 2025, at 2:34 AM UTC	None
Disconnected	The connector is no longer sending user traffic to private resources.	Disconnected Last update on Oct 8, 2025, at 2:34 AM UTC	Run diagnostics to identify the issue. If problems persist, contact Support.

Status Label	Status Description	Example Status Message	Action Required
Disabled	An administrator has disabled this connector intentionally.	Disabled Last update on Oct 8, 2025, at 2:34 AM UTC	Re-enable the connector in Secure Access. For more information, see Enable a Connector in Secure Access
Connected warning	The connector is sending user traffic to private resources as expected. Secure Access detects a condition on the resource connector.	Connected warning Last update on Oct 8, 2025, at 2:34 AM UTC	Check the summary of the connector status and the diagnostic information provided at the top of the page.

Certificate Status

For each resource connector, Secure Access provides the state and information about the certificate used for securing communications with the connector.

Status Label	Status Description	Example Status Message	Action Required
Expired	The certificate for the resource connector expired.	Expired This connector's certificate expired Oct 8, 2025.	Deploy a new resource connector.
Expiring soon	The connector's certificate will expire within ten days from the current date.	Expiring soon This connector's certificate will expire on Oct 8, 2025.	Deploy a new resource connector.
Valid	The certificate is valid and will remain valid for more than ten days from the current date.	Valid This connector's certificate will expire on Oct 8, 2025.	None
Not synced	Secure Access is unable to sync with the connector. Secure Access was unable to sync with the connector for the last three days and 15 minutes from the current date.	Not synced Expiry date is Oct 8, 2025. Data may be out-of-date.	Check your firewall settings.
Unknown	Secure Access is unable to sync with the connector. No information is available for the last three days.	Unknown Connector has not synced in 3 days or more.	Check your firewall settings.
Unknown (may be expired)	Secure Access is unable to sync with the connector for the last three days. The connector expiration date has passed.	Unknown (may be expired) Connector has not synced in 3 days or more.	Check your firewall settings and run diagnostics.

Configuration Status

For each resource connector, Secure Access provides the state and information about the tunnel configuration.

Status Label	Status Description	Example Status Message	Action Required
Synced	Secure Access synced with the connector and obtained the tunnel configuration.	Synced	None
Not synced	Secure Access cannot sync with the connector and did not get the latest tunnel configuration.	Not synced Cannot retrieve the DNS configurations or status of the tunnel configuration. Check your firewall settings.	Check your firewall settings.

OS Version Status and Connector Software Version Status

For each resource connector, Secure Access provides the state and information about the connector software version and the OS version of the connector image.

A connector status may apply to the connector software version, the OS version of the connector image, or both versions.

Status Label	Status Description	Example Status Message	Action Required
Vulnerable OS version	The OS version of the connector image has vulnerabilities.	Vulnerable 2402180000 (latest 2505200000) This OS version presents vulnerabilities. Delete this connector and deploy a new one using the latest image.	Delete this connector and deploy a new one using the latest connector image.
Vulnerable Connector software version	The connector software version has vulnerabilities.	Vulnerable v2.0.60 (latest v2.0.90) This connector version presents vulnerabilities. Delete this connector and deploy a new one using the latest image.	Delete this connector and deploy a new one using the latest connector image.
Not supported Connector software version	The connector software has not been updated in the last six months.	Not supported v2.0.60 (latest v2.0.90) This connector version is not supported. Delete this connector and deploy a new one using the latest image.	Delete this connector and deploy a new one using the latest version of the connector image.

Status Label	Status Description	Example Status Message	Action Required
Not supported OS version	This OS version of the connector image is not supported and has not been updated in over a year.	Not supported 2410180000 (latest 2505200000) This OS version is not supported. Delete this connector and deploy a new one using the latest image.	Delete this connector and deploy a new one using the latest image.
Update failed Connector software version only	The software update for this connector failed.	Update failed v2.0.60 (latest v2.0.90) Connector update failed. Delete and replace it or run diagnostics.	Verify that your firewall rules allow for outbound traffic. Secure Access will automatically retry the update.
Not synced Connector software version OS version	Secure Access was unable to sync with the connector for the last three days and 15 minutes from the current date.	Not synced v2.0.60 (latest v2.0.90) Data may be out of date. Cannot retrieve data.	Check your firewall settings and run diagnostics.
Unknown Connector software version OS version	Secure Access cannot sync with the connector for the last three days.	Not synced v2.0.60 (latest v2.0.90) Data may be out-of-date.	Check your firewall settings and run diagnostics.
Outdated Connector software version	Firewall settings may have blocked Secure Access from updating the connector software, or the connector was not available when the update was scheduled to occur.	Outdated v2.0.60 (latest v2.0.90) Automatic connector updates occur daily during off-hours. This connector will be updated automatically during the next update period.	If a connector is offline during an update or deployed later, its version will be listed as outdated. To resolve this condition, wait for the next automatic update or deploy a new connector using the latest image.
Outdated OS version	The latest version of the OS is no longer supported.	Outdated 2505200000 This connector's OS is outdated. It is operational, but will be unsupported in 30 days. Delete and replace it before that date.	Delete this connector and deploy a new one using the latest connector image.
Updating Connector software version only	Secure Access is updating the connector.	Updating v2.0.60 (latest v2.0.90) Automatic update in progress.	None

Status Label	Status Description	Example Status Message	Action Required
Up-to-date Connector software version OS version	The latest version of the connector software or OS version is installed on the connector.	Up-to-date 2505200000	None

View a Connector's Status

View the status and notification details for a resource connector deployed in the organization.

View the status and notification details for a resource connector deployed in the organization.

Secure Access provides detailed state information for a connector in the **Connector Status**.

A connector's status consists of these states:

- **Tunnel status**
- **Certificate status**
- **Configuration status**
- **Connector IP address**
- **Connector version**
- **Added**
- **OS version**

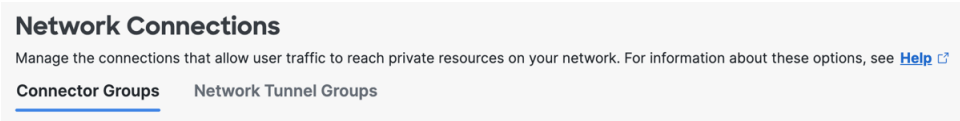
Each status has a label and a notification. A notification varies depending on the conditions detected on the resource connector.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

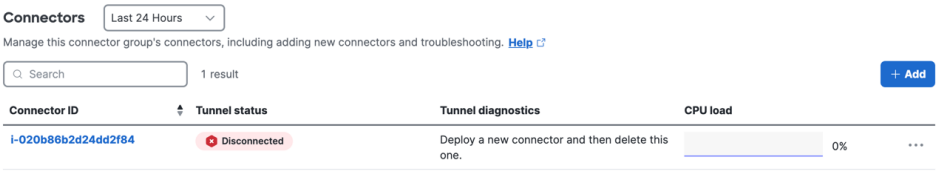
1. Navigate to **Connect** > **Network Connections**.



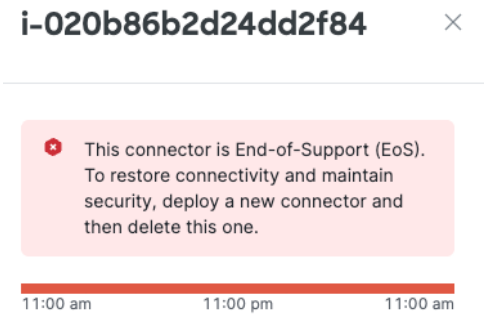
2. On **Connector Groups**, navigate to the **Connector Groups** table and then click on the name of a connector group.



3. On **Connectors**, navigate to the **Connectors** table.

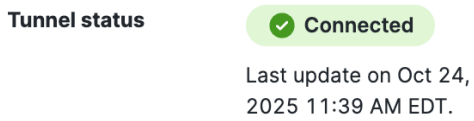


4. Navigate to the **Connector ID** column and then click on the ID of a resource connector.
   - At the top of the page, Secure Access displays the connector ID.
   - If error conditions are detected on the connector, Secure Access provides a summary of the connector status during the last 24 hours and recommended steps to resolve the error conditions.

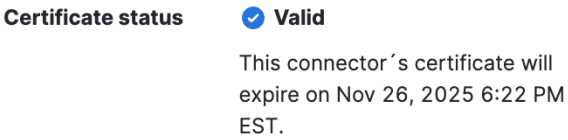


5. Navigate to **Connector status**.

   Tunnel status–The state of the tunnel on the connector and the last date when Secure Access synced with the tunnel.



   Certificate status–The state of the certificate that is associated with the connector and the expiry date of the certificate.



   Configuration status–The state of the tunnel configuration associated with the connector and the date when Secure Access last synced with the resource connector.



   Connector IP address–The IP address of the resource connector.



   Connector version–The state of the connector software and the latest version of the software deployed on the connector.



Added–The date when the connector first registered with Secure Access.

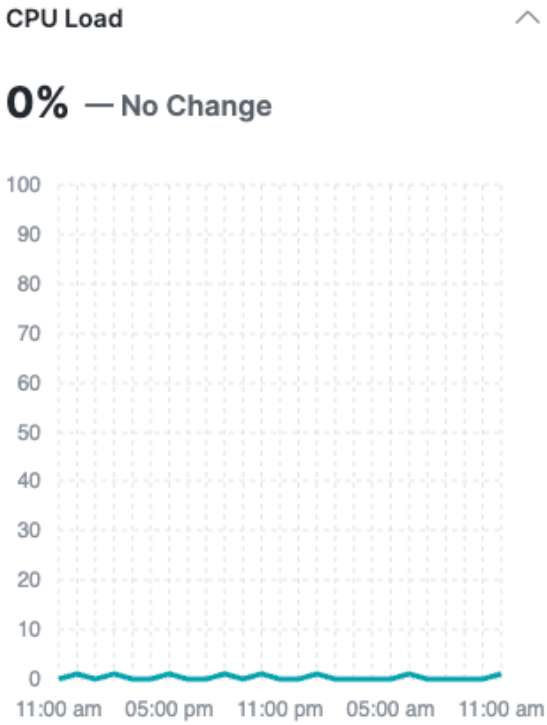


OS version–The state of the base operating system (OS) of the connector image and the latest version of the OS.



6. Navigate to **CPU load**.

   A graph of the CPU load on the connector for the last 24 hours.



Enable a Connector in Secure Access

Enable a connector in Secure Access.

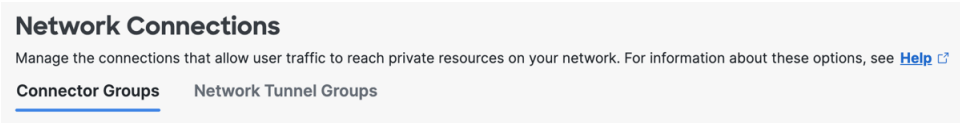
If a connector is disabled, you can re-enable it in the Secure Access organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

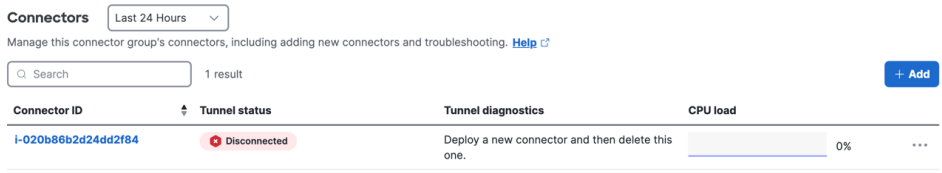
1. Navigate to **Connect** > **Network Connections**.



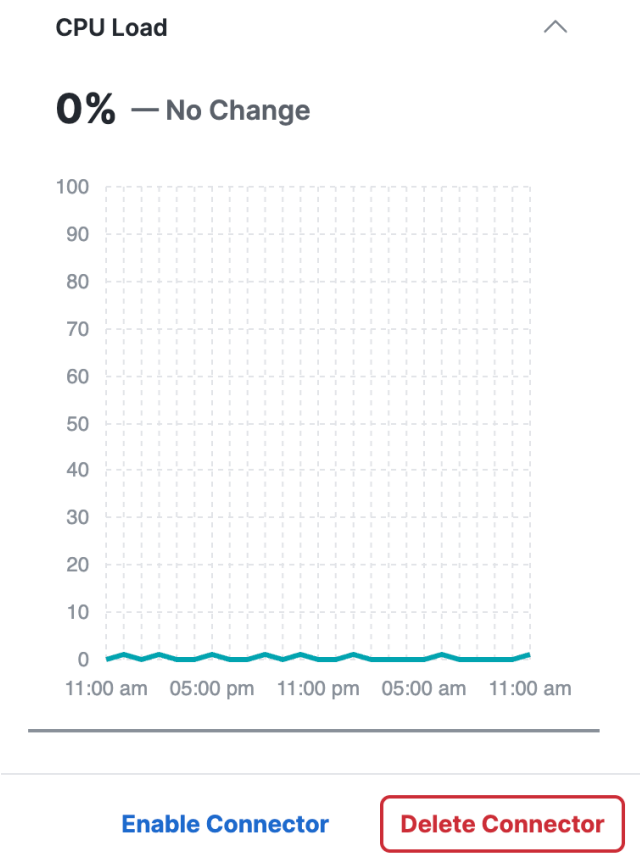
2. On **Connector Groups**, navigate to the **Connector Groups** table, and then click on the name of a connector group.



3. On **Connectors**, navigate to the **Connectors** table.



4. Navigate to the **Connector ID** column, and then click on the ID of a resource connector.
5. Navigate to the bottom of the page after **CPU load** and click **Enable Connector**.



6. Click **Enable**.
   Secure Access enables the connector and the connector begins to send traffic to the private resources.

Increase Connector Group Capacity

Describes Increase Connector Group Capacity in Cisco Secure Access. In order to accommodate traffic volume, you may need to add connectors to a connector group.

In order to accommodate traffic volume, you may need to add connectors to a connector group. To check connector group capacity utilization, navigate to the Overview page and look at the Connectivity section. If you see **Overloaded CPU**, especially if this status continues over time, consider adding more connectors.

For more information, see Add Connectors to a Connector Group.

Check Connector CPU Load

Describes Check Connector CPU Load in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

1. Navigate to **Connect > Network Connections > Connector Groups**.
2. Locate the connector group of interest.
3. Check the **Average CPU load** column. If you see **Incomplete data** or a break in the line, this indicates that at least one connector was not fully active during the entire time period, because it was newly deployed, experiencing connectivity issues, or unable to communicate with the Secure Access cloud.
4. If the average load is unexpectedly high, click the connector group name and look at the **CPU Load** column for individual connectors to look for problems.

Schedule Upgrade Windows or Delay for a Connector Group

When updated software for a resource connector is available, configure an upgrade window to determine when that upgrade will occur.

Secure Access updates the software on the Resource Connectors in a Connector Group that are deployed in an organization periodically. Administrators can choose to schedule when upgrades occur for the Connector Group by configuring upgrade windows. Otherwise, Secure Access schedules any upgrades automatically on any day of the week. Administrators can configure a date to delay the upgrades for the Connector Group. The calendar enforces the latest allowed resume date shown in the **Delay upgrade windows** dialog.

> **Note**
>
> These upgrade and delay settings apply only to resource connector software updates and do not include operating system updates for the connector host.

Configuring Upgrade Windows on Connector Groups

To configure when an upgrade occurs, add a single upgrade window or a series of upgrade windows for a Connector Group in your organization. An upgrade window controls the day and time period when Secure Access updates the Resource Connectors in a Connector Group.

> **Note**
>
> You can add a total of 10 upgrade windows for a Connector Group.

Secure Access will use any upgrade windows that you configure to schedule the updates to the connectors in the Connector Group. For each upgrade window, configure the day of the week, start time, and duration. You must choose a time period for the upgrade window that is between one and 24 hours.

For information about setting up upgrade windows, see Add Upgrade Windows for a Connector Group.

Configuring a Delay of Upgrades on Connectors in a Connector Group

To delay the software updates on the Resource Connectors in a Connector Group, configure the date after which Secure Access will schedule the updates. The date that you can choose is between the current date and the time period determined by Secure Access for the updates. For information about setting up a delay, see Add Delay of Upgrades for a Connector Group.

Add Upgrade Windows for a Connector Group

This topic describes how to add upgrade windows to schedule software updates for resource connectors within a connector group.

Add upgrade windows for a connector group to control when Secure Access updates your resource connectors. The duration for each upgrade window must be between one and 24 hours.

> **Note**
>
> You can add 10 upgrade windows for a Connector Group in the organization.

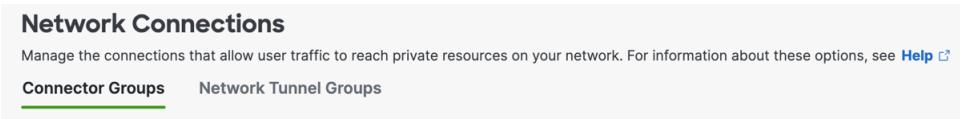
For more information, see Schedule Upgrade Windows or Delay for a Connector Group.

Before you begin

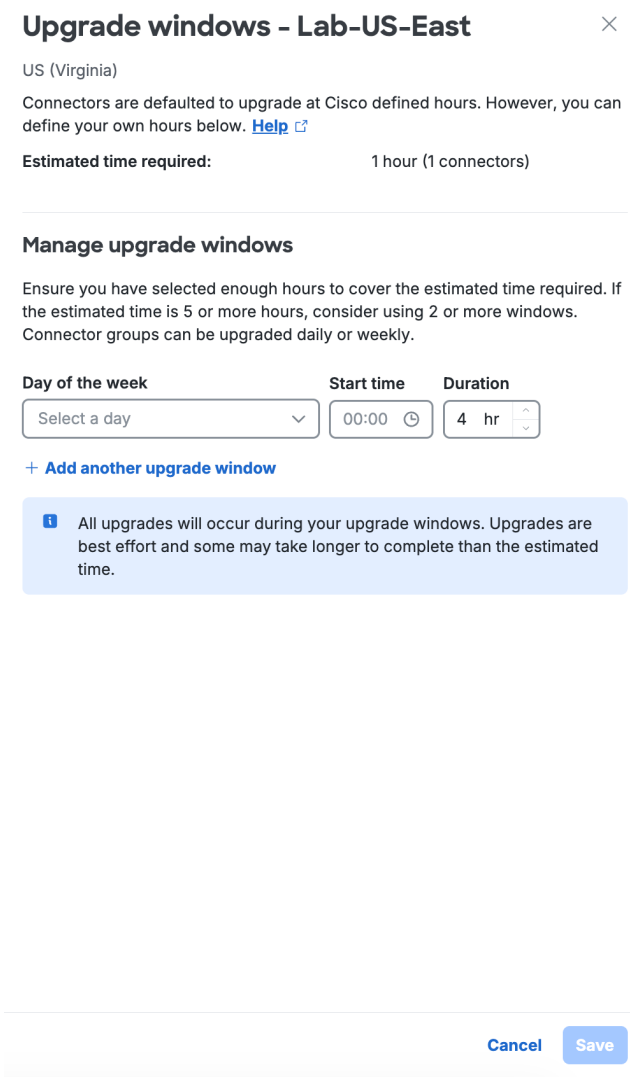
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.



2. Locate a Connector Group in the table, click the ellipsis (**...**) icon at the end of the row, and choose **Manage upgrade windows**.



3. Review the region name and the estimated time required to complete the upgrades on the connectors in the connector group.

> **Note**
>
> If the estimated time is 5 or more hours, consider using 2 or more upgrade windows.

4. Configure the upgrade window:
   a) For **Day of the week**, choose **Daily** or a specific day.
   b) For **Start time**, choose the hour and minutes during the 24 hour period to begin the upgrade.
   c) For **Duration**, choose the number of hours after the start time for the upgrade. You must choose a duration between one and 24 hours.
5. (Optional) Click **+ Add another upgrade window** to configure another upgrade window.
6. (Optional) Click the trashcan icon (delete) to remove an upgrade window.
7. Click **Save**.

Add Delay of Upgrades for a Connector Group

This topic describes how to delay software updates for resource connectors within a connector group.

You can delay software updates for resource connectors in a connector group. Secure Access uses your configured upgrade windows to schedule updates after the delay period. The calendar enforces the latest allowed resume date shown in the **Delay upgrade windows** dialog.

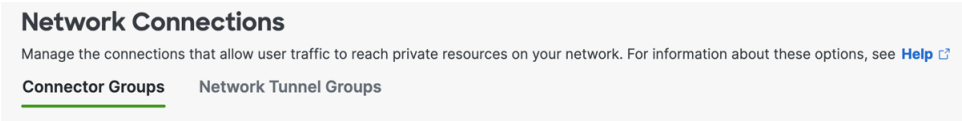
For more information, see Schedule Upgrade Windows or Delay for a Connector Group.

Before you begin

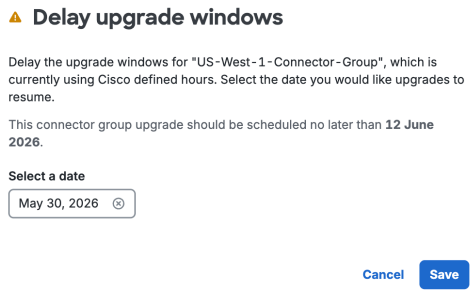
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Network Connections** > **Connector Groups**.

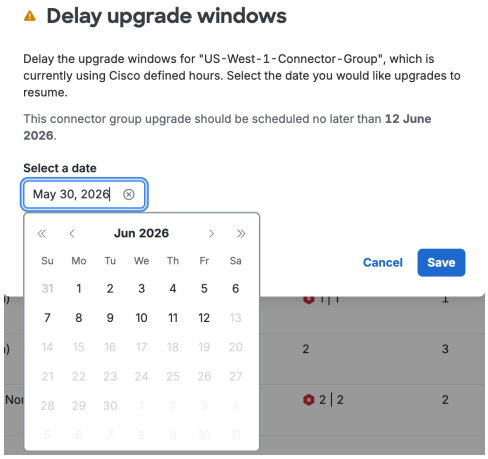


2. Locate the connector group in the table, click the ellipsis (**...**) icon at the end of the row, and choose **Delay upgrade windows**.



3. In the **Select a date** field, click the date to open the calendar and select the date when you want upgrades to resume.

   The calendar enforces the latest allowed resume date shown in the dialog.



> **Note**
>
> The delay date represents the beginning of the period when the upgrade can start. For example, if your upgrade schedule is May 30 at 01:00 UTC and you select May 31, the next upgrade starts at 01:00 UTC on May 31.

4. Click **Save**.

Troubleshoot Resource Connectors and Connector Groups

Troubleshooting information for common issues that can occur with resource connectors and connector groups.

If you encounter issues with your deployed Cisco Secure Access Resource Connectors, follow the instructions to troubleshoot before calling Cisco Support. You can run the diagnostic commands in the Connector Diagnostics command-line interface (CLI) or the troubleshooting tools for containers to get the status of a resource connector.

About Resource Connector Issues

Resource Connectors may be exchanging traffic successfully but not communicating otherwise with Secure Access.

This can cause problems with automatic software updates, monitoring connector health, gathering metrics, and deleting or revoking a connector, including automatically deleting inactive connectors.

These issues are typically temporary and self-repairing.

- If they are not, first try restarting the connector instance.
- If the issues continue, you can run diagnostics on the connector to troubleshoot these issues. For more information, see Connector Diagnostics (CLI) and Connector Troubleshooting Tools.

General Troubleshooting

If you see issues with the resource connectors or resource connector groups that are deployed, try the following:

- Check the **Connectivity** section on the **Overview** in Secure Access.

  The Secure Access **Overview** provides a high-level view of the status of your organization's configured connectors and connector groups. For more information, see Secure Access Overview Dashboard.

- Check the Connector Groups page for issues.

  Navigate to > **Connect** > **Network Connections** > **Connector Groups** and look at the **Status** column for the applicable connector group.

- Check **Monitor > Activity Search** for logged events related to connectors.
- Determine whether the issue affects a single connector or all connectors in the group.

  If the issue affects only one connector, you can delete the connector and deploy a new one.

- Check for a Secure Access service outage. For more information, see Secure Access Status Portal.
- Temporarily disable a connector, then enable the connector again as appropriate.
- Run diagnostics on a resource connector that is deployed with virtual machines. For more information, see Connector Diagnostics (CLI).

- Run diagnostics on a resource connector that is deployed in a container. For more information, see Connector Troubleshooting Tools.

> **Note**
>
> Some troubleshooting guidance outside of this document may refer to connectors as "agents", "app connectors", or "application connectors".

Throughput Capacity is Less Than Expected

Describes Throughput Capacity is Less Than Expected in Cisco Secure Access. Ensure that connectors are using DTLS and not TLS.

- Ensure that connectors are using DTLS and not TLS.
- Run diagnostics on the connector and look for Protocol in the output. For more information, see Connector Diagnostics (CLI) and Connector Troubleshooting Tools.
- If the protocol shows TLS, check the following:
  - DTLS and TLS connections must originate from the same IP address.
  - The egress firewall must allow UDP connections on port 443.
  - The connector is the required instance type. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.
  - In the connector instance, **Auto-Assign Public IP** must be enabled.
- If you make changes, reboot the instance.

> **Note**
>
> If you are using Standard_D4as_v5 instance type and intend to enable Accelerated Networking, rebooting does not push changes. Enable **Accelerated Networking** on the connector VM's network interface. In the Azure portal, select **Enable accelerated networking** on the **Networking** tab when you create the VM. Accelerated Networking improves network throughput and reduces CPU load on the connector. To enable it on an existing connector VM:
>
> 1. Stop the VM so that its status is **Stopped**. Restarting the VM is not enough.
> 2. Open the VM's network interface, then enable **Accelerated networking**.
> 3. Start the VM. You can confirm the setting with the Azure CLI: `az network nic show -g <resource-group> -n <nic-name> --query enableAcceleratedNetworking`. The output is `true` when Accelerated Networking is enabled.

Users Cannot Connect to Private Resources

Describes Users Cannot Connect to Private Resources in Cisco Secure Access. Ensure that you have assigned the resource to the applicable connector group.

- Ensure that you have assigned the resource to the applicable connector group. For more information, see Assign Private Resources to a Connector Group.
- Verify that all connectors in the group can reach the resource.
- Check the status of the connector group that the resource is associated with: Navigate to **Connect** > **Network Connections** > **Connector Groups** and look at the **Status** column for the applicable connector group.
- For causes of user connectivity issues that are not specifically related to resource connectors, see Troubleshoot Private Access Rules.

Connector Software Auto-Upgrades

Describes Connector Software Auto-Upgrades in Cisco Secure Access. For general information about over-the-air (OTA) connector updates, see Maintain and Monitor Resource Connectors and Connector Groups.

For general information about over-the-air (OTA) connector updates, see Maintain and Monitor Resource Connectors and Connector Groups.

Troubleshooting Connector Software Updates

- If the upgrade fails for a single connector, Secure Access does not update the software on the other connectors in the connector group.

  Try deleting the connector instance and then deploy a new connector. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.

  Secure Access automatically retries updates on all connectors. The upgrade problem may be temporary and self-repairing.

- The network requirements for traffic on resource connectors may change. We recommend that you review the your organization's firewall or access control list periodically. For information about the network requirements for Resource Connectors, see Allow Resource Connector Traffic to Secure Access.

- If the upgrade of the connector continues to fail, check for problems with your network or the deployed connector instances.

  Run diagnostics on the connector. For more information, see Connector Diagnostics (CLI) and Connector Troubleshooting Tools.

Connector Operating System (OS) Version has Security Vulnerabilities

Describes Connector Operating System (OS) Version has Security Vulnerabilities in Cisco Secure Access. Secure Access shows connector version issues in a list of connectors with a yellow icon (Yellow icon: Connector version issue).

Secure Access shows connector version issues in a list of connectors with a yellow icon (). Hover over the icon to identify the problem.

If you see a yellow icon for a connector version on the connector group's list of connectors, the connector operating system (OS) may have vulnerabilities. To determine whether this is the case, hover over the status icon. If OS vulnerabilities have been reported, you should replace the affected connectors.

For more information, see Maintain and Monitor Resource Connectors and Connector Groups.

Manage Access Control and Vulnerabilities for Containers

- The organization's administrators are responsible for the management of vulnerabilities and access control on the host or virtual machine.

Connector is Expired

Describes Connector is Expired in Cisco Secure Access. To ensure the integrity of your deployed connectors, Secure Access validates each connector during the connector's renewal period.

To ensure the integrity of your deployed connectors, Secure Access validates each connector during the connector's renewal period. The renewal period spans several weeks where Secure Access checks the status of a deployed connector. Toward the end of the renewal period if the connector's state is not valid, Secure Access disconnects the resource connector and the connector expires.

Check the Status of Your Connector

We recommend that you log into a deployed resource connector periodically and check the status of the connector.

1. Log in to the virtual machine for the resource connector.
2. In the connector's diagnostic output, locate **sse_cloud**, and then review the resource connector's diagnostic information.

If your resource connectors expire frequently, we recommend that you review the prerequisites for deploying resource connectors in your environment. For more information, see Requirements and Prerequisites for Resource Connectors and Connector Groups.

(VMware Only) View Connector Diagnostic Information

The resource connector console on VMware displays diagnostic information before the resource connector is shutdown.

For example:

```
systemd-shutdown\[1\]\: Failed to acquire terminal, using /dev/null
stdin/stdout/stderr instead: Input/output error
```

Check for an Expired Connector in Secure Access

1. Navigate to **Connect > Network Connections > Connector Groups**.
2. Locate the Connector Group table and click on a Connector Group.
3. Locate the connector and confirm that its **Status** is `Expired`.

Clean Up an Expired Connector

1. Delete the expired connector instance from your virtual environment.
2. Delete the expired connector from the connector group in Secure Access. For more information, see Disable, Revoke, or Delete Resource Connectors and Groups.
3. If needed, deploy a new connector. For more information, see Add Connectors to a Connector Group.

Delete the Connector Container

For information about removing the connector container, see Delete the Container.

Stop a Connector

Describes Stop a Connector in Cisco Secure Access. If you need to stop a Resource Connector for any reason, power it off from within the deployment environment (for example: AWS, VMware, Azure).

If you need to stop a Resource Connector for any reason, power it off from within the deployment environment (for example: AWS, VMware, Azure).

Stop the Connector Container

For information about stopping the connector container, see Deploy a Connector in Docker-Stop Container.

Unable to Revoke or Delete a Connector

Describes Unable to Revoke or Delete a Connector in Cisco Secure Access. This includes the inability of Secure Access to automatically delete an inactive resource connector.

This includes the inability of Secure Access to automatically delete an inactive resource connector.

This situation is likely to be temporary and self-repairing, and can occur even if the connector is still passing traffic to private resources. If the problem does not resolve itself, run diagnostics on the resource connector. For more information, see Connector Diagnostics (CLI).

Unable to Sync

Describes Unable to Sync in Cisco Secure Access. An unable to sync error condition indicates that the resource connector can not connect to the Secure Access Controller component.

An unable to sync error condition indicates that the resource connector can not connect to the Secure Access Controller component.

When a resource connector is unable to sync, Secure Access does not:

- Display the metrics for the resource connector.
- Update the configuration for the resource connector.
- Perform over-the-air upgrades on the resource connector.

To troubleshoot the error condition, run the Command-line Interface (CLI) diagnostic tool to check the internet connectivity on the Controller. Also ensure that the firewall rules in the organization's environment allow the resource connector to make outbound connections to the Controller. For more information, see Allow Resource Connector Traffic to Secure Access.

If the error condition persists, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Connector-Related Status Graphs are not Current

Describes Connector-Related Status Graphs are not Current in Cisco Secure Access. For example, the CPU Load chart does not have current data, or the graphs that you see when you click a connector ID in the list of connectors in a group are not up to date.

For example, the CPU Load chart does not have current data, or the graphs that you see when you click a connector ID in the list of connectors in a group are not up to date.

This situation is likely to be temporary and self-repairing, and can occur even if the connector is still passing traffic to private resources. If the problem does not resolve itself, we recommend that you get the diagnostic information about the resource connector. For more information, see Connector Diagnostics (CLI) and Connector Troubleshooting Tools.

(Container Only) Connector Troubleshooting Tools

Describes (Container Only) Connector Troubleshooting Tools in Cisco Secure Access. To troubleshoot connector issues that cannot be resolved by restarting or redeploying the connector instance, run the Secure Access troubleshooting scripts on the container and connector instance.

To troubleshoot connector issues that cannot be resolved by restarting or redeploying the connector instance, run the Secure Access troubleshooting scripts on the container and connector instance.

To understand the results of the **diagnostic** command, see Diagnostic Codes.

Supported Standard Linux Troubleshooting Commands

You can use these Linux commands to provide information about a resource connector instance:

- **ping**
- **nslookup**
- **traceroute**

- **tcptraceroute**
- **netstat**
- **free**
- **df**
- **vmstat**
- **iostat**
- **mpstat**
- **reboot**
- **uptime**
- **date**
- **clear**

Run Diagnostic or Techsupport Scripts

For more information, see Run Diagnostic and Techsupport Scripts.

The **diagnostic** script runs a series of ping and DNS tests on the local IP address, gateway, Secure Access APIs, and headend IP addresses. The script also checks connectivity on HTTPS ports to various Secure Access endpoints, along with system artifacts created through the connector instance provisioning process.

> **Note**
>
> The diagnostic ping tests provide additional network troubleshooting information. The diagnostic output may report a ping failure reaching the Secure Access hosts, which does not indicate network connectivity issues with the resource connector.

The **techsupport** script provides information about the resource connector:

- Version of the resource connector software.
- VPN tunnel state and related information.
- System monitoring metrics, such as disk and memory statistics.
- Information snapshot of the connector host, from DNS to Network interface details, iptables, routes, sysctl system settings, and monitoring information.
- Recent periodic resource connector software logs.

Troubleshoot Container Deployments

For more information, see Troubleshoot Container Deployments.

(VM Only) Connector Diagnostics (CLI)

Describes (VM Only) Connector Diagnostics (CLI) in Cisco Secure Access. To troubleshoot connector issues that cannot be resolved by restarting or redeploying the connector instance, run diagnostic commands on the connector instance.

To troubleshoot connector issues that cannot be resolved by restarting or redeploying the connector instance, run diagnostic commands on the connector instance.

> **Note**
>
> The diagnostic ping tests provide additional network troubleshooting information. The diagnostic output may report a ping failure reaching the Secure Access hosts, which does not indicate network connectivity issues with the resource connector.

Supported Commands

Secure Access supports commands that you can run on a resource connector instance. For more information, see Supported Standard Linux Troubleshooting Commands.

For more information about using tcpdump with resource connectors, see Run tcpdump on Resource Connectors.

Command	Description
diagnostic	Try this command first when troubleshooting using the CLI. Runs a series of ping and DNS tests on the local IP address, gateway, Secure Access APIs, and headend IP addresses. It also checks connectivity on HTTPS port to various Secure Access endpoints, along with system artifacts created through the connector instance provisioning process.
help	Lists commands available to the `acadmin` user.
routeadd	Add routes to the resource connector. Use `routeadd -n IP/MASK -g GW_IP` where the network is `-n IP/MASK` and the gateway is `-g GW_IP`. Routes added with this command do not persist across reboots.
routedel	Delete routes added using the routeadd command. Use `routedel -n IP/MASK -g GW_IP` where network is `-n IP/MASK` and gateway is `-g GW_IP`. This command does not delete system created routes.
routeshow	Display all routes in the system.
sshkey	In addition to the SSH key configured when you deployed the resource connector, you can add short-lived SSH keys on the resource connector. Use the `sshkey` command to manage the resource connector's public SSH keys for the `acadmin` user. Run `sshkey -h` to list the command-line options.
tcpdump	Display packet capture information and filter on IP address and port, with limited functionality. Use the `tcpdump` command with the supported filters to capture the network events on the resource connector. Run `tcpdump -h` to list the available command-line options.

Command	Description
techsupport	Displays the following information: • Software version. • VPN tunnel state and related information. • System monitoring metrics, such as disk and memory statistics. • Information snapshot of the connector host, from DNS to Network interface details, iptables, routes, sysctl system settings, and monitoring information. • Recent periodic resource connector software logs.
version	Show the connector software version and the platform OS version running on the connector instance.

Run the Diagnostic Command on the Resource Connector

Provides instructions for completing the Run the Diagnostic Command on the Resource Connector workflow in Cisco Secure Access. To understand the results of the diagnostic command, see Diagnostic Codes.

To understand the results of the **diagnostic** command, see Diagnostic Codes.

In a shell on the resource connector, run the **diagnostic** command, which displays a summary of events or the details for all events on the resource connector.

Procedure

1. Run **ssh** with the SSH key that you configured while deploying the connector instance.
2. Sign in with the **acadmin** username.
3. At the shell prompt, enter **diagnostic**.

Supported Standard Linux Troubleshooting Commands

Describes Supported Standard Linux Troubleshooting Commands in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You can use these Linux commands to provide information about a resource connector instance:

- **ping**
- **nslookup**
- **traceroute**
- **tcptraceroute**
- **netstat**
- **free**
- **df**
- **vmstat**
- **iostat**
- **mpstat**
- **reboot**
- **uptime**

- **date**
- **clear**

Run tcpdump on Resource Connectors

Provides instructions for completing the Run tcpdump on Resource Connectors workflow in Cisco Secure Access. An instance of a resource connector deployed in a virtual machine (VM).

Run tcpdump on a resource connector to view the connector's packet capture (PCAP) file or upload the connector's PCAP file to Cisco Support or a remote host.

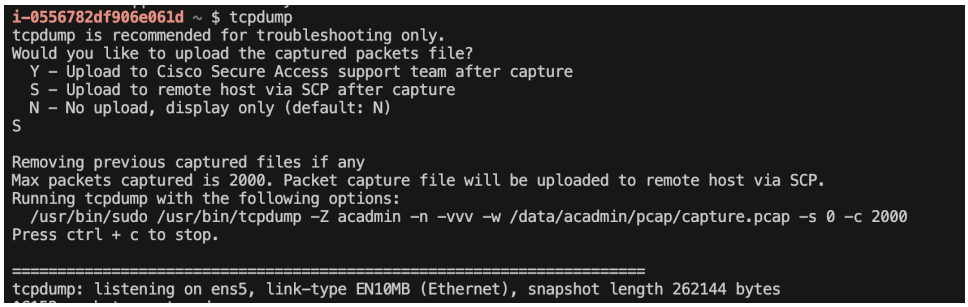
Before you begin

- An instance of a resource connector deployed in a virtual machine (VM).
- Credentials that you will use with SSH to sign in to the connector.

Procedure

1. Run `ssh` with the SSH key that you configured while deploying the connector instance.
2. Sign in to the connector with the `acadmin` username.
3. At the shell prompt, enter `tcpdump` with one of the available options.

   The default option is **N**, which displays the output of the PCAP file in the connector's shell.



   a) Choose **Y** to upload the resource connector's PCAP file to Cisco Secure Access Support.
   b) Choose **S** to upload the resource connector's PCAP file to a remote host using the Secure Copy Protocol (SCP). Enter the details of the remote host where the system will upload the PCAP file.
      - Remote host username.
      - Remote host IP address or hostname.
      - Remote host directory path where the system will upload the packet capture file.
      - Password for the remote user.

Diagnostic Codes

Describes Diagnostic Codes in Cisco Secure Access and outlines Diagnostic Codes for Connector Update Issues and Diagnostic Codes for Other Connector Issues. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

When you run the **diagnostic** commands, you will see state codes. For any issues that are not described with a diagnostic code, contact Cisco Secure Access Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

If an issue is not listed in the following tables, or an issue persists after you have taken the recommended action, contact Cisco TAC.

Diagnostic Codes for Connector Update Issues

Code for Upgrade State	Description	Recommended Action	If Issues Persist
1–99	Normal state or upgrade is in progress.	No action needed.	N/A
100,102	Upgrade failed.		Contact Support (Cisco TAC).
101	Secure Access will automatically attempt the upgrade again.	Monitor to ensure successful retry.	Contact Support (Cisco TAC).
200	Docker login authentication failure. Check docker login credentials for container.	For VM, monitor to ensure successful retry.	Contact Support (Cisco TAC) to provide guidance when setting up the Docker account.
201–204	Secure Access will automatically attempt the upgrade again.	Monitor to ensure successful retry.	Contact Support (Cisco TAC).
204	Issue may be self-repairing.	Monitor to ensure successful upgrade.	Contact Support (Cisco TAC).
206	Upgrade failed.	Check for full disk.	Contact Support (Cisco TAC).
207,208	Upgrade failed.	To get more information, run the **techsupport** diagnostic command.	Contact Support (Cisco TAC).
210	Upgrade failed.	Secure Access will automatically attempt the upgrade again. Check for disk issue. Monitor to ensure successful retry.	Contact Support (Cisco TAC).
211	Secure Access will automatically attempt the upgrade again.	Monitor to ensure successful retry.	Contact Support (Cisco TAC).
217	Docker hub download failed due to rate limiting.	Authenticate with docker, using docker login.	Contact Support (Cisco TAC) to provide guidance when setting up the Docker account.
219	Host does not have sufficient disk space.	Free up at least 2G of disk space in host to ensure this auto recovers.	Contact Support (Cisco TAC).

Diagnostic Codes for Other Connector Issues

Code for Daemon Init State	Recommended Action	If Issues Persist
6	None; there are no issues.	N/A
101	Deploy a new connector instance.	--

Code for Daemon Init State	Recommended Action	If Issues Persist
102	Deploy a new connector instance. Ensure that you have correctly copied the provisioning key.	--
103	Deploy a new connector instance.	Contact Support (Cisco TAC)
104	Deploy a new connector instance.	Contact Support (Cisco TAC)
105	Deploy a new connector instance.	--
106	Ensure that you have correctly copied the provisioning key. Ensure that connector can connec to the Secure Access cloud. For more information, see Allow Resource Connector Traffic to Secure Access.	--
108	Ensure that the connector disk is writeable.	--
109	Ensure that the connector disk is writeable.	--
110	Ensure that the connector disk is writeable.	--
111	Ensure that connector can connect to the Secure Access cloud. For more information, see Allow Resource Connector Traffic to Secure Access.	--
112	Ensure that the connector instance time is correct. Ensure that connector can connect to the Secure Access cloud. For more information, see Allow Resource Connector Traffic to Secure Access.	--
113	Ensure that the connector disk is writeable.	--
114	Deploy a new connector instance. Ensure that connector can connect to the Secure Access cloud. For more information, see Allow Resource Connector Traffic to Secure Access.	--
115	Unable to sync the resource connector with Secure Access. If the error condition persists, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html Ensure that the connector can connect to Secure Access. For more information, see Allow Resource Connector Traffic to Secure Access.	--
116	Deploy a new connector instance.	Contact Support (Cisco TAC)
117	Deploy a new connector instance.	Contact Support (Cisco TAC)
118, 119	Deploy a new connector instance.	--

Code for Daemon Init State	Recommended Action	If Issues Persist
All others	Deploy a new connector instance.	Contact Support (Cisco TAC)

13 Roaming Devices

Topics:

- Manage Roaming Devices
- View Internet Security Settings for Roaming Devices
- Edit Internet Security Settings for Roaming Devices
- Delete a Roaming Device

Provides an overview of Roaming Devices in Cisco Secure Access, including Manage Roaming Devices, View Internet Security Settings for Roaming Devices, and Edit Internet Security Settings for Roaming Devices. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Roaming Devices

Describes Manage Roaming Devices in Cisco Secure Access. Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module.

Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module. The Cisco Secure Client syncs with Secure Access to manage the DNS and Web security on the device. As part of the sync, a Roaming Device resource is added to Secure Access. An administrator of the organization can apply policy rules to the Roaming Device resource. For more information about the Cisco Secure Client with the Umbrella Roaming Security module, see Manage Internet Security on Cisco Secure Client.

In Secure Access, you can view Roaming Devices in the organization. You can edit the Internet Security settings for certain devices or all devices. You can override the Internet Security settings for the devices or delete a Roaming Device.

- View Internet Security Settings for Roaming Devices
- Edit Internet Security Settings for Roaming Devices
- Delete a Roaming Device

View Internet Security Settings for Roaming Devices

Describes View Internet Security Settings for Roaming Devices in Cisco Secure Access. A Roaming Device resource represents a user device that has deployed the Cisco Security Client with the Umbrella Roaming Security module.

A Roaming Device resource represents a user device that has deployed the Cisco Security Client with the Umbrella Roaming Security module.

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- DNS-layer security
- Web security

Once deployed, the Cisco Secure Client registers the user device with Secure Access. Cisco Secure Access adds the device to the list of Roaming Device resources managed by the organization. Cisco Secure Client syncs with Secure Access periodically and the device's DNS and web traffic is protected by the organization's policy rules. As an administrator, you can override, enable, or disable the internet security settings for the roaming devices in the organization.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Cisco Secure Client version 5.1.8.105 or later deployed with the Umbrella Roaming Security module or a PAC file for browsers in the environment is required for SWG protection status in Secure Access. For more information, see Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1.

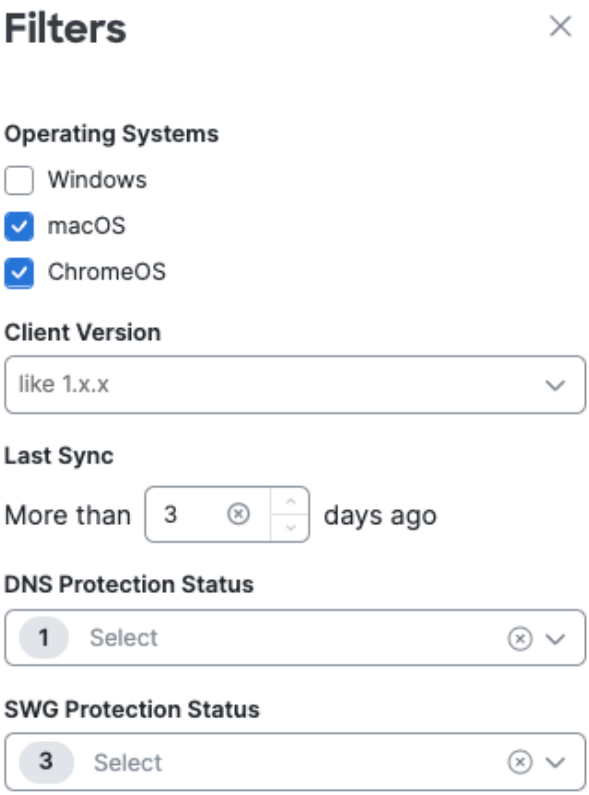
> **Note**
>
> IPS in Cisco Secure Access does not support traffic from the Secure Client roaming module.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Filter by device operating system, Cisco Secure Client version, last sync, DNS protection status, and SWG protection status.



3. Click a device name to open the Roaming Device resource.



4. The Roaming Device resource displays the device's internet security details.

   These details include:

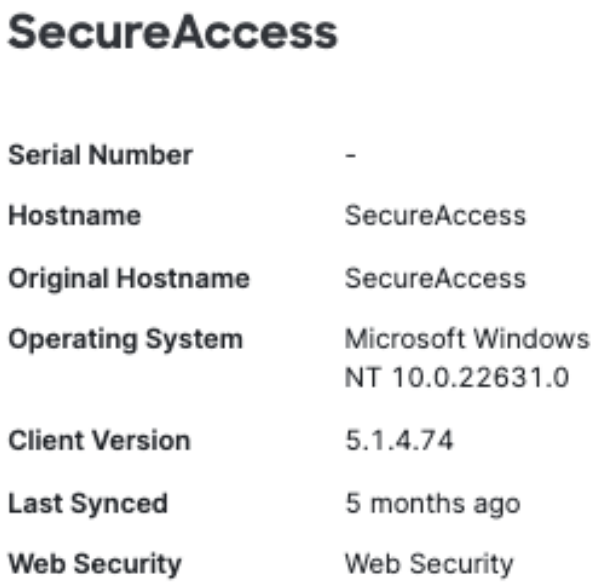
   - Host Information
   - Secure Web Gateway Status
   - Security Information - IPv4
   - Security Information - IPv6

Host Information

Describes Host Information in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- **Name**–name of the device
- **Serial Number**–serial number of the device

- **Original Hostname**–original hostname of the device
- **Operating System**–operating system and version
- **Client Version**–version of Cisco Secure Client installed on the device
- **Last Synced**–last date when Cisco Secure Client received a sync from Secure Access
- **Web Security**–specifies whether Cisco Secure Client has internet security deployed



Secure Web Gateway

Describes Secure Web Gateway in Cisco Secure Access. SWG Protection Status–specifies when the Secure Web Gateway roaming device status is Offline, Protected, Unprotected, Configuration Error, Cloud Service Unavailable, Disabled, Disabled due to VPN, or Disabled due to trusted network.

- **SWG Protection Status**–specifies when the Secure Web Gateway roaming device status is Offline, Protected, Unprotected, Configuration Error, Cloud Service Unavailable, Disabled, Disabled due to VPN, or Disabled due to trusted network. For more information about these status values, see SWG Protection Status and Status in Umbrella Roaming Security Tile.



Cisco Secure Client version 5.1.8.105 or later deployed with the Umbrella Roaming Security module or a PAC file for browsers in the environment is required for SWG protection status in Secure Access.

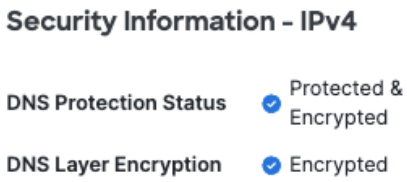
For more information, see the following resources:

- Manage Internet Security
- Configure Cisco Secure Client Settings
- Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1
- Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1

Security Information – IPv4

Describes Security Information - IPv4 in Cisco Secure Access. DNS Protection Status–specifies whether DNS-layer security roaming device status for IPv4 traffic is Offline, Unprotected, Protected, Protected and Encrypted, Protected by VA, Protected by Network, Disabled by User, Disabled on Full-Tunnel VPN, or Uninstalled.

- **DNS Protection Status**–specifies whether DNS-layer security roaming device status for IPv4 traffic is Offline, Unprotected, Protected, Protected & Encrypted, Protected by VA, Protected by Network, Disabled by User, Disabled on Full-Tunnel VPN, or Uninstalled.
- **DNS Layer Encryption**–specifies whether DNS-layer security is encrypted for IPv4 traffic.



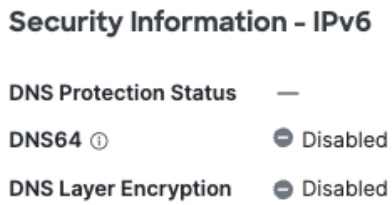
Security Information – IPv6

Describes Security Information - IPv6 in Cisco Secure Access. DNS Protection Status–specifies whether DNS-layer security roaming device status for IPv6 traffic is Offline, Unprotected, Protected, Protected and Encrypted, Protected by VA, Protected by Network, Disabled by User, Disabled on Full-Tunnel VPN, or Uninstalled.

- **DNS Protection Status**–specifies whether DNS-layer security roaming device status for IPv6 traffic is Offline, Unprotected, Protected, Protected & Encrypted, Protected by VA, Protected by Network, Disabled by User, Disabled on Full-Tunnel VPN, or Uninstalled.
- **DNS64**–specifies whether DNS64 service is enabled (returns synthetic IPv6 addresses to clients for IPv4-only destinations).

> **Note**
>
> IPv6 queries for domains with IPv4-only addresses are not resolved by Secure Access at this time. These queries may be answered by your local DNS resolver and would not be protected by Secure Access.

- **DNS-layer Encryption**–specifies whether DNS-layer security is encrypted for IPv6 traffic.



Edit Internet Security Settings for Roaming Devices

Describes Edit Internet Security Settings for Roaming Devices in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices.

The Cisco Secure Client Umbrella Roaming Security module enables secure internet access on user devices. The Umbrella Roaming Security module includes:

- DNS-layer security
- Web security

The Cisco Secure Client default deployment enables DNS-layer security. You must activate the Secure Web Gateway (SWG) internet security settings in your instance of Secure Access.

Secure Access has various options to configure the Internet Security settings on Roaming Devices:

- Always enable the Secure Web Gateway settings for all Roaming Devices
- Always Override the Secure Web Gateway settings for all Roaming Devices
- Use the Secure Web Gateway settings in the default policy rule

Prerequisites

- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

Describes Procedure in Cisco Secure Access. You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices.

You can override the internet security settings globally or disable the Cisco Secure Client Umbrella Roaming Security module on individual Roaming Devices. Unless configured, all devices follow the global settings for internet security in the Cisco Secure Client Umbrella Roaming Security module settings.

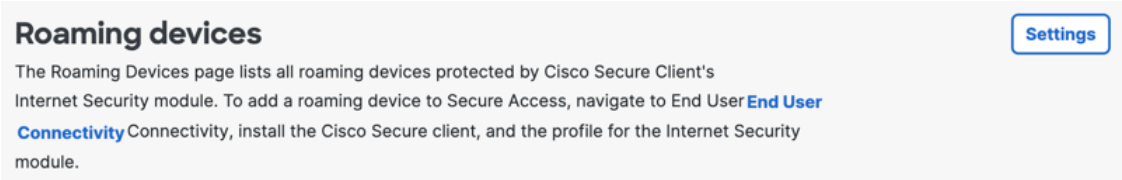
For example, in a scenario where there are 100 Roaming Devices and internet security is enabled globally, you have the option to override any of those 100 devices to disable internet security. However, if Secure Access internet security is disabled globally, the devices that are enabled through the override remain enabled.

Edit the Auto-Delete Interval for Roaming Devices

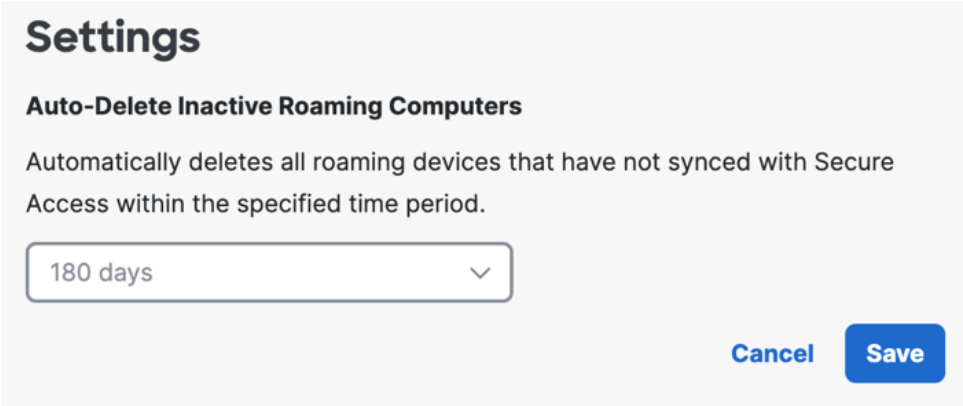
Provides instructions for completing the Edit the Auto-Delete Interval for Roaming Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Click **Settings** to set the auto-delete interval setting.



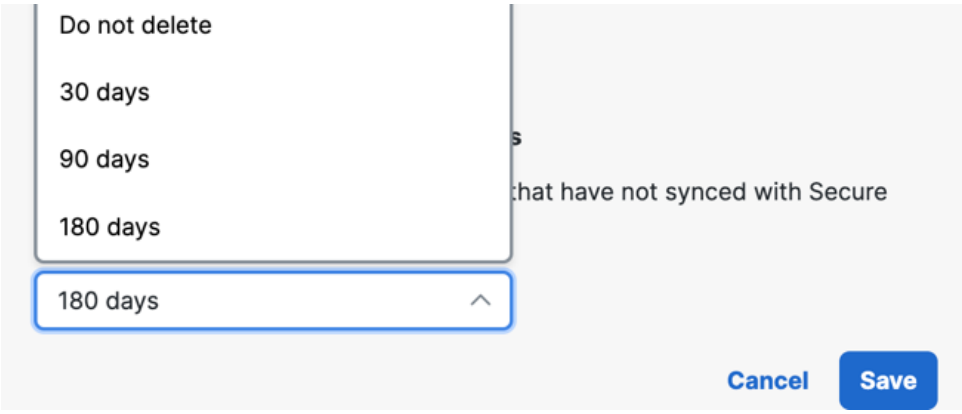
3. From the dropdown, choose **Do not delete** or the time period that the roaming devices must sync with Secure Access before the devices are deleted from the organization, and then click **Save**.



What to do next

The time intervals to sync roaming devices with Secure Access are:

- **Do not delete**–do not delete the Roaming Devices in the organization.
- **30 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 30 days.
- **90 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 90 days.
- **180 days**–delete the Roaming Devices in the organization if the devices have not synced with Secure Access in 180 days.



Disable the Internet Security Settings

Provides instructions for completing the Disable the Internet Security Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Roaming Devices**.
2. Select the devices to disable the SWG setting.
3. From the **Action** menu, select **Disable SWG**.

What to do next

The SWG Agent displays as **Disabled** in the Roaming Computer's details. The SWG Agent only appears in the details when the override is used.

Enable the Internet Security Settings

Provides instructions for completing the Enable the Internet Security Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Roaming Computers**.
2. Select the devices for which you want to enable the SWG module. You can select up to 100 devices at a time on the page.
3. From the **Action** menu, select **Enable SWG**.

> **Note**
>
> The Action menu does not appear until you select a device.

What to do next

The SWG Agent displays as **Enabled** in the Roaming Computer's details. The SWG Agent only appears in the details when the override is used.

Remove the Internet Security Override on Roaming Devices

Provides instructions for completing the Remove the Internet Security Override on Roaming Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

It is also possible to remove the SWG override and revert to the global setting. For example, in a scenario where 100 Roaming devices have SWG enabled globally, but 50 have been disabled through the override, those devices can have the override removed to revert back to the global setting.

Procedure

1. Navigate to **Resources** > **Roaming Computers**.
2. Select the devices for which you want to remove the SWG override. You can select up to 100 devices at a time on the page.

> **Note**
>
> Select the checkbox at the top of the column to select all devices on the page.

3. From the **Action** menu, select **Follow Global Settings**. You can select up to 100 devices at a time on the page.

Delete a Roaming Device

Provides instructions for completing the Delete a Roaming Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

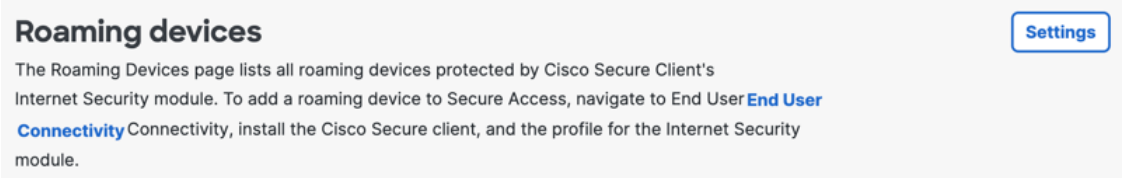
An administrator can delete a Roaming Device resource in Secure Access. Once deleted, the Roaming Device is removed from any Secure Access policy rules and is no longer protected by Secure Access.

Before you begin

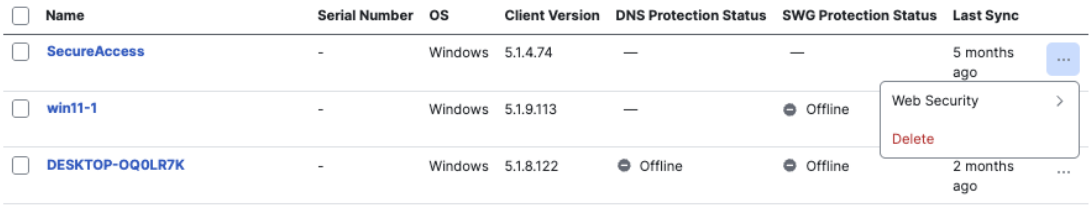
- Full Admin user role. For more information, see Manage Accounts.

Procedure

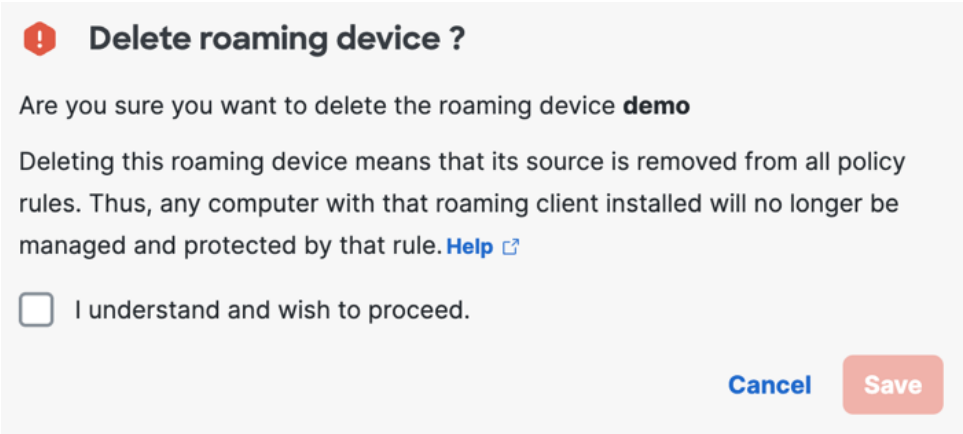
1. Navigate to **Resources** > **Roaming Devices**.



2. Click the ellipsis (**...**) to open the action menu, and then click **Delete**.



3. Check **I understand and wish to proceed**, and then click **Save**.



14 Private Resources

Topics:

- Manage Private Resources

Provides an overview of Private Resources in Cisco Secure Access, including Manage Private Resources. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Private Resources

Private resources are applications, networks, or subnets that are not publicly accessible from outside your network.

Private resources are applications, networks, or subnets that your organization controls. These resources are not publicly accessible from outside your network. Examples of private resources are:

- Applications and services that run on-premises in your data center
- Resources running on private clouds hosted from your data center

You can configure private network entities and add private resources in your Secure Access organization. Follow these steps to add a private resource and set up network connectivity to the resource, Then, set up profiles and certificates, add the private resources on the policy rules, and set up the Cisco Secure Client and distribute a URL to the private resource.

> **Warning**
>
> If you attach an empty private resource group to a policy, the entire rule containing the empty private resource is dropped.

Step 1: Set Up Private Resources

Configure end user connections to a private resource, and then add a private resource to a private resource group.

- **Understand your connection options**.

  Specify connection requirements for private resources where you want to allow access.

  For more information, see Comparison of Zero Trust Access and VPN and Manage Branch Connections.

- **Add Private Resources**.

  Work with resource owners to gather the information needed to configure each resource. For more information, see Add Private Resources.

- **Add new Private Resources to Resource Connector Groups**.

  If your traffic connects through Resource Connectors rather than Network Tunnels, and you add a private resource after you add the resource connector group, you must add the new resource to a connector group. For more information, see Assign Private Resources to a Connector Group.

- **(Optional) Block zero-trust access to specified subdomains**.

  If you configure a Private Resource with an IP address having a leading wildcard (for example: ***.example.com**), you can block zero-trust connections to subdomains that you specify.

  User devices must have the Cisco Secure Client deployed. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.

  If you have deployed the zero trust client on iOS devices, see unique matching information in the "Guidelines and Limitations" section of Set up the Zero Trust Access App for iOS Devices.

- **(Optional) Add Private Resource Groups**.

  To speed creation and management of access rules, and ensure consistent handling of related private resources, create groups of private resources that you want to manage as a unit. For more information, see Add Private Resource Groups.

Step 2: Set Up Network Connections, VPN Profiles, and Certificates

> **Note**
>
> To support decryption of traffic to private resources, you must enable global decryption. For more information, see Decryption.

- **Configure network connectivity for zero-trust connections**.

  Add Network Tunnel Groups or Resource Connectors to allow Secure Access to communicate with and direct traffic to your private resources. For more information, see Manage Network Connections.

- **Add VPN profiles**.

  To allow VPN connections to private resources, add VPN profiles to your organization. VPN configurations such as VPN traffic steering rules must exist for the applicable network address spaces. For more information, see Manage Virtual Private Networks.

- **Add and manage certificates for private resources**.

  Secure Access requires certificates in order to connect user traffic with your private resources and decrypt that traffic for inspection by the Intrusion Prevention System (IPS). You can upload the certificate for a resource when you configure the resource, or manage certificates from the certificate list. For more information, see Certificates for Private Resource Decryption.

Step 3: Add Private Resources in Policy Rules

> **Note**
>
> If an Access policy rule applies to traffic selected with the "Any" private destinations component, Secure Access does not evaluate the traffic using the DLP policy. Secure Access forwards the private traffic to the DLP engine only if an Access policy rule matches the traffic for the selected private resources or private resource groups.

Add private access rules to the Access policy or Real Time rules to the Data Loss Prevention (DLP) policy. After you add private resources to your organization, these resources are available for you to use as destinations in your policy rules. You can use private resources in your Access policy or DLP policy.

- **Add private access rules to the Access policy**.

  Private access rules define which users and devices can access the private resource in the organization. For more information, see Add a Private Access Rule.

- **Add Real Time rules to the Data Loss Prevention (DLP) policy**.

  Real-time DLP rules define the resources that the system scans for violations in HTTP/HTTPS and non-HTTP/non-HTTPS (such as SMB and FTP) traffic in both upload and download directions for all supported file types not including forms data. For more information, see Supported File and Form Types and Add a Real Time Rule to the Data Loss Prevention Policy.

Step 4: Set Up the Cisco Secure Client and Distribute URLs

- **Ensure that user devices are set up for client-based Zero Trust Access**.

To configure resources for client-based zero-trust access, ensure that user devices meet the requirements for Zero Trust. You must have the Cisco Secure Client Zero Trust Access module deployed on the devices in your organization. For more information, see Zero Trust Access Requirements and Limitations on page 1207.

- **Distribute URLs for browser-based Zero Trust Access**.

  Establish a system for making users aware of the special URLs needed for browser-based Zero Trust Access.

Add a Private Resource

Configure a private resource with connection information, then add access rules in the Access policy to determine which users and devices can access the resource.

Private resources are the applications, networks or subnets that are internal resources hosted in your data center. Private resources may include resources hosted on a private cloud in your data center or resources that have a login page that cannot be accessed from outside the network.

Configure a private resource with the connection information for the resource, then add access rules in the Access policy to determine which users and devices can access the resource using the connection methods that you have enabled.

For information on using Secure Access to learn about private resources based on your private network traffic, see Discover Private Resources.

Prerequisites: Add Private Resources

- Have a full Admin user role. For more information, see Manage Accounts.
- Gather IP or CIDR addresses for your private resources. Private resources cannot use IP addresses or networks listed in IP Address Restrictions.
- If you specify resource addresses using fully-qualified domain names (FQDNs), add at least one internal DNS server that can route traffic to your resource. For more information, see Add DNS Servers.
- For each resource, choose connection options. For descriptions of the options, see the topics under Manage Connections to Private Destinations.
- If you enable Zero Trust Access for the resource:
  - Meet the requirements in Requirements for Zero Trust Access.
  - To allow client-based Zero Trust Access and inspect traffic using the Intrusion Prevention (IPS), file inspection, and file type blocking features, provide the resource's certificate to Secure Access so that Secure Access can display it to end-user devices.
  - Cisco recommends using a certificate signed by a publicly recognized certificate authority (CA).
  - If you enable browser-based zero trust access using SSH or Remote Desktop (RDP), see Allow SSH and RDP Access to Private Resources.
- Plan your private resource configurations to avoid configuration conflicts such as unintentional duplicate or overlapping addresses.

  For example, if a resource can be reached using multiple addresses, decide in advance whether you will create a single resource with multiple addresses or multiple resources. For more information about this particular scenario,z see Private Resource Configuration Examples.

Define a Private Resource

Provides instructions for completing the Define a Private Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure a resource that is controlled by your organization.

Before you begin

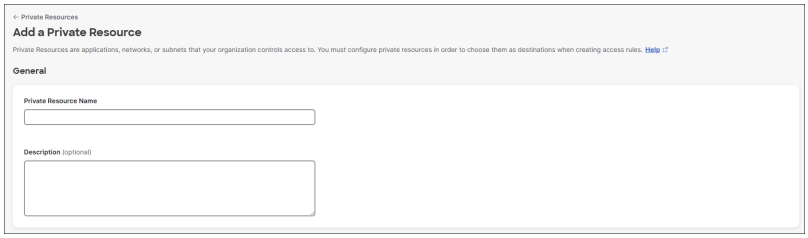
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Private Resources**, and then click **+Add**.



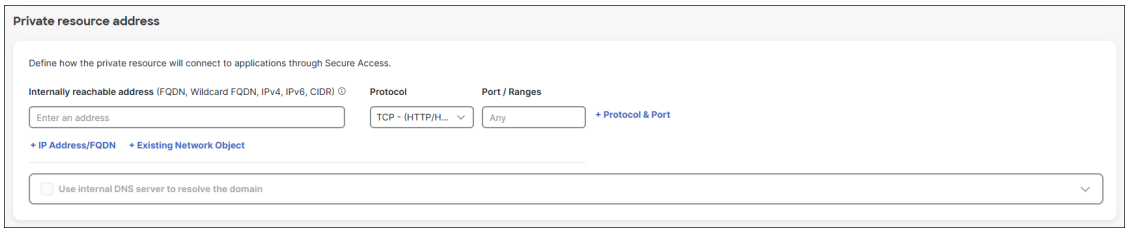
2. For **Private Resource Name**, enter a meaningful name for the resource.
3. For **Description**, we recommend that you provide information such as the purpose of the resource or the name of the resource owner.



Private Resource Address

Provides instructions for completing the Private Resource Address workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Provide the network address information for communicating with the private resource.



Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Private Resources**.
2. For **Internally reachable address**, enter an IP address, FQDN, wildcard FQDN (in the format ***.example.com**), Network Objects, protocol, and port or port ranges.

   You do not have to provide an address that is publicly accessible from outside the network.

   If you will allow browser-based access to this resource by users who do not have the Cisco Secure Client installed on their devices, the protocol you select must include HTTP/HTTPS.

   Use caution when adding addresses that duplicate or overlap with addresses in other configured private resources. If you will enable browser-based zero trust access using SSH or Remote Desktop (RDP) protocols, see Allow SSH and RDP Access to Private Resources.

If you will decrypt traffic to this resource, follow these guidelines.

- In each address line, you can specify a single IP address (no address ranges) or CIDR block, or a comma-separated list of addresses or CIDR blocks, or an FQDN with or without wildcard. Add addresses and FQDNs as separate lines.

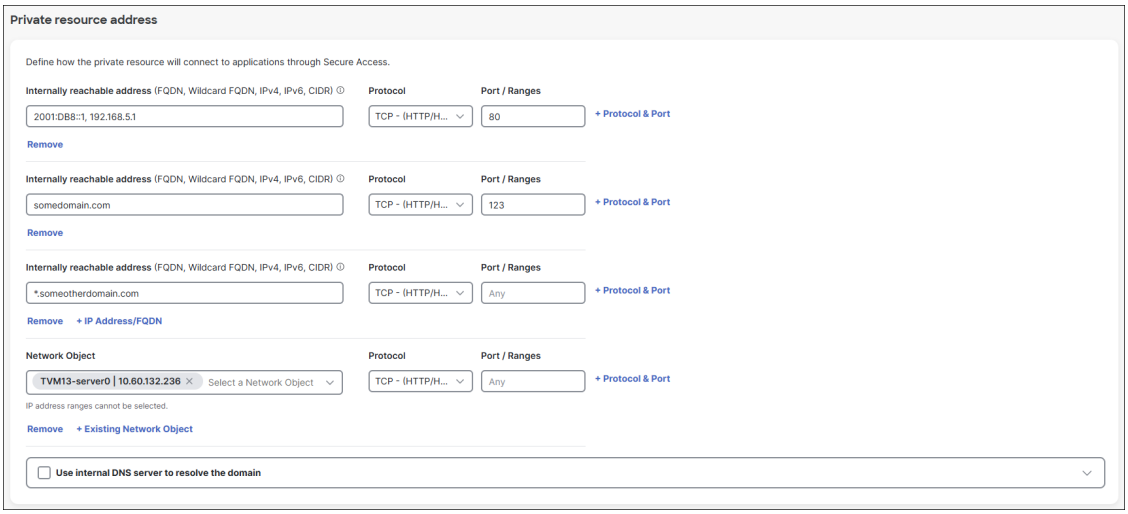
  If the address includes a wildcard FQDN, the wildcard must be the first character in the address string (***.example.com**).

  Specify a single port or "Any" port; no comma-separated port numbers, no port ranges.

  If you need to decrypt traffic to multiple ports for the same address, click **+ IP Address/FQDN** and add a separate address line for each port.

  Select a protocol that includes TCP and does not include UDP.

  Example configurations:



If you enter a domain and Secure Access will route traffic to this resource using network tunnels, follow these guidelines.

- Select an internal DNS server that can route traffic to the specified resource address.

  To configure an internal DNS server, see Add DNS Servers.

Endpoint Connection Methods

Describes Endpoint Connection Methods in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Choose the connection methods to allow communications to the private resource. For more information, see Comparison of Zero Trust Access and VPN.

> **Note**
>
> If you do not allow Zero Trust Access or VPN connections for the private resource, only branch connections are enabled on the private resource. Branch connections are pre-selected for a private resource. For more information, see Manage Branch Connections.

You can allow any of these connection options:

- **Zero-trust connections**
  - **Client-based connection**–For devices with the Cisco Secure Client or the Zero Trust Access mobile application installed.
  - **Browser-based connection**–For devices without the Cisco Secure Client or the Zero Trust Access mobile application installed, or when you only want to allow access using a browser.
- **VPN connections**–For devices that allow VPN connections to the private resource.

Client-Based Zero-Trust Connections

Provides instructions for completing the Client-Based Zero-Trust Connections workflow in Cisco Secure Access. Configure Zero Trust Access (ZTA) for end users that connect to destinations using the Secure Client.

Configure Zero Trust Access (ZTA) for end users that connect to destinations using the Secure Client.

You can allow connections to a private resource from devices for contractors or vendors, or Bring-Your-Own devices. To allow the devices that your organization does not manage to connect to a private resource, you must enable browser-based access.

Note

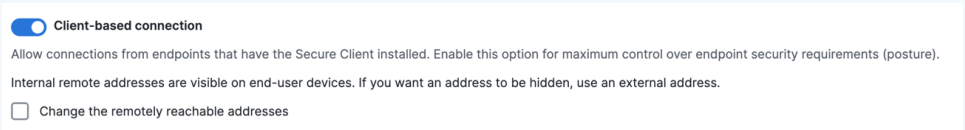
Before you begin

Procedure

1. Navigate to **Resources** > **Destinations** > **Private Resources**.
2. Enter the appropriate details for a private resouce; for more informationon prerequisites and steps, see Add a Private Resource on page 481
3. For the **Endpoint Connection Method** select zelect **Zero-trust connections** to allow connections from devices with and without the Secure Client installed.
4. For **Client-based connection**, enter the address you want users to use in order to connect to this resource. For best security (to keep the internal IP address of this resource private), you should provide a domain rather than an IP address. Your internal DNS server must be able to route traffic to this address. For example, you can enter **mail.example.com**.

   Note

   This address can be the same as the address you entered above for Secure Access to connect to the resource.

5. Continue creating the private resource and complete the **VPN Connections** section. For steps to complete this procedure and finalize your private resource, see for more information.

Browser-Based Zero-Trust Connections

Provides instructions for completing the Browser-Based Zero-Trust Connections workflow in Cisco Secure Access. The Allow unauthenticated pre-flight OPTIONS request function is currently Controlled availablility and must be manually enabled through your Cisco represenative or Cisco Support.

Configure Zero Trust Access (ZTA) for end users that connect to destinations using the browser.

You can allow connections to a private resource from devices for contractors or vendors, or Bring-Your-Own devices. To allow the devices that your organization does not manage to connect to a private resource, you must enable browser-based access.

Browser-based (clientless) Zero Trust Access offers fewer security controls on devices than client-based Zero Trust Access.

Before you begin

The **Allow unauthenticated pre-flight OPTIONS request** function is currently **Controlled availablility** and must be manually enabled through your Cisco represenative or Cisco Support. Open a ticket and request this feature to initiate the Cross-Origin Resource Sharing (CORS) request. Here is an example of a CORS prelight request:

```
OPTIONS /doc HTTP/1.1
Host: bar.company.com
Origin: https://foo.company.com
Access-Control-Request-Method: POST
Access-Control-Request-Headers: X-PINGOTHER, Content-Type
<..>

HTTP/1.1 204 No Content
Access-Control-Allow-Origin: https://foo.company.com
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Allow-Headers: X-PINGOTHER, Content-Type
<..>
```

You **must** have the following prerequisites completed prior to deploying:

- The primary and secondary domains must already be defined as **browser-based access applications** and are allows in a policy. Only the secondary domain is requied to enable the **Allow unauthenticated pre-flight OPTIONS request** functionality.
- It is expected that the *foo.company.com* (origin) domain is authenticated and has a valid authentication cookie via Browser-based Access for the CORS resource (*bar.company.com*) OPTIONS request to be allowed unauthenticated.
- You must include this HTTP header as part of the HTTP response of the resource:

  ```
  Access-Control-Allow-Credentials: true
  ```

- Both requests *foo.company.com* (primary) and *bar.company.com* (secondary) must originate from the same source egress (public) IP.
- In the HTTP response to the CORS resource, this HTTP header must be included: `Access-Control-Allow-Credentials: true`. The header enables the browser to add the authentication cookie for the GET request to the CORS resource request (after the OPTIONS preflight request succeeds).

Completeing the prerequisites listed above allows the following expected functionality:

1. `GET foo.company.com`. The first request gets directed ot the IdP and then Browser Access sets a cookie for the domain *company.com* after the authentication.
2. `GET foo.company.com`. An authentication cookie needs to be set for the secondary domain. The second request returns a fetch API to obtain resources from the secondary domain.

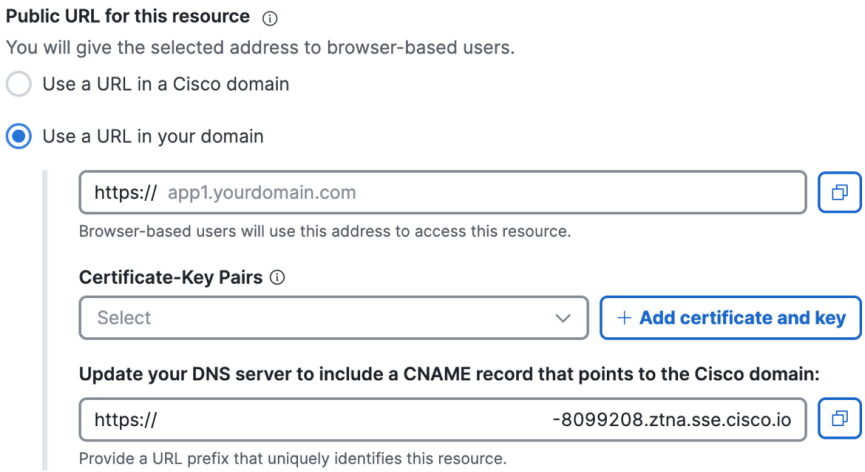
3. `OPTIONS bar.company.com`. When the **Allow unauthenticated pre-flight OPTIONS request** option is enabled on the secondary domain, the third request forwards to the destination without an auth cookie.

Procedure

1. Navigate to **Resources** > **Destinations** > **Private Resources**.
2. Enter the appropriate details for a private resource; for more information on prerequisites and steps, see Add a Private Resource on page 481.
3. For the **Endpoint Connection Method** select **Zero-trust connections** to allow connections from devices with and without the Secure Client installed.
4. For **Browser-based connection**, configure a public URL for the resource that you will give to users. You have the option to use either a Cisco domain or a custom domain. End users can reach a resource from outside their network. Secure Access forwards authorized connections to the resource.

> **Note**
>
> For browser-based ZTA, you must configure the network address of the private resource with these controls:
>
> - For **Internally reachable address**, you must add either a single fully qualified domain (FQDN) or one or more IP addresses.
> - For **Protocol**, you must choose either **TCP – (HTTP,HTTPS) only**, **TCP – SSH** or **TCP – RDP**.
> - For **Port / Ranges**, you must add a single port number.
>
> For more information, see Private Resource Address.

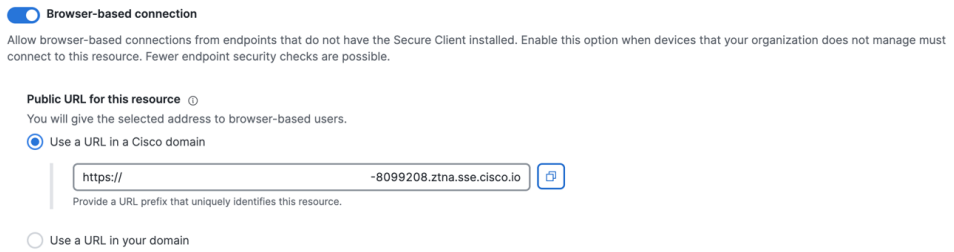
5. For **Use a URL in your domain**, complete the configuration of the components that are required to use your own custom domain for browser-based ZTA connections.



6. For **Use a URL in a Cisco domain**, provide a URL prefix that uniquely identifies this resource.

   Secure Access will join the prefix to `<your organization's tenant ID>-ztna.sse.cisco.io` to form the public URL address. Secure Access will route traffic using this address to the resource.

   If you don't provide a URL prefix, Secure Access adds one for you based on the resource name.



7. Provide a full URL from your custom domain name. The URL field supports domains (example.com) and subdomains (subdomain.example.com).
8. For **Certificate-Key Pairs**, choose from the list of cryptographic certificate-key pairs or click **+Add certificate and key** to upload .pem files or paste new certificate and key data.

   You may also browse to **Secure** > **Certificates** and click the **Private resources** tab to upload and manage certificates used by private resources with browser-based ZTA.

   Cisco recommends using a certificate signed by a publicly recognized certificate authority (CA).

   The DNS server for your domain requires an additional canonical name (CNAME) record that maps your custom URL to the Secure Access URL provided in the field **Your DNS server must be able to route this traffic to this address**. Format the CNAME records as follows:

   - **Record type**: CNAME
   - **@**: **subdomain.example.com**
   - **Value**: **[custom-prefix]-[org ID].ztna.sse.cisco.io**

9. Configure the protocol, Custom host header, Server Name Indication (SNI).



10. For **Protocol**, choose **HTTPS** or **HTTP**.
11. Add a custom host header if your resource requires it to validate HTTP or HTTPS connections.

    Custom Host Header is optional for both a Cisco domain and a custom domain.

    - If **Protocol** is set to **HTTP** and the **Custom host header** field is left empty, the host header is the same as the Public URL for this resource.
    - If **Protocol** is set to **HTTPS** and both the **Custom host header** and **Server Name Indication (SNI)** fields are left empty, the host header is the same as the Public URL for this resource.
      - If the **Server Name Indication (SNI)** field has a value, the host header is the SNI value.
      - If end users typically use the fully qualified domain name (FQDN) to request the private resource, enter the FQDN for the private resource in the **Server Name Indication (SNI)** field.

12. For **Server Name Indication (SNI)**, enter the hostname.

    SNI is the hostname that the browser connects with to start a TLS handshake. If this resource shares a single IP address with other resources that present different certificates, enter the SNI hostname to connect traffic to this resource.

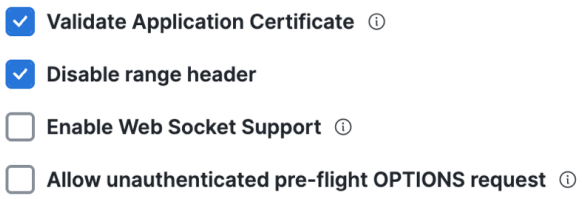
    If the internally reachable address is an fully qualified domain name (FQDN), consider using the FQDN as the SNI. If the field is left blank, the SNI will not be used.

    Secure Access recommends that you add the Server Name Indication (SNI) information for the browser-based ZTA connections.

13. Click **Validate Application Certificate**.

    If you enable **Decrypt Traffic** for the private resource, Secure Access disables this certificate validation setting.

    Validate Application Certificate is enabled by default.



14. Click **Disable range header**.

    When you activate the **Disable range header** option, Secure Access ignores the HTTP Range header in the requests on the ZTA browser-based connections. Disabling the HTTP Range header prevents the reading of partial requests and ensures that incomplete or malicious files are not downloaded by end users.

15. Click **Enable Web Socket Support** to enable real-time browser communication by allowing Web Socket connections for the resource.

    To enable web socket protocols, you must have **TCP – (HTTP/HTTPS)** only selected as the protocol.

    Web Sockets come with unique security risks. Only enable web sockets if essential.

    Enable Web Socket Support is disabled by default.

16. (**Controlled Availability**. Open a ticket with Cisco Support to enable this feature.) Click **Allow unauthenticated pre-flight OPTIONS request** to permit unauthenticated OPTIONS HTTP requests for the resource. This option allows a web server to explicitly grant permission for resources (such as fonts, scripts, or data) to be loaded from a domain different from the one that served the original web page. Browsers enforce the Same-Origin Policy (SOP) method by default which can prevent a script on one origin (e.g., https://site-a.com) from making requests to another origin (e.g., https://api.site-b.com). Enabling this setting provides a standardized way to bypass this restriction without risking security; with pre-flight OPTIONS the browser performs a preliminary check to ensure the request is genuine and free of malicious agents before allowing the request to pass.

    > **Note**
    >
    > We do **not** recommend using the wildcard character (*) for authenticated requests.

17. Continue creating the private resource and complete the **VPN Connections** section. For steps to complete this procedure and finalize your private resource, see for more information.

VPN Connections

Provides instructions for completing the VPN Connections workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

VPN connection allow endpoints to communicate to a private resource when connected to the network using VPN.

> **Note**
>
> If you enable both Zero Trust connections and VPN connections, users will connect to the resource using Zero Trust.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Private Resources**.
2. Select **VPN connections**.

Resource Connector Groups

Provides instructions for completing the Resource Connector Groups workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Associate the private resource with the Resource Connector Groups.

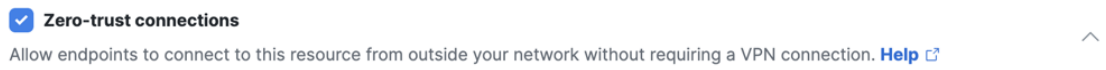
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

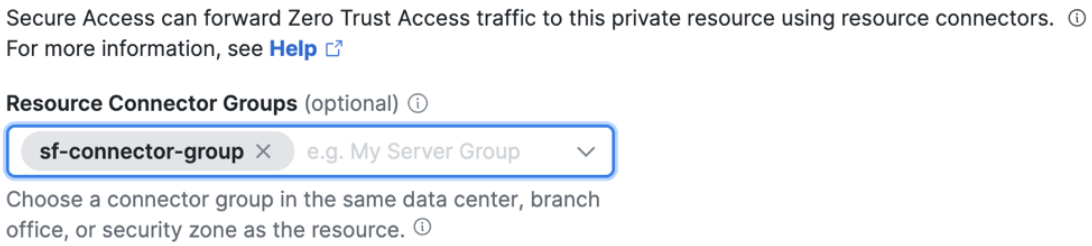
1. Navigate to **Resources** > **Private Resources**.
2. (Optional) For **Resource Connector Groups**, choose the resource connector groups that can forward traffic to this resource.

   > **Note**
   >
   > Before you can choose a Resource Connector Group, you must enable **Zero Trust connections** for this resource. You can also choose a connector group for this resource later, or assign resources on the Connector Group page.

3. Choose a group or groups that have deployed connectors, which are located in the same data center, branch office, or security zone as the resource.

   For more detailed guidelines, or an alternative place to associate resources with connector groups, see Assign Private Resources to a Connector Group.



Decryption

Provides instructions for completing the Decryption workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

For effective inspection of encrypted traffic, enable decryption on the private resource and enable global decryption. For information about enabling global decryption, see Manage Global Settings for Access Rules: Decryption.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

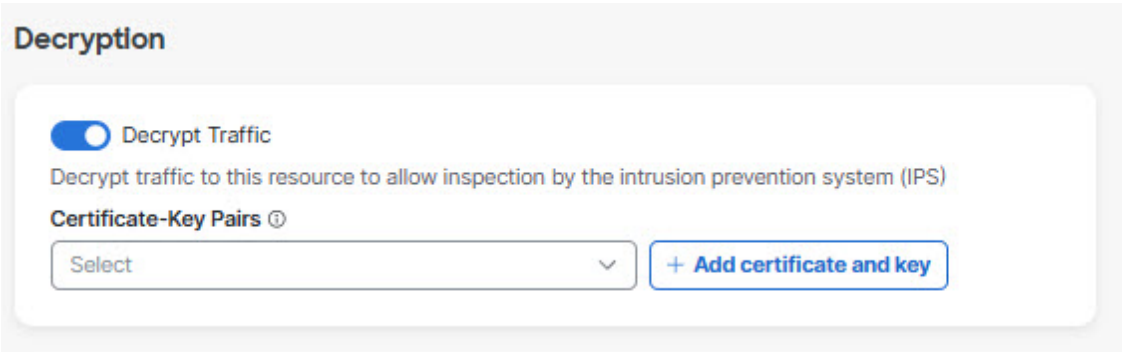
Procedure

1. Navigate to **Resources** > **Private Resources**.
2. Navigate to **Decryption** and toggle on **Decrypt Traffic**.

> **Note**
>
> If you enable decryption, Secure Access disables the option to **Validate application certificate** for browser-based traffic, even if you have previously enabled it. This is expected.

Decryption is required in order to inspect traffic for threats using the Data Loss Prevention (DLP) policy, Intrusion Prevention (IPS), file inspection, and file type blocking. For security reasons, you should enable this option.

You can enable this option depending on the resource address. For details, see information about the **Internally Reachable Address** field.



3. Select a certificate or upload a new certificate.

   Include all intermediate certificates in the certificate chain.

   Only PEM encoding is supported.

Because traffic is routed through Secure Access, Secure Access must be able to display the resource's certificate to end-user devices.

a) If you have already uploaded the certificate for the private resource, click **Select** to choose the certificate from the drop-down menu.

For information about uploading certificates in Secure Access, see Manage Certificates for Private Resource Decryption.

b) Click **+Add certificate and key** to upload or paste the application certificate (including both the public and private keys) used by the private resource.

View Access Rules Associated with a Private Resource

Provides instructions for completing the View Access Rules Associated with a Private Resource workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a private resource in Secure Access, you can view the attributes of the private resource. The attributes of the private resource include the private access rules in the Access policy associated with the private resource.

Before you begin

- A minimum user role of Read only. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Resources** > **Private Resources**.
2. Navigate to a row in the table of private resources.
   a) Click the ellipsis (**...**) at the end of the row, choose **Edit**, and then navigate to **Associated Rules**.
   b) Click on the name of a private resource and then navigate to **Associated Rules**.

   You can view and link to the access rules that are associated with the private resource.

What's Next

Describes What's Next in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

1. Test the connection between Secure Access and your private resources. For more information, see Test Private Resource Reachability.
2. (Optional) If you entered a FQDN of the format **.example.com* and you want to exclude subdomains from the ability to connect to this resource, add exceptions to the Traffic Steering page. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.
3. (Optional) You can exclude subdomains from this Private Resource configuration and then add one or more separate Private Resources and access rules to allow different access for those subdomains.
4. Configure requirements that you want to apply to this resource, such as endpoint requirements (using posture profiles) and Intrusion Prevention (IPS) profiles. For more information, see Components for Private Access Rules.
5. After you have configured other requirements, add policy rules to access this resource.
   - Add private access rules to allow users and devices to access this resource. For more information, see Get Started With Private Access Rules.

- Allow DLP real-time rules to scan for violations in upload, download, or both upload and download traffic. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.

> **Note**
>
> If an Access policy rule applies to traffic selected with the "Any" private destinations component, Secure Access does not evaluate the traffic using the DLP policy. Secure Access forwards the private traffic to the DLP engine only if an Access policy rule matches the traffic for the selected private resources or private resource groups.

6. When you are ready for end-users to access the resource and you have enabled browser-based access, give your users the dummy URL that you configured in this procedure.

Discover Private Resources

Provides instructions for completing the Discover Private Resources workflow in Cisco Secure Access. Secure Access Private Resource Discovery monitors your VPN and Zero Trust Access (ZTA) traffic to help you identify frequently accessed resources and make informed configuration decisions.

Secure Access Private Resource Discovery monitors your VPN and Zero Trust Access (ZTA) traffic to help you identify frequently accessed resources and make informed configuration decisions. Based on this traffic monitoring, the feature provides a list of suggested destinations and a workflow for defining them as private resources.

For more information, refer to:

- Manage Private Resources
- Manage Connections to Private Destinations
- Comparison of Zero Trust Access and VPN

Procedure

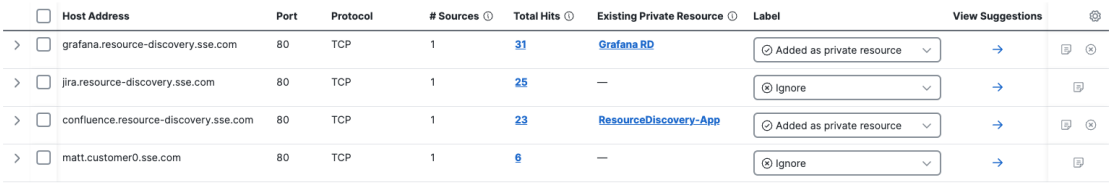
1. To access the report, navigate to **Monitor** > **Reports** > **Private Resource Discovery**.

   The report displays destinations accessed via your VPN and ZTA traffic.

   > **Note**
   >
   > Data may take up to 24 hours to appear or refresh. If there is insufficient traffic over the past 30 days to generate suggestions, no further action is required.

2. When sufficient usage data is available, the **Private Resource Discovery** page provides the following tools:
   - **Time filter:** Filter traffic for the last 24 hours, the last 7 days, or the last 30 days (default).
   - **Filter tiles:** Update the view based on labels applied to suggestions.
   - **Search:** Search by host address, protocol, or label.
   - **Export:** Download the data as a CSV file.
   - **Column customization:** Click the gear icon in the top-right corner of the table to select which columns to display.

3. The **Suggestions** table provides details for each discovered resource.

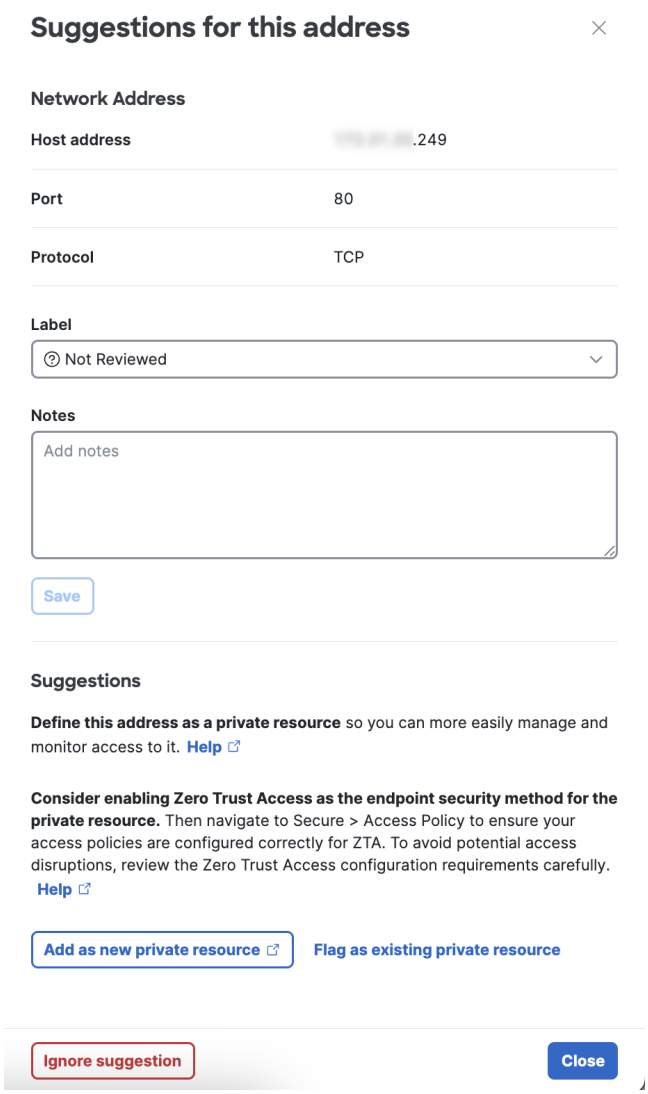


Host Address	Port	Protocol	# Sources	Total Hits	Existing Private Resource	Label	View Suggestions
grafana.resource-discovery.sse.com	80	TCP	1	31	Grafana RD	Added as private resource	
jira.resource-discovery.sse.com	80	TCP	1	25	—	Ignore	
confluence.resource-discovery.sse.com	80	TCP	1	23	ResourceDiscovery-App	Added as private resource	
matt.customer0.sse.com	80	TCP	1	6	—	Ignore	

Table columns:

- **Host Address:** Displays the IP address or FQDN. Expand the entry to view multiple IP addresses routing to a single FQDN.
- **Port / Protocol:** The port and protocol used for the connection.
- **# Sources:** The number of unique sources. Users connecting via VPN or ZTA are counted as individual sources; users accessing resources via network tunnel groups are counted as a single source.
- **Total Hits:** The total access count. Hover over the number for details.
- **Existing Private Resource:** The private resource currently associated with the address, if any.
- **First Seen / Last Seen:** The timestamp of the first and most recent access.
- **Label:** Current status (e.g., Not reviewed, Added as private resource, Flag for review, Ignore). Labels are for reference only and do not affect traffic or configurations.

4. Click the **View Suggestions arrow (→)** or the **notepad icon** to open the slide-in menu for a specific suggestion. You can perform the following actions:
   - **Add as new Private Resource**: Redirects you to the procedure for creating a new private resource. Refer to Add a Private Resource.
   - **Flag as an existing private resource**: Associates the address with an existing resource for future review. This does not modify the resource configuration.
   - **Ignore suggestion**: Applies the *Ignore* label to the suggestion.



5. Select multiple suggestions to enable the **Bulk Actions** menu. You can add selected suggestions as new or existing private resources, update their labels, or remove them from the list.



Map a Discovered Resource to Existing Private Resources

Provides instructions for completing the Map a Discovered Resource to Existing Private Resources workflow in Cisco Secure Access. Secure Access automatically evaluates discovered private resources against your existing private resource definitions.

Secure Access automatically evaluates discovered private resources against your existing private resource definitions. This feature reduces the need for manual correlation by identifying resources that are already managed. This allows you to focus on new or unmanaged assets. By correlating discovery signals with your defined resources, Secure Access helps streamline least-privilege policy cleanup and prevents the creation of duplicate resource definitions.

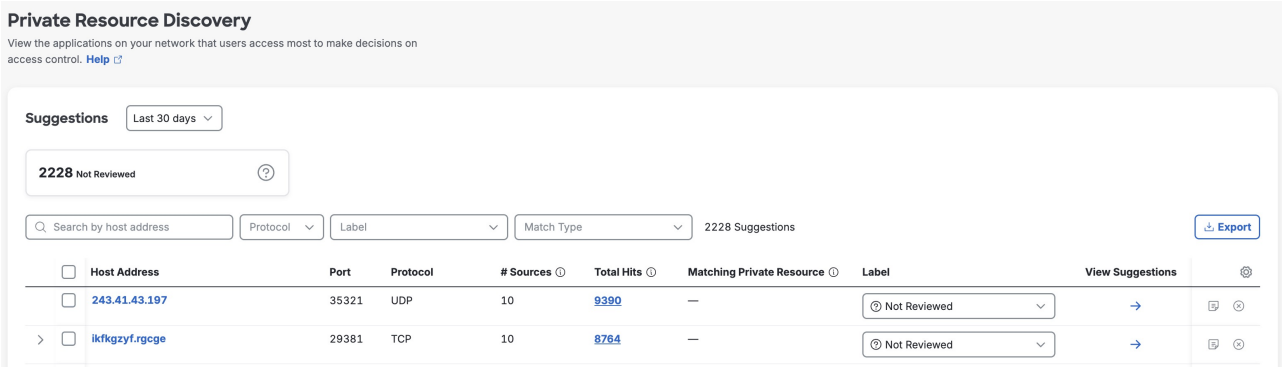
For a resource to be considered mapped, the discovered attributes must align with the defined private resource based on the following criteria:

- IP or CDR

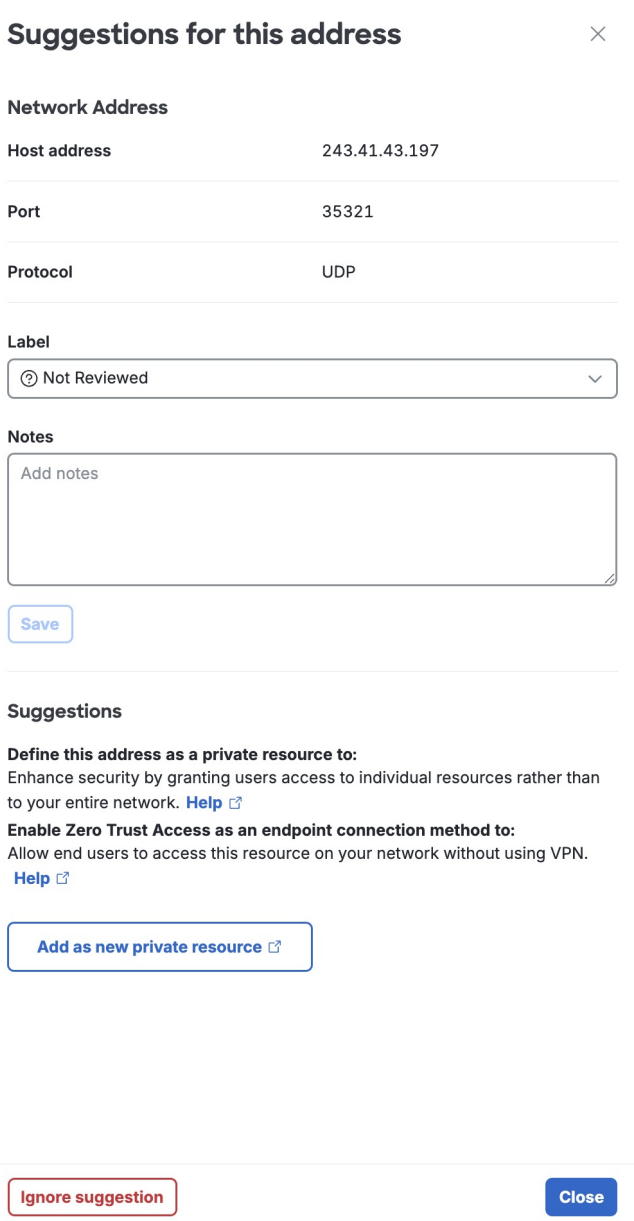
- Exact FQDN
- FQDN (Wildcard)
- Port and Protocol

Procedure

1. Navigate to **Monitor** > **Reports** > **Private Resource Discovery**.
2. Review the list of discovered private resources and their associated **Matching Private Resource**.

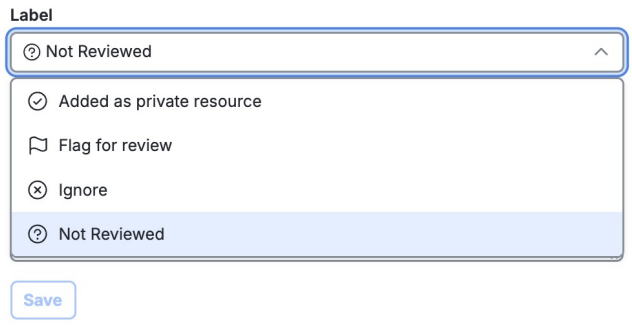


3. Locate the chosen resource and click the **View Suggestions arrow (→)** to review the Matching private resources section to identify potential matches.



4. You can perform the following actions:
   - **Add as new Private Resource**: Redirects you to the procedure for creating a new private resource.
   - **Ignore suggestion**: Applies the Ignore label to the suggestion.

5. Select a Label from the drop down list.



6. Enter any relevant Notes to provide context for the mapping.
7. (Optional) If not applicable, click **Ignore suggestion** to dismiss the match.

Test Private Resource Reachability

Provides instructions for completing the Test Private Resource Reachability workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Test the connection between Secure Access and your private resources. View the details of an existing private resource, then verify Secure Access can reach it.

Before you begin

Reachability testing may only be used to test private resources with the following configuration:

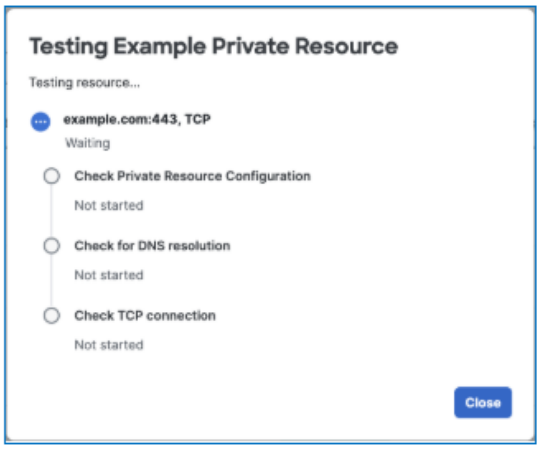
- Under **Communication with Secure Access Cloud**, one or more rows must have an internally reachable address with only a single FQDN or IP address.
  - Internally reachable address fields with multiple FQDNs or IP addresses are not supported by reachability testing.
  - Subnets, IP address ranges, and FQDN wildcards are not supported by reachability testing.
- **Protocol** must include TCP. Reachability testing supports the protocol options **TCP – (HTTP/HTTPS) only**, **Any TCP**, and **Any TCP, Any UDP**.
- **Port / Ranges** must be configured with one and only one port.
- Under **Endpoint Connection Methods**, reachability testing only supports Zero-trust connections.

Procedure

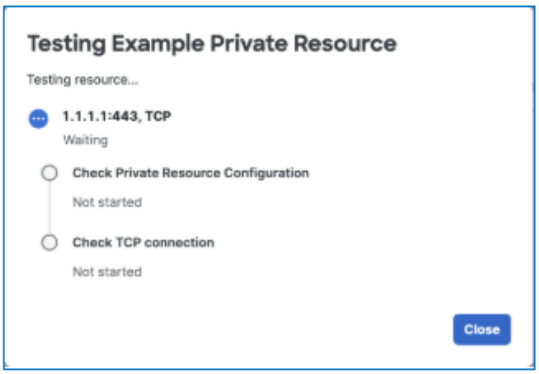
1. Navigate to **Resources** > **Private Resources**.
2. In the **Private Resources** tab, click the name of an existing private resource with a **Connection Method** of Client-based ZTA or Browser-based ZTA. The resource detail menu will open to the right of the resource list.
3. Scroll to the bottom of the detail menu and click **Test Reachability**.



4. The **Testing** menu will show the name of the resource and the tests performed.



FQDN test including DNS resolution



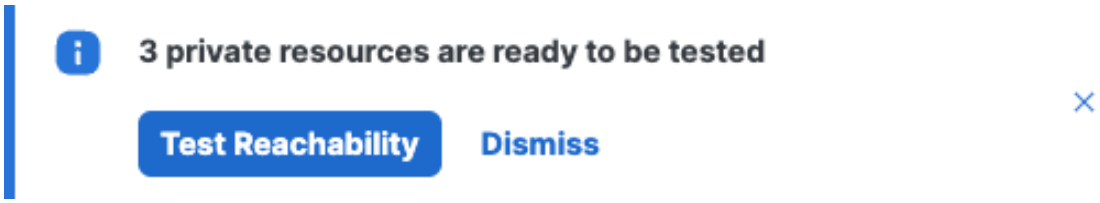
IP address test without DNS resolution

- **Resource tested, all addresses reachable:** Secure Access can reach your new private resource.
- **Resource tested, no addresses reachable:** Secure Access failed to reach your private resource due to one of the following error conditions. Follow the error message instructions to troubleshoot.
  - **Check Private Resource configuration:** This resource will be ready to test soon. Please try again in a few minutes.
  - **Check for DNS resolution:** Check your DNS server connectivity and configuration. For more information, see Manage DNS Servers. **Note:** Secure Access tests DNS resolution for an internally reachable FQDN but skips this test for an internally reachable IP address.
  - **Check TCP connection:**
    - **Unable to forward traffic to the resource:** Check your Resource Connector Group and the connector configurations, or your network configuration and resource. For more information, see Assign Private Resources to a Connector Group.
    - **'[Network Tunnel Group-name]' was unable to route traffic to this resource:** Check your Network Tunnel Group and tunnel configurations to ensure that traffic from tunnels can reach the resource. For more information, see Manage Network Tunnel Groups.
    - **No connectivity to this resource was found:** Either associate a Resource Connector Group with this resource or configure a Network Tunnel Group that can route traffic to this resource. For more information, see Assign Private Resources to a Connector Group and Manage Network Tunnel Groups.

5. When you add a new private resource or edit one that satisfies the prerequisites for reachability testing, you will see the option to **Save and Test** or **Save**.



If you click **Save and Test**, the main **Private Resources** menu will display a banner when the private resource is ready to be tested. It can take two minutes before a private resource is ready to be tested.



The banner will persist until an administrator tests reachability with a result of **Resource tested, all addresses reachable** for all resources that are ready to be tested.

If any resources fail the reachability test, they will remain ready for testing in the banner menu.

If an administrator dismisses the banner by clicking **Dismiss** or **X**, the banner will reappear when the page is reloaded.

Add a Private Resource Group

Provides instructions for completing the Add a Private Resource Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can create private resource groups with private resources and use these components as destinations in private access rules in your Access policy, or in real-time rules in a DLP policy. Private resource groups enable you to apply access rules consistently to all resources in the group.

> **Warning**
>
> If you attach an empty private resource group to a policy, the entire rule containing the empty private resource is dropped.

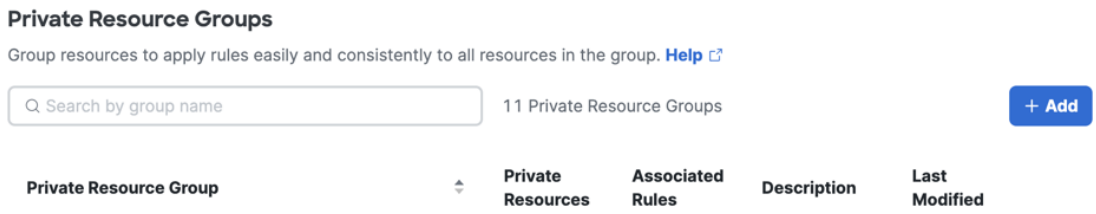
Configure a resource group with the private resources in your organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

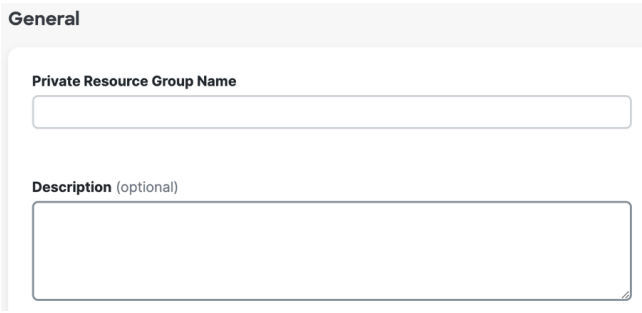
Procedure

1. Navigate to **Resources** > **Private Resources**.
2. Choose **Private Resource Groups**, and then click **+Add**.

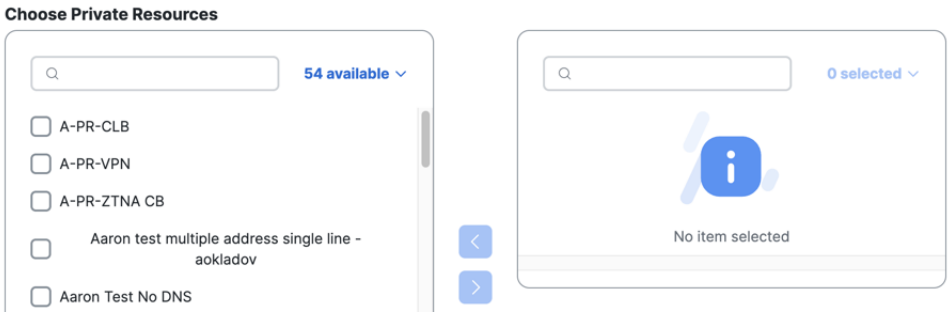


3. For **Private Resource Group Name**, enter a meaningful name for the resource group.
4. For **Description**, we recommend that you provide information about the purpose of the resource group.

> **Note**
>
> The description is optional.



5. For **Choose Resources**, add the resources to the group.
   a) For **Copy from existing private resource group**, choose a resource group name to add the resources in that group to your new resource group.
   b) For **Choose Private Resources**, check the resources and click the **arrow (greater than sign)** to add the selected resources to the group.



6. Click **Save**.

Private Resource Configuration Examples

Describes Private Resource Configuration Examples in Cisco Secure Access. Use these examples for configuring private resources when using Resource Connector Groups to connect traffic.

Private Resource Located in Multiple Locations

Use these examples for configuring private resources when using Resource Connector Groups to connect traffic.

Suppose you have a private resource Application1 deployed in Location1 and Location2:

- If users will access using browser-based connections, create a separate private resource for each location.
- If users access the resource using different IP addresses in Location1 and Location2:

  Configure a separate private resource for each resource location, and associate each private resource with a resource connector group in the appropriate region.
- If the private resource is defined using an FQDN that is common to Location1 and Location2:

  Configure a single private resource and associate the resource with different connector groups in different regions if applicable.

- If the private resource is accessed in both locations using the same IP address:

  Configure a single private resource and associate the resource with different connector groups in different regions if applicable.

- If the private resource is defined with multiple IP addresses, and it is accessible in any location using any of the addresses:

  Configure a single private resource with multiple entries for "Internally reachable address." Associate the resource with different connector groups in different regions if applicable.

Catch-All Private Resource to Prevent Exposing Internal Networks

Connection requests by remote devices, including requests for private resources, are typically resolved using public DNS, exposing information about those requests to the public internet. Connection requests for private destinations that are enabled for client-based Zero Trust Access do not go through public DNS and thus do not expose this information.

To avoid exposing information about your network to the public internet via DNS requests:

Add a private resource for your namespace, following the model ***.example.com**, for Any TCP, Any UDP, for all ports, and enable client-based Zero Trust Access for this resource. This creates a traffic steering rule that routes all client-based traffic to any destination in your namespace through Zero Trust Access. You do not need to create an access rule specifically for this resource, because the default private access rule will block access unless another access rule applies.

15 Connections to Private Destinations

Topics:

- Manage Connections to Private Destinations
- Manage Branch Connections
- Allow SSH and RDP Access to Private Resources
- Application Portal for Zero Trust Access Browser-Based User Access

Provides an overview of Connections to Private Destinations in Cisco Secure Access, including Manage Connections to Private Destinations, Manage Branch Connections, and Allow SSH and RDP Access to Private Resources. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Connections to Private Destinations

Describes Manage Connections to Private Destinations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports several types of connections to private resources:

- **Zero Trust Access** (ZTA) –Sometimes called Zero Trust Network Access (ZTNA)
  - **Client-based**
  - **Browser-based**
- **VPN**–Remote Access Virtual Private Network
- **Branch Network**–Access to private destinations while on a branch network.

For details, see:

- Comparison of Zero Trust Access and VPN
- Comparison of Client-Based and Browser-Based Zero Trust Connections
- Manage Branch Connections

You will enable connection options for each private resource when you configure the resource. You can enable any or all of these options for each private resource.

If you enable both zero-trust and VPN connections for a resource, users will connect to the resource using zero trust. For details, see Connection Scenarios for Private Destinations.

Using Private Resources for SaaS Internet Destinations

Describes Using Private Resources for SaaS Internet Destinations in Cisco Secure Access. You can configure a private resource to ensure specific egress IP addresses for traffic to specific SaaS internet destinations outside your network, such as YourCompany.OtherCompany.com.

You can configure a private resource to ensure specific egress IP addresses for traffic to specific SaaS internet destinations outside your network, such as *YourCompany.OtherCompany.com*. For details, see Zero Trust Access to Internet Destinations.

Comparison of Zero Trust Access and VPN

Describes Comparison of Zero Trust Access and VPN in Cisco Secure Access. Cisco Zero Trust Access is an alternative to VPN for secure remote access connections to configured private resources.

Cisco Zero Trust Access is an alternative to VPN for secure remote access connections to configured private resources. You can allow either or both connection methods for each private resource.

Zero Trust Access security benefits

- Zero Trust Access is enabled for each private resource.
- Remote users connect to specific private resources rather than to an entire network, minimizing risk surface area.
- An attacker who breaches a device or zero-trust connection cannot glean information about your internal network
- You can allow authorized users of unmanaged devices to connect to specific resources without granting them access to your network. You will enable browser-based zero trust access for those resources, then distribute a dummy URL to those users, so the real address is not exposed. This solution lets you securely provide browser-based access to end users such as:
  - contractors, vendors, trainers, outside legal counsel, and others.
  - employees on leave

- End-users' endpoint/device posture is evaluated continuously to verify that the end-user device meets requirements. Posture can be assessed each time they access a resource, rather than just once when they join the network.
- When access to a resource is blocked, client-based users see a block page rather than a browser time-out error.
- Simpler setup than VPN.

Zero Trust Access end user benefits

- Remote users can connect to internal resources in situations where they cannot use VPN. For example, an employee who is visiting a customer or vendor site can connect.
- Users do not need to log in separately to the network before they can access resources configured for zero trust access.
- After a user with a managed device has completed initial setup of Cisco Secure Client, the user has the same experience accessing a resource whether in the office or working remotely.
- Faster performance than VPN.

When to enable VPN

- To allow end users to connect to all resources on the network that are not configured to disallow VPN access.
- To enable connections to private destinations that are not configured as private resources.
- To enforce some endpoint requirements that are not currently available in client-based zero-trust posture profiles.
- While transitioning your organization to Zero Trust Access.
- For traffic that cannot be connected using Zero Trust Access, including traffic to applications that don't meet the requirements in Requirements for Zero Trust Access.

Timeout Intervals for Zero Trust Access Sessions

Describes Timeout Intervals for Zero Trust Access Sessions in Cisco Secure Access. Cisco Secure Access Zero Trust Access (ZTA) provides secure, remote connectivity for end users to configured private resources and internet destinations.

Cisco Secure Access Zero Trust Access (ZTA) provides secure, remote connectivity for end users to configured private resources and internet destinations. This guide is a reference that describes the Secure Access ZTA session timeout intervals for end users.

About Zero Trust Access Sessions

While a client using Secure Access ZTA exchanges network traffic on private resources or internet destinations, the client's ZTA session is active. Secure Access proxies the network traffic on the ZTA session to the private resources or internet destinations. When an end user's ZTA connection is not in use for a specific time period, the client's ZTA session expires.

Secure Access manages the timeout intervals of the ZTA sessions for the Cisco Secure Client. After a user's ZTA session expires and then the Secure Client requests a private resource or internet destination, Secure Access reconnects the session automatically and transparently for the end user.

Secure Access determines when the ZTA session timeout occurs based on the session's network traffic, IPS and file malware scanning settings enabled in the Access policy, and the protocol and ports used to connect to the private resources or internet destinations.

> **Note**
>
> For browser-based Secure Access ZTA, browsers manage the ZTA sessions and timeout intervals transparently.

ZTA Connections to Private Resources

Describes ZTA Connections to Private Resources in Cisco Secure Access. An end-user's ZTA session with the Cisco Secure Client times out periodically.

An end-user's ZTA session with the Cisco Secure Client times out periodically. Secure Access determines the ZTA session timeout interval based on the ports and protocol where the Secure Client connects to the private resources.

Secure Access supports these session timeout intervals for connections to private resources.

Protocol and Ports	ZTA Timeout Interval
UDP	300 seconds
TCP ports 80/443	1200 seconds
All TCP ports except 80/443	3600 seconds

ZTA Connections to Private Resources with IPS or File Malware Scanning

Describes ZTA Connections to Private Resources with IPS or File Malware Scanning in Cisco Secure Access. An end-user's ZTA session with the Cisco Secure Client times out periodically.

An end-user's ZTA session with the Cisco Secure Client times out periodically. Secure Access determines the ZTA session timeout interval based on the ports and protocol where the Secure Client connects to the private resources. Whether the organization configures IPS or file malware scanning on the private resources also contributes to the session timeout interval.

Secure Access supports these session timeout intervals for connections to private resources with IPS or file malware scanning.

Protocol and Ports	ZTA Timeout Interval
UDP	30 seconds
TCP ports 80/443	1200 seconds
All TCP ports except 80/443	3600 seconds

ZTA Connections to Internet Destinations

Describes ZTA Connections to Internet Destinations in Cisco Secure Access. An end-user's ZTA session with the Cisco Secure Client times out periodically.

An end-user's ZTA session with the Cisco Secure Client times out periodically. Secure Access determines the ZTA session timeout interval based on the ports and protocol where the Secure Client connects to internet destinations.

Secure Access supports these session timeout intervals for connections to internet destinations.

Protocol and Ports	ZTA Timeout Interval
UDP	30 seconds
TCP ports 80/443	1200 seconds
All TCP ports except 80/443	3600 seconds

Comparison of Client-Based and Browser-Based Zero Trust Access Connections

Describes Comparison of Client-Based and Browser-Based Zero Trust Access Connections in Cisco Secure Access. You can configure users to connect to private resources using Zero Trust Access.

You can configure users to connect to private resources using Zero Trust Access.

About Client-Based Connections

- The Cisco Secure Client is installed on the end-user device.
- Users can access resources using any protocol.
- Users access using the internal resource address you specify in the Private Resource.
- The client-based posture profile offers more options for controlling endpoint (device) requirements than the browser-based posture profile offers.
- You can block access to specified subdomains when the resource address for client-based connections is configured as a wildcard FQDN. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.
- If traffic is blocked, the user sees a Block page if all requirements are met. For more information, see Block pages for Private Resources.

About Browser-Based Connections

- Access does not require a client installed on the user endpoint device.
- Use this option to allow access from devices with an operating system that the client does not support.
- You can enable this option for private resources to allow connections from users who do not have managed devices, such as contractors, vendors, and others with bring-your-own (BYOD) devices, and from devices that do not have a client. You do not need to install anything on such devices.
- Access is solely from the browser.
- Users access private resources using a dummy URL that does not expose your actual resource address. Secure Access redirects browser-based traffic to the actual resource if access rules allow the traffic.
- You can specify endpoint (device) requirements for these connections, but fewer than in the client-based posture profile.
- If traffic is blocked, the user sees only a standard browser error. This prevents bad actors from obtaining information about your resources.
- Users who have the client installed can always access a resource using the clientless browser-based URL if your access rules allow them access.
- The Browser-Based Connection (BAP) session timer limits any BAP session to a maximum of thirty minutes.

Requirements for Zero Trust Access

Describes Requirements for Zero Trust Access in Cisco Secure Access and explains Resource Requirements for Client-Based Zero Trust Access, Resource Requirements for Browser-Based Zero Trust Access, and Network Requirements for Zero Trust Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Resource Requirements for Client-Based Zero Trust Access

A resource that you want users to reach using zero trust access must meet the following requirements:

- Does not serve client-to-client traffic.

  Example: Peer-to-peer Voice over IP (VoIP).

- Does not serve server-to-client traffic.

  Example: Remote assistance.

- Does not require a unique client IP address.

Example: Applications that use the SMBv1 protocol.

- Does not perform an ICMP connectivity check before connecting using TCP or UDP.
- Does not have any dependencies that have any of the above conditions.
- All of the resource's dependencies and any redirects must be also be defined as private resources with client-based zero trust access enabled.

Resource Requirements for Browser-Based Zero Trust Access

- Cisco recommends using a certificate signed by a publicly recognized certificate authority (CA).
- The resource must not serve content or links using absolute URLs. All site content must be referenced using relative URL paths.

Network Requirements for Zero Trust Access

See the Zero Trust client-based access sections in Network Requirements for Secure Access.

Client Requirements for Client-Based Zero Trust Access

For more information, see Zero Trust Access Requirements and Limitations on page 1207.

Configure Client-Based Zero Trust Access for Private Destinations

Describes Configure Client-Based Zero Trust Access for Private Destinations in Cisco Secure Access. Client-based Zero Trust Access is generally used by employees of your organization who are authenticated by your organization's identity providers and who are using devices that are managed by your organization.

Client-based Zero Trust Access is generally used by employees of your organization who are authenticated by your organization's identity providers and who are using devices that are managed by your organization.

To understand and configure client-based Zero Trust Access for private destinations, review the following topics:

1. Understand Zero Trust Access in general and client-based zero trust access specifically. For more information, see Manage Connections to Private Destinations and relevant subtopics including the comparison topics and the relevant parts of Requirements for Zero Trust Access.
2. Configure one or more private resources to allow client-based Zero Trust Access connections. For more information, see Add a Private Resource.
3. Define requirements for user endpoint devices for client-based Zero Trust Access connections. For more information, see Add a Client-Based Zero Trust Access Posture Profile on page 1250.
4. Understand Network Authentication for Zero Trust Access and configure the default user authentication interval for private access rules in Rule Defaults: Default Settings for Access Rules.
5. Make sure you have set up Network Tunnels or Resource Connectors to connect user traffic. For more information, see Manage Network Connections and subtopics.
6. (Optional) Modify zero trust access traffic steering rules if necessary. For more information, see important information at Traffic Steering for Zero Trust Access Client-Based Connections. Traffic steering rules are added automatically when you enable a private resource for client-based zero trust access.
7. Create at least one private access rule that specifies a private resource or other destination that has been added to the Traffic Steering page. For more information, see Get Started With Private Access Rules and subtopics.
8. Configure user authentication. For more information, see Manage User Authentication Profiles.
9. Install Cisco Secure Client on user endpoint devices and enroll those devices in Zero Trust Access. For more information, see the relevant topics under Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices.

10. Test your configurations.

Configure Browser-Based Zero Trust Access to Private Resources

Describes Configure Browser-Based Zero Trust Access to Private Resources in Cisco Secure Access. Browser-based access to your internal applications allows authorized user endpoint devices that are not managed by your organization to securely access internal resources.

Browser-based access to your internal applications allows authorized user endpoint devices that are not managed by your organization to securely access internal resources. For more details, see Comparison of Client-Based and Browser-Based Zero Trust Access Connections.

> **Note**
>
> User endpoint devices do not require the Cisco Secure Client with the Zero Trust Access module.

The following configurations apply to browser-based access to a private resource:

- Requires a browser. For more information, see Requirements for Zero Trust Access.
- Configure the private resource:
  - The internally reachable address must be available via HTTP or HTTPS.
  - Browser-based zero trust access must be enabled.
  - Define the URL that users will use to access the resource.
  - Other settings may be required or optional for your environment. For more information, see Add a Private Resource.
  - An identity certificate signed by a publicly recognized certificate authority (CA) should be installed on the resource. If you install a certificate signed by your corporate CA, you must install the root certificate of your corporate certificate authority in the trust store of the user endpoint device.
- Configure endpoint requirements in the default posture profile for browser-based zero trust access, or create a different posture profile for this purpose. For more information, see Add a Browser-Based Zero Trust Access Posture Profile.
- Configure user authentication. For more information, see Manage User Authentication Profiles.
- Add a private access rule to grant access to authorized users. Optionally, choose a posture profile other than the default. See Get Started With Private Access Rules and subtopics.
- Give users the special URL you configured in the private resource for browser-based access.

Network Authentication for Zero Trust Access

Describes Network Authentication for Zero Trust Access in Cisco Secure Access. In addition to any other authentication requirements you configure, you can require end users to re-authenticate themselves at an interval that you choose before they can connect to private resources using Zero Trust Access.

In addition to any other authentication requirements you configure, you can require end users to re-authenticate themselves at an interval that you choose before they can connect to private resources using Zero Trust Access.

End users need to sign in only once during the interval you specify; after signing in, users can connect to any private resources that are enabled for Zero Trust Access, when rules allow access. When the interval ends, users must sign in again to regain Zero Trust Access to allowed private resources for the specified period of time.

iOS devices do not support this feature. You must disable this feature in access rules that will apply to iOS users, or users of iOS devices will be unable to access resources. Users of iOS devices will not be able to re-authenticate after initial authentication.

You will want to balance security needs with end-user convenience. For example, for some applications, you may want to require that users re-authenticate daily, while for others, once a week may be enough.

The interval specified on the Rule Defaults page is used by default for all new private access rules. To set or change the default interval, see Important Information About Changing Rule Defaults and Edit Rule Defaults and Global Settings.

For each private access rule that includes at least one private resource as a destination, you can choose to use the default interval or specify a different interval. See Add a Private Access Rule.

These authentication options are in addition to any sign-in requirements required by mechanisms outside of Secure Access, such as those required to access individual resources. The User Authentication Interval setting is unrelated to device enrollment in Zero Trust Access, including enrollment renewal.

If you disable this authentication option, users are never prompted to sign in again after they have authenticated once.

Connection Scenarios for Private Destinations

Describes Connection Scenarios for Private Destinations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

If both the client-based zero trust and VPN options are enabled for the resource:

- If the client is installed on the user device and enrolled for zero trust access, the connection uses client-based zero trust access. Otherwise, the connection uses VPN.
- If a client that is enabled for zero trust access cannot reach a resource that is configured for client-based zero trust access, the system does not attempt to connect using VPN.

If a private resource is not configured in Secure Access but the VPN client is installed on the end-user device, the user can access the resource using VPN if:

- A VPN traffic steering rule routes traffic to the applicable network address space
- A private access rule allows traffic to the applicable network address space

If a user accesses a resource with their browser using the address configured in a private resource for that purpose, the connection will always use browser-based zero trust access, even if Cisco Secure Client is installed.

If a private access rule allows traffic to a destination that is not configured as a private resource, for example the destination is entered directly in a private access rule: Traffic may use zero trust access if a traffic steering rule for the destination has been added to the list on the **Connect** > **End User Connectivity** > **Zero Trust** page.

Manage Branch Connections

Describes Manage Branch Connections in Cisco Secure Access. Secure Access protects users and devices that are connected on an organization's branch and internal networks.

Secure Access protects users and devices that are connected on an organization's branch and internal networks. An enterprise may have multiple branch offices distributed across various geographical locations. Each branch office may allow connections only to certain applications and services managed by the organization and block connections to other private resources.

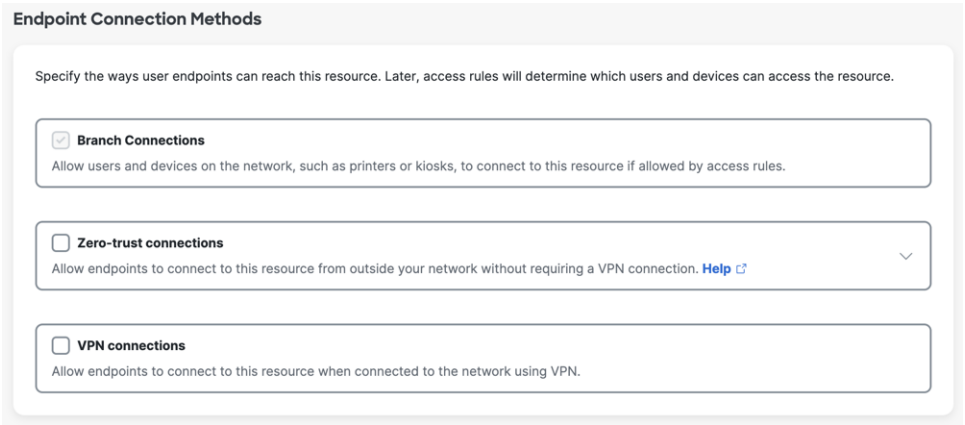
When on a branch network protected by Secure Access, users and devices can connect seamlessly to the internet and private applications and services. You can control how users and devices connect to private resources by adding private access policy rules for network sources and destinations. For example, you can define policy rules that block or allow access to private resources from IOT devices, kiosks, or printers.

Endpoint Connection Methods

Describes Endpoint Connection Methods in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports various types of network connections to private resources:

- **Branch connections**
- **Zero-trust connections**
- **VPN connections**



When you add a private resource to Secure Access, Secure Access automatically enables **Branch Connections** to the private destination. For information about Zero Trust and VPN connections, see Manage Connections to Private Destinations.

A Branch network may represent an IP or CIDR address of a router or device in your enterprise. You can configure Branch networks to connect through a Network Tunnel Group to a private resource. For more information about Network Tunnel Groups, see Manage Network Tunnel Groups.

Branch Networks in Private Access Rules

Describes Branch Networks in Private Access Rules in Cisco Secure Access. Once you add a private resource to Secure Access for your organization, you can configure private access rules that protect the branch connections to your private resources.

Once you add a private resource to Secure Access for your organization, you can configure private access rules that protect the branch connections to your private resources. A private access rule may include branch networks in both source and destination components. For more information, see Add a Private Access Rule.



Users and Groups Connections to Private Resources

Describes Users and Groups Connections to Private Resources in Cisco Secure Access. Users, groups, and devices on your corporate networks, including branch offices, can always connect to a private resource if allowed by private access rules.

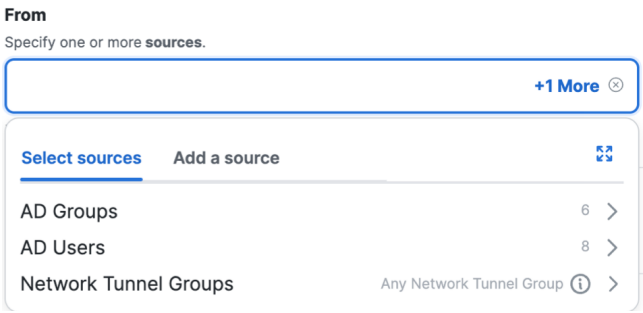
Users, groups, and devices on your corporate networks, including branch offices, can always connect to a private resource if allowed by private access rules. When users, groups, and user devices connect to private resources from a branch network, Secure Access does not evaluate the device's endpoint posture.

Sources for Branch Network Connections

Describes Sources for Branch Network Connections in Cisco Secure Access. In your private access rules, select the sources that you configured for your organization, or add individual branch or internal network IP or CIDR addresses.

In your private access rules, select the sources that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Sources.

- **Users**–Users appear in private access rules after you add them to your organization.
- **Groups**–Groups appear in private access rules after you add them to your organization.
- **Network Tunnel Groups**–Network Tunnel Groups appear in private access rules after you add them to your organization. The source is identified by the Network Tunnel Group ID.
- **IP** or **CIDR**–A branch or internal network's IP or CIDR address that you add to the access rule. The source is only available in the access rule.

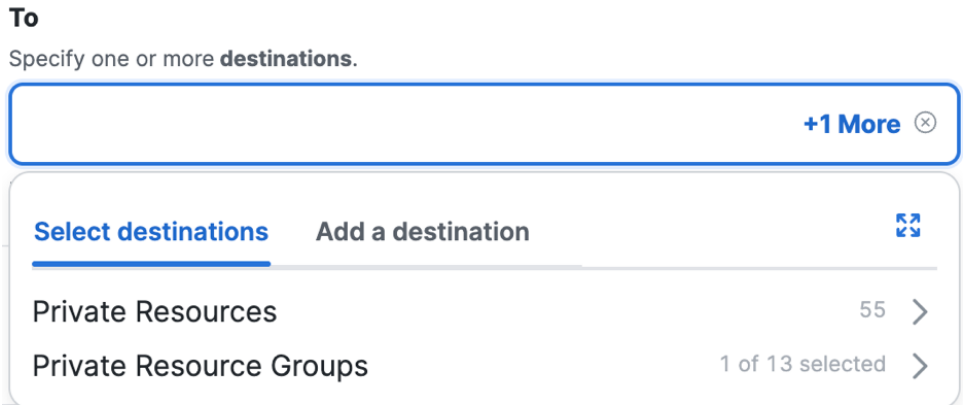


Destinations for Branch Network Connections

Describes Destinations for Branch Network Connections in Cisco Secure Access. In your private access rules, select the destinations that you configured for your organization, or add individual branch or internal network IP or CIDR addresses.

In your private access rules, select the destinations that you configured for your organization, or add individual branch or internal network IP or CIDR addresses. For more information, see Add a Private Access Rule: Destinations.

- **Private Resources**–Private Resources appear in private access rules after you add them to your organization. The destination component is an IP, CIDR, fully-qualified domain name (FQDN), port, and protocol.
- **Private Resource Groups**–Private Resource Groups appear in private access rules after you add them to your organization. The destination component is an IP, CIDR, fully-qualified domain name (FQDN), port, and protocol.
- **IP** or **CIDR**, **Port**, **Protocol**–A branch or internal network's IP or CIDR address, port, and protocol that you add to the access rule. The destination is only available in the access rule.



Source Connections to Destinations

Describes Source Connections to Destinations in Cisco Secure Access. Secure Access supports connections from Branch network source components to various destination components.

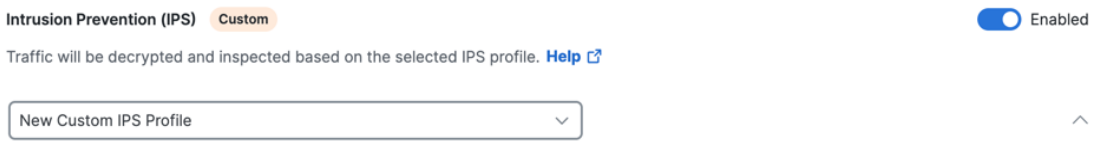
Secure Access supports connections from Branch network source components to various destination components.

Source	Private Destination
Network Tunnel Group	• Private Resource Group • Private Resource
IP or CIDR (Branch network) defined on the private access rule.	• Private Resource Group • Private Resource • IP or CIDR (Branch network) defined on the private access rule.
IP or CIDR (Internal network) defined on the private access rule.	IP or CIDR (Internal network) defined on the private access rule.

Add an IPS Profile on Private Access Rules

Describes Add an IPS Profile on Private Access Rules in Cisco Secure Access. When you add a private access rule that includes branch connections to private resources, configure the security controls on the rule by adding an IPS profile.

When you add a private access rule that includes branch connections to private resources, configure the security controls on the rule by adding an IPS profile. For more information, see Add a Private Access Rule: Configure Security Control Options.



Secure Access protects branch connections to private resources, internal networks, and other branch networks through the Intrusion Prevention System (IPS) profile. For more information, see Manage IPS Profiles.

Log Connections From Branch Networks to Private Resources

Describes Log Connections From Branch Networks to Private Resources in Cisco Secure Access. Secure Access logs every connection and event from a branch network to a private application, service, internal network, or branch network.

Secure Access logs every connection and event from a branch network to a private application, service, internal network, or branch network. The events are recorded in the Admin Audit log. Secure Access enforces access to private applications and follows industry compliance and security standards. For more information, see Manage Logging.

Allow SSH and RDP Access to Private Resources

Describes Allow SSH and RDP Access to Private Resources in Cisco Secure Access. Secure Access Packages and Feature Availability.Not all of the features described here are available to all Secure Access packages.

> **Note**
>
> Secure Access Packages and Feature Availability.
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the **Admin** > **Licensing** page. For more information, see Determine Your Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. See also, Cisco Secure Access Packages

You can allow Zero Trust Access to private resources using SSH and Microsoft's Remote Desktop Protocol (RDP).

> **Note**
>
> You can set your keyboardlayout to an alternate language upon logging into your RDP. If you opt to switch the input method for your keyboard, the keyboard layout is in effect until you log out or the session terminates. You must reselect the language preference the next time you or a user logs into the remote desktop. This option supports browser-based RDP access only.

Browser-Based Zero Trust Access

Describes Browser-Based Zero Trust Access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Configuration overview: Browser-based zero trust access using SSH or RDP
- Notes for browser-based SSH and RDP access
- Supported option for SSH access

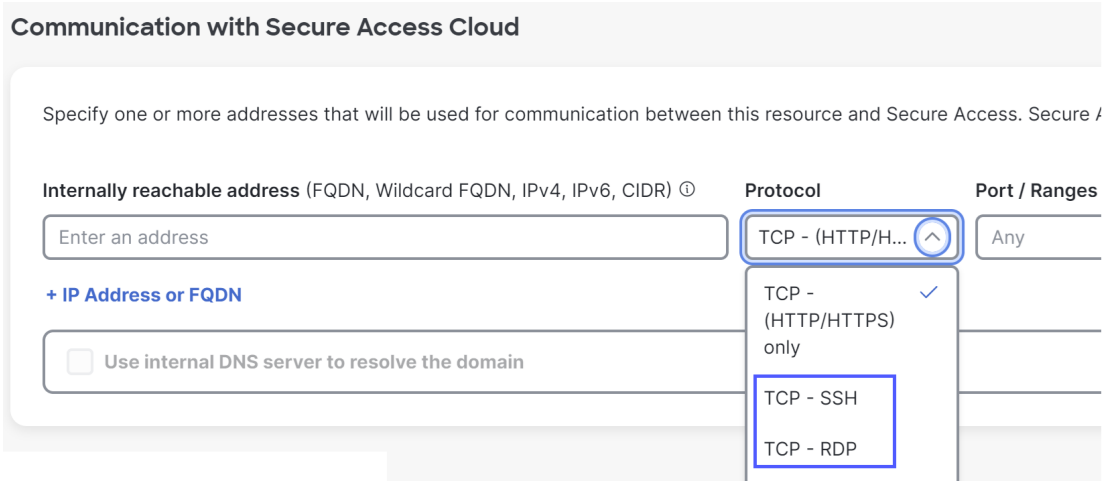
Configuration overview: Browser-based zero trust access using SSH or RDP

Provides instructions for completing the Configuration overview: Browser-based zero trust access using SSH or RDP workflow in Cisco Secure Access. If you are using older SSH servers, see Details: Supported options for SSH.

Use the following procedure to allow clientless browser-based Zero Trust Access to private resources using SSH or RDP:

Procedure

1. If you are using older SSH servers, see Details: Supported options for SSH.
2. Configure your private resource:
   a. Allow access using the applicable protocol for the internally reachable address. See Add a Private Resource.



Note

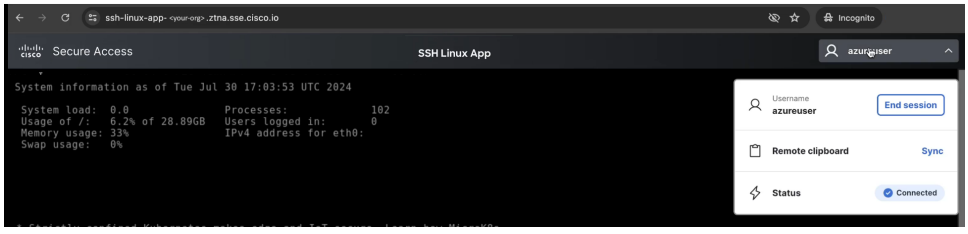
The resource name will appear at the top of your users' SSH or RDP window.

3. In the Private Resource, enable Zero-trust connections, then enable and configure browser-based connections.
4. Follow the instructions for granting access to private destinations in Get Started With Private Access Rules.
5. If your environment has a web proxy or firewall between end user browsers and the Secure Access cloud, you must allow websocket access on port 443 from your users' browsers to Secure Access.
6. When you give users the applicable SSH or RDP credentials or private key for the resource, also provide the public URL for browser-based Zero Trust Access that you configured on the Private Resource page. Neither Secure Access nor the browser stores the credentials or private key.

Notes for browser-based SSH and RDP access

Describes Notes for browser-based SSH and RDP access in Cisco Secure Access. For limits on the number of user sessions, see the Service Connections section in Limitations and Range Limits.

- For limits on the number of user sessions, see the Service Connections section in Limitations and Range Limits.
- You can set your keyboardlayout to an alternate language upon logging into your RDP. If you opt to switch the input method for your keyboard, the keyboard layout is in effect until you log out or the session terminates. You must reselect the language preference the next time you or a user logs into the remote desktop. This option supports browser-based RDP access only.
- For those who configure a private resource to use RDP, logging into your RDP presents the option to select an alternate language for your keyboard layout. This election remains in effect until the end of the session. At this time we support English, French, German, Chinese, and Hindi.
- The user experience will look like this:



- SSH and RDP users can paste text copied from their local machine by using the remote clipboard feature, shown in the image above. Follow these steps in order for each text string that needs to be copied and pasted:
  1. Copy text on your local machine.
  2. Click **Sync** to the right of the Remote clipboard menu item in the browser-based SSH or RDP session.
  3. Paste into the remote session.

  > **Note**
  >
  > The **Sync** button is not necessary when copying from the remote session to your local machine.

- RDP users will not be able to upload files or images.

Supported options for SSH access

Describes Supported options for SSH access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Most SSH connections will be successful. If you are using older SSH servers, the following options are supported.

Key Exchange (KEX)	Symmetric Cipher	Message Authentication Code (MAC)	Server Host Key Algorithm	Compression Schemes	Authentication
diffie-hellman-group-exchange-sha256	aes256-gcm@openssh.com	hmac-sha2-512	ssh-ed25519	zlib	password
diffie-hellman-group1-sha1	aes128-gcm@openssh.com	hmac-sha2-512-etm@openssh.com	ssh-ed25519-cert-v01@openssh.com	zlib@openssh.com	public key
diffie-hellman-group14-sha1	hmac-sha2-256	hmac-sha2-256	ecdsa-sha2-nistp521	none	n/a
diffie-hellman-group-exchange-sha1	hmac-sha2-256-etm@openssh.com	hmac-sha2-256-etm@openssh.com	ecdsa-sha2-nistp384	n/a	n/a
n/a	hmac-sha1	hmac-sha1	ecdsa-sha2-nistp256	n/a	n/a
n/a	hmac-sha1-96	hmac-sha1-96	ssh-rsa	n/a	n/a
n/a	hmac-md5	hmac-md5	ssh-dss	n/a	n/a
n/a	hmac-md5-96	hmac-md5-96	n/a	n/a	n/a
n/a	hmac-ripemd160 (hmac-ripemd160@openssh.com)	hmac-ripemd160 (hmac-ripemd160@openssh.com)	n/a	n/a	n/a

Client-Based Zero Trust Access

Describes Client-Based Zero Trust Access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Client-based SSH and RDP access does not require special configurations. No user experience specific to Secure Access is required.

Application Portal for Zero Trust Access Browser-Based User Access

Describes Application Portal for Zero Trust Access Browser-Based User Access in Cisco Secure Access. Provide your users with an application portal that displays links to private resources that are enabled for browser-based Zero Trust Access.

Provide your users with an application portal that displays links to private resources that are enabled for browser-based Zero Trust Access.

If you do not set up this portal, you must give browser-based users a special link for each resource. These links are created during private resource configuration.

The application portal lets you give users just the one URL for the portal, simplifying browser-based user access to these resources and streamlining administrative overhead.

All private resources that are configured to appear on the portal will be visible to all users who have access to the portal.

What Users Experience

1. Users point their browser to the portal URL that you provide.
2. Users sign in to Zero Trust Access.
3. The user sees all resources that are configured to be displayed in the portal.
4. The user clicks an application to open a new browser tab with that resource.

Prerequisites

Describes Prerequisites in Cisco Secure Access and explains Users and User Endpoint Devices Prerequisites and Application Portal Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Users and User Endpoint Devices Prerequisites

- Supported browsers
- Cisco Secure Client is NOT required on user devices.

Application Portal Prerequisites

- If you will upload a company logo for the portal or logos for applications, create or obtain graphics that meet these requirements:
- File type: PNG, transparent background recommended
- Size: 250 x 150 pixels
- All configurations required for browser-based zero trust access to a private resource must be completed before users can use the portal. This includes but is not limited to private resource configuration, posture profiles, user authentication, and access rules. See Configure Browser-based Zero Trust Access to Private Resources.

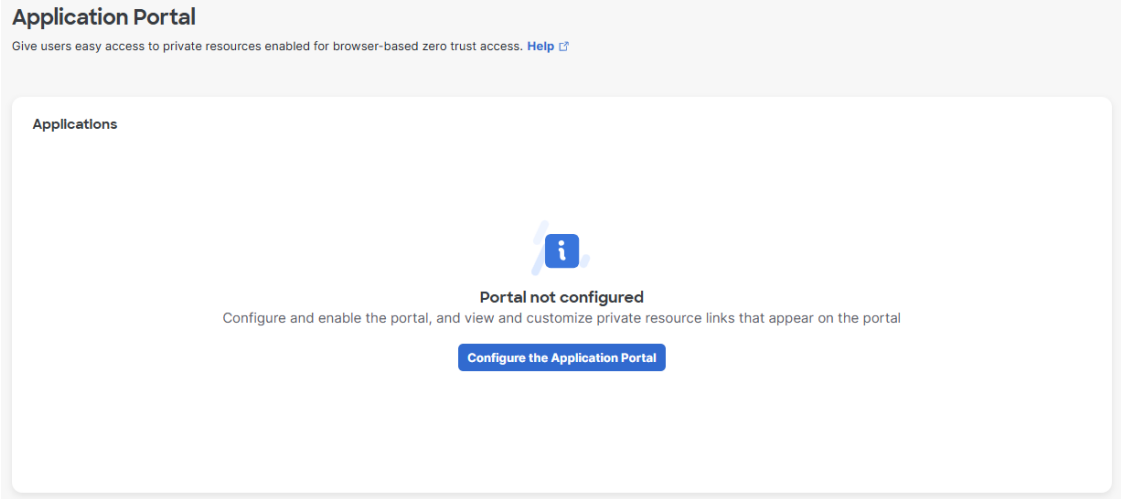
Configure an Application Portal for Zero Trust Access Browser-Based User Access

Provides instructions for completing the Configure an Application Portal for Zero Trust Access Browser-Based User Access workflow in Cisco Secure Access. Enable and configure the Application Portal: Navigate to Resources Destinations Application Portal and click Configure the Application Portal.

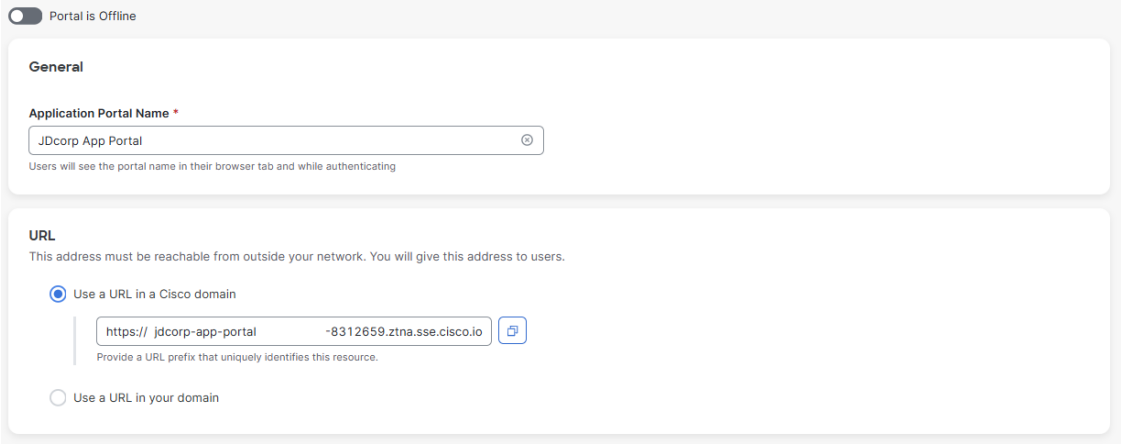
Procedure

1. Enable and configure the Application Portal:

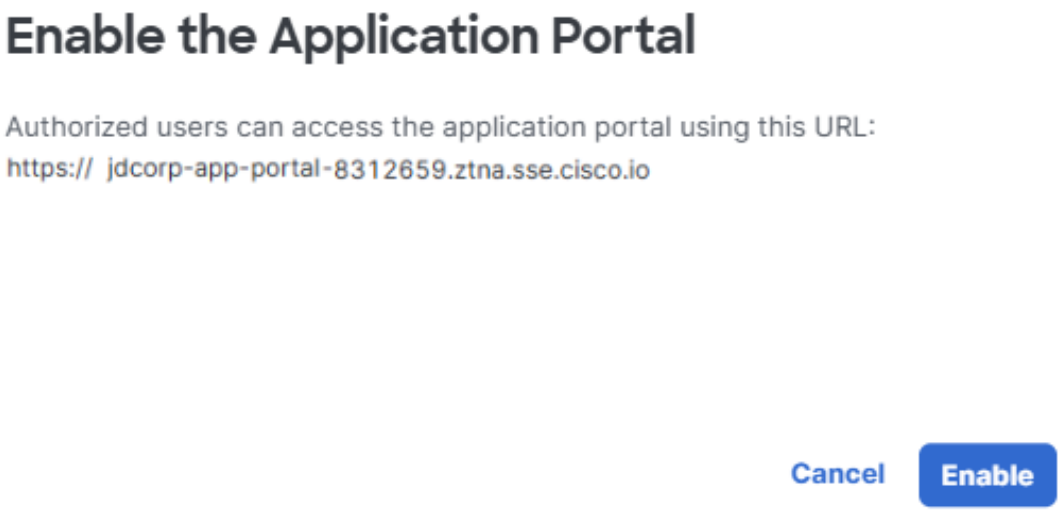
a. Navigate to **Resources** > **Destinations** > **Application Portal** and click **Configure the Application Portal**.



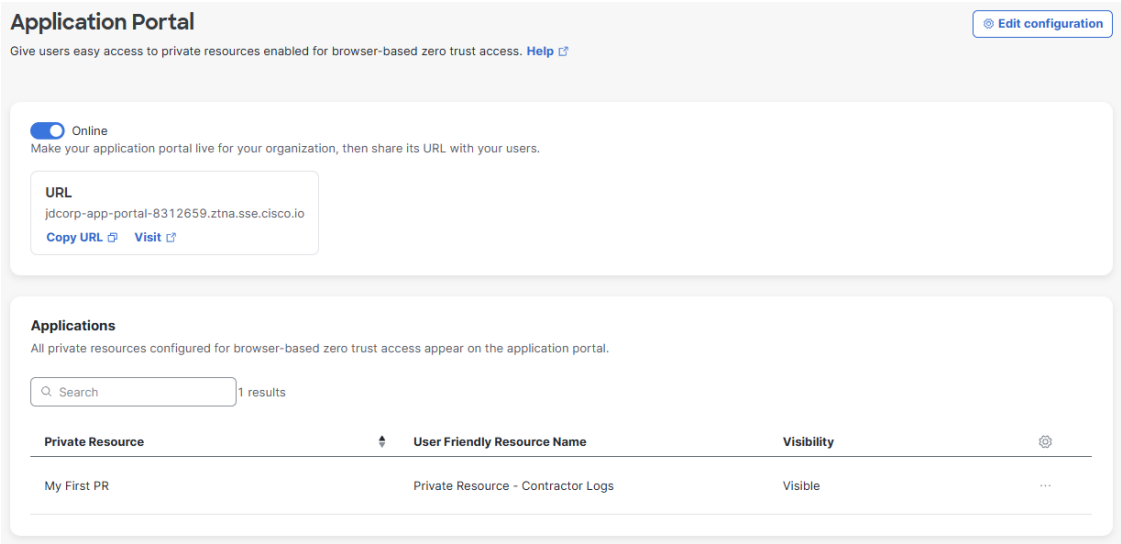
b. Enter an **Application Portal Name** and **URL** for the portal. The portal hostname/URL and alias must be unique.



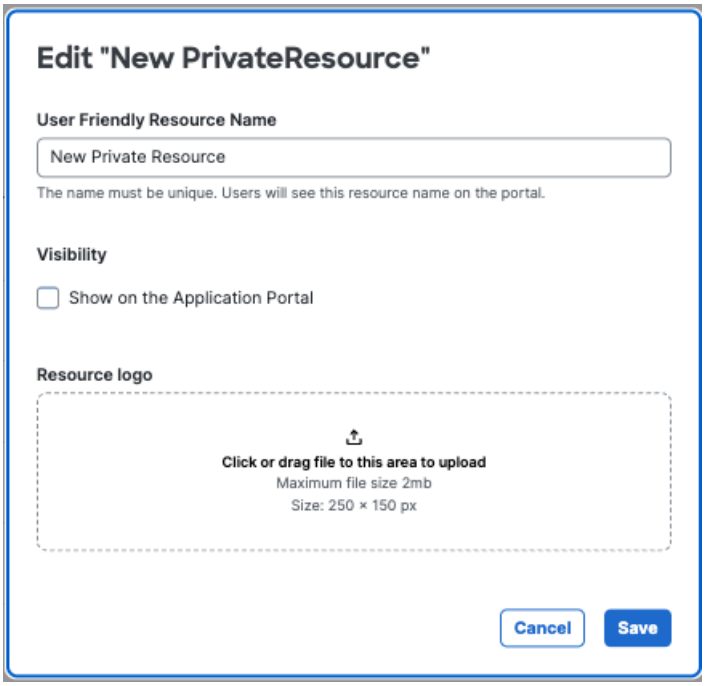
c. Enable the portal by sliding the activation toggle to right.



d. Click **Save** to enable the configured Application Portal. The server identity certificate should be signed by a public certificate authority unless you will install the validating root certificate in the trust store of user endpoint devices.



2. Configure each Private Resource that you want to appear on the portal:
   a. Enable browser-based Zero Trust Access.
   b. Select the option to display the resource on the application portal.
   c. Configure the application portal name and optional logo.



3. Create at least one private access rule to grant authorized users access to the portal itself.
   a. In the **Destinations** box, choose **Select Destinations** > **Private Resources** and select the **Application Portal Name** that corresponds to the portal you defined.
4. Ensure that the toggle at the top of the **Application Portal** configuration page is set to **Online**.
5. Distribute the portal URL to your users.

Filter Policies Based on Applications

Provides instructions for completing the Filter Policies Based on Applications workflow in Cisco Secure Access. You must have Admin permissions to execute the following procedure.

You can add or remove applications your access policy and thusly modify which applications are visible to your employees or end users. Allow or block users from certain applications by adding or removing applications as a private resource to a rule. You must configure an application portal for your ZTA experience first. See Application Portal for Zero Trust Access Browser-Based User Access for more information.

If you are unsure if an application is associated with a rule, navigate to **Resources** > **Settings** > **Destinations** > **Private Resources** and view what resources are associated to rules. You can view the applications currently available to your organization on the **Resources** > **Application Portal** page.

Before you begin

You must have the following already established before you start this procedure:

- You must have **Admin** permissions to execute the following procedure. See Edit Account Settings on page 192 for more information,
- You must have at least one rule associated to your access policy.
- You must have the application portal already configured for Zero trust Access browser-based access. See Application Portal for Zero Trust Access Browser-Based User Access for more information.
- You must have at least one application added to your application portal.

Procedure

1. In the Secure Access dashboard, navigate to **Secure** > **Access Policy**.
2. Locate and select the rule you want to update and edit it. You can do this by either selecting the checkbox by the rule name, clicking the ellipses icon (**...**) and clicking **Edit**; you can also click the **Rule Name** and clicking **Edit** from the pop-up window.
3. In the **Specify Access** section of the rule configuration page, in the **To** field, click **+ Add** to add an application as a private resource.

   To remove an application from a rule, click **+ Add** for the **To** field box and then manually remove the application of your choice.
4. **Save** the changes made to the rule. You can verify the changes by viewing the **Resources** > **Settings** > **Destinations** > **Private Resources** page and select the application you just added or removed. If added to a rule, the rule is included in the list of **Associated Rules**. If the application has been removed, it is not include in the list.

(Optional) Modify Settings

Describes (Optional) Modify Settings in Cisco Secure Access. After the portal is configured, you can view the private resources that have been configured to display on the portal, and optionally edit display settings.

- After the portal is configured, you can view the private resources that have been configured to display on the portal, and optionally edit display settings.
- To modify the portal configuration or certificate, click **Edit Configuration** in the top right corner of the Application Portal page.
- If you disable the portal (using the **Online** toggle at the top of the page), users can continue to access private resources if they have the direct URL that is defined for browser-based zero trust access on the resource's configuration page.

16 Network and Service Objects

Topics:

- Get Started with Network and Service Objects
- Manage Network Objects and Groups
- Manage Service Objects and Groups

Provides an overview of Network and Service Objects in Cisco Secure Access, including Get Started with Network and Service Objects, Manage Network Objects and Groups, and Manage Service Objects and Groups. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with Network and Service Objects

Describes Get Started with Network and Service Objects in Cisco Secure Access. Cisco Secure Access connects end users on networks to the internet and private destinations.

Cisco Secure Access connects end users on networks to the internet and private destinations. In Secure Access, administrators can add Network and Service Objects as resources and configure access rules with these resources in the Access policy.

When you include Network and Service Objects on the access rules, you can apply security controls on these resources for the organization.

About Network and Service Objects and Groups

Network Objects and Groups are reusable resources that you add in Secure Access either for the networks that end users will connect on to reach destinations or networks that end users will use to connect to from other networks.

Service Objects and Groups are reusable resources that you add in Secure Access for the applications that end users in the organization will connect to from private and public networks.

Benefits of Adding and Using Network and Service Objects

- **Reuse**–Include the network and service resources in any number of access rules in the Access policy.
- **Groups**–Manage groups of resources instead of single networks or services.
- **Observability**–View the reports for the traffic on the networks and to the networks and services.
- **Resource management**–Add, edit, duplicate, and delete large quantities of resources.
- **Protecting end users**–Apply pre-configured security controls on the Network and Service resources included in the access rules.

General Limits for Objects

- Secure Access supports adding up to 50000 Network Objects and 50000 Service Objects in an organization.

  The total number of Network or Service Objects includes any non-reusable objects that you add directly to a group.

- Secure Access supports the import of 1000 rows of object properties in a comma-separated values (CSV) file.

  The CSV file cannot exceed 10MB.

- Secure Access supports the selection of 10 objects and 10 groups in an access rule.
- Secure Access supports including up to 50000 objects in a group.
- The total number of objects referenced in the internet and private access rules combined cannot exceed 50000. For example, since the maximum number of rules that an organization can configure is 10000, if you have 10000 rules, you cannot configure more than 5 objects on each rule in the Access policy.

  The total number of objects referenced in the access rules includes the use of the same object in any number of access rules.

General Limits for Groups

- Secure Access supports adding up to 10000 Network Object Groups and 10000 Service Object Groups in an organization.
- Secure Access supports three levels of nested Network Object Groups and three levels of Service Objects Groups.
- Secure Access supports adding up to 1500 Network Object Groups in a Network Object Group.
- Secure Access supports adding up to 1500 Service Object Groups in a Service Object Group.

Network Objects and Network Object Groups

- For information about Network Objects, see Add a Network Object.
- For information about Network Object Groups, see Add a Network Object Group.
- For information about Importing Network Objects, see Import CSV File of Network Objects.

Service Objects and Service Object Groups

- For information about Service Objects, see Add a Service Object.
- For information about Service Object Groups, see Add a Service Object Group.
- For information about Importing Service Objects, see Import CSV File of Service Objects.

Quickstart: Network and Service Objects

Provides instructions for completing the Quickstart: Network and Service Objects workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes the high-level steps to get started with Network and Service Objects:

- Add Network and Service Objects in Cisco Secure Access.
- Select Network and Service objects on the internet and private access rules in the Access policy.
- Identify the traffic in the Activity Search report for the selected sources and destinations on the enforced access rules in the Access Policy.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Add Network and Service Objects.
   For more information, see Add a Network Object and Add a Service Object.
2. (Optional) Add Network Object Groups and Service Object Groups.
   For more information, see Add a Network Object Group and Add a Service Object Group.
3. Add internet or private access rules in the Access policy where you select the Network and Service Objects and Groups.
   - For more information, see Access Rules: Selecting Network and Service Objects.
   - For more information, see Add an Internet Access Rule.
   - For more information, see Add a Private Access Rule.
4. From end-user devices on certain networks, make requests to another network or service defined by the Network or Service resources.
5. Review the traffic in the Activity Search report and verify that Secure Access received the traffic from the source and allowed or blocked the traffic on the destinations defined in the access rules.
   For more information, see Activity Search Report.

Access Rules with Network and Service Objects

Describes Access Rules with Network and Service Objects in Cisco Secure Access. Cisco Secure Access supports adding Network and Service Objects on the internet and private access rules in the Access policy.

Cisco Secure Access supports adding Network and Service Objects on the internet and private access rules in the Access policy. For more information, see Add an Internet Access Rule and Add a Private Access Rule.

This guide describes the best practices to use when selecting Network and Service Objects and Groups on access rules.

About Network or Service Objects in Access Rules

Once you add the Network Objects and Groups and Service Objects and Groups in Secure Access, you can select the objects and groups on the access rules in the Access policy.

Supported Source Components in Access Rules	Supported Destination Components in Access Rules
Network Objects and Network Object Groups	Network Objects and Network Object Groups Service Objects and Service Object Groups

Internet or Private Access Rules

- For the sources in an access rule, Secure Access combines all selected sources together with the OR operator when enforcing the rule.
- For the destinations in an access rule, Secure Access combines all selected destinations together with the OR operator when enforcing the rule.
  - (Optional) For the destinations in an access rule, Secure Access can combine the selected Network Objects with the Service Objects into a single destination using the logical AND operator.
- Service Objects and Groups are available only on destination components in access rules.

Using Network Objects for Sources in Access Rules

You can select Network Objects for sources on the internet and private access rules in the Access policy. Sources are the **From** side of the access rule in the Access policy.

- You can select at most 10 Network Objects for a source or destination in an internet or private access rule.
- You can select at most 10 Network Object Groups for a source or destination in an internet or private access rule where each group has no more 50000 objects in the group.
- Sources that have Network Objects with an fully-qualified domain name (FQDN) are ignored and Network Groups that include Network Objects with an FQDN are also ignored. If access rules have other sources selected besides the Network Objects with an FQDN, Secure Access enforces the rule for those sources.

  Secure Access displays a warning message that the access rule will ignore the Network Object or Group with an FQDN.

Using Network and Service Objects for Destinations in Access Rules

You can select Network and Service Objects for destinations on the internet and private access rules in the Access policy. Destinations are the **To** side of the access rule on the Access policy.

- You can select at most 10 Network Objects and 10 Service Objects for a destination in an internet or private access rule.
- You can select at most 10 Network Groups and 10 Service Groups for a destination in an internet or private access rule where each group has no more 50000 objects in the group.
- A VPN profile that includes the configuration of a VPN split tunnel supports Network Objects only.

- To select Network Objects and Service Objects in a rule, the rule must have either the `allow` or `block` action.
- You can use logical AND to combine Network Objects and Groups and Service Objects and Groups for destinations on both internet and private access rules in the Access policy.

Combine Destinations with Boolean Logic

Describes Combine Destinations with Boolean Logic in Cisco Secure Access. The Cisco Secure Access policy is the collection of an organization's internet and private access rules.

The Cisco Secure Access policy is the collection of an organization's internet and private access rules. On each rule in the Access policy, you can select sources and destinations. When you select Network and Service Objects and Groups for destinations in an access rule, Secure Access provides the option to combine the destinations with the logical **AND** operator.

How Destinations are Combined on Access Rules

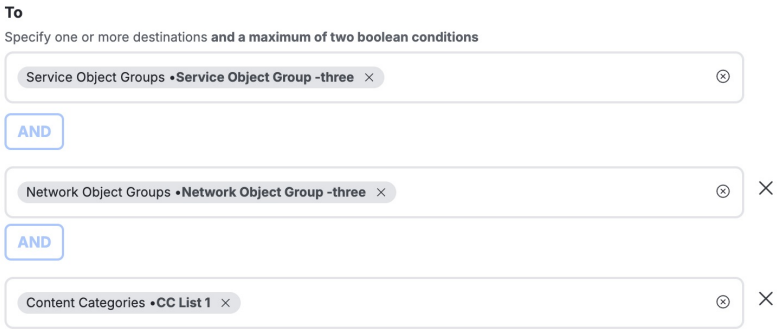
- Generally, Secure Access supports the use of the logical **OR** operator to combine the selected destination components together on both the source and destinations sides of the internet or private access rule. All types of destinations, and all destinations within a type, are combined together using the boolean **OR** operator. Traffic to each destination that you specify in a rule matches the rule.
- The logical **AND** capability supports Network Objects, Service Objects, Application Protocols, Internet Applications, and Content Categories. This enhancement allows for granular and flexible policy definitions by enabling combinations such as Destination Lists **AND** Content Category + Application pairs.

> **Note**
>
> Destination lists do not support Network Objects.

Logical AND Operator with Network and Service Objects

If you enable the **AND** option for the destinations in the access rule, then depending on the destination components that you selected, Secure Access combines the destinations together using certain logical operators.

Additionally, you can create logical **AND** combinations with additional destination components including Application Protocols, Internet Applications and Content Categories.



Supported Combinations of Destinations with Logical AND/OR Operators

In order to trigger **AND** you can choose any of the supported boolean items. Secure Access supports specific combinations of Network and Service Objects with the logical **AND** operator for destinations on access rules.

AND logic is order-independent (operands may appear in any sequence). Up to three conjuncts per destination condition.

You can also include combinations with Application Protocols, Internet Applications, and Content Categories as follows:

Table 14: Supported OR Combinations

	Application List	Application Category	Application	Category	Category List	Destination List	Network Object	Service Object	Network Object Group	Service Object Group
Application List	N/A	N/A	N/A	N/A	N/A	OR	N/A	N/A	N/A	N/A
Application Category	N/A	N/A	OR	N/A	N/A	OR	N/A	N/A	N/A	N/A
Application	N/A	OR	N/A	N/A	N/A	OR	N/A	N/A	N/A	N/A
Category	N/A	N/A	N/A	N/A	N/A	OR	N/A	N/A	N/A	N/A
Category List	N/A	N/A	N/A	N/A	N/A	OR	N/A	N/A	N/A	N/A
Destination List	OR	OR	OR	OR	OR	N/A	OR	OR	OR	OR
Network Object	N/A	N/A	N/A	N/A	N/A	OR	N/A	OR	OR	OR
Service Object	N/A	N/A	N/A	N/A	N/A	OR	OR	N/A	OR	OR
Network Object Group	N/A	N/A	N/A	N/A	N/A	OR	OR	OR	N/A	OR
Service Object Group	N/A	N/A	N/A	N/A	N/A	OR	OR	OR	OR	N/A

A check (✓) marks an explicitly supported 2-way or 3-way **AND** combination. The order is not significant.

Table 15: Supported AND Combinations

	Internet Application	Application Protocol	Content Category	Destination List	Network Object/Group	Service Object/Group
Internet Application	N/A	N/A	N/A	✓	✓	✓
Application Protocol	N/A	N/A	✓	✓	✓	✓
Content Category	✓	✓	N/A	N/A	✓	✓
Destination List	✓	✓	N/A	N/A	N/A	✓
Network Object/Group	✓	✓	✓	N/A	N/A	✓
Service Object/Group	✓	✓	✓	✓	✓	N/A

Manage Network Objects and Groups

Describes Manage Network Objects and Groups in Cisco Secure Access. In Cisco Secure Access, you can add a reusable Network Object and configure the resource with a single IPv4 address, CIDR block (IPv4 or IPv6 addresses), range of IPv4 addresses, wildcard mask, or fully-qualified domain name (FQDN).

In Cisco Secure Access, you can add a reusable Network Object and configure the resource with a single IPv4 address, CIDR block (IPv4 or IPv6 addresses), range of IPv4 addresses, wildcard mask, or fully-qualified domain name (FQDN).

A Network Object Group is a collection of Network Objects and other Network Object Groups.

Get Started with Network Objects

Describes Get Started with Network Objects in Cisco Secure Access and outlines About Network Objects, Guidelines: Add Network Objects in Secure Access, and Add a Network Object. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To get started, add Network Objects in Secure Access. After you add a Network Object, you can view, edit, duplicate, or delete the resource.

You can select the Network Objects as source or destination components on internet and private access rules in the Access policy. For more information, see Components for Internet Access Rules and Components for Private Access Rules.

About Network Objects

- A Network Object is defined by the type of the network resource and domain name or IP address information. A Network Object is either a **FQDN**, **Host**, **Range**, or **Network**.
  - **FQDN**–A fully-qualified domain name, for example: **cisco.com**.
  - **Host**–An IPv4 address, for example: **10.10.10.10**.
  - **Range**–A range of IPv4 addresses, for example: **192.168.0.0 - 192.168.0.10**.
  - **Network**–An IPv4 or IPv6 CIDR block or wildcard mask.
    - **IPv4 CIDR block**–IPv4 addresses, for example: **192.168.1.0/24**.
    - **Wildcard mask**–An IPv4 address with a wildcard mask, for example: **192.168.10.0/0.0.0.255**.
    - **IPv6 address**–An IPv6 address, for example: **fd00:b0fc:8844:3345:186a:6fd7:bab:5f72/24**.
- A Network Object must have a unique name for all Network Objects in the organization.

Guidelines: Add Network Objects in Secure Access

- A Network Object is defined by the type of the network resource and domain name or IP address information.
- Review the recommendations for adding Network and Service Objects in your organization. For more information see General Limits for Objects on page 521.
- A Network Object must have a name that is unique for all Network Objects in the organization.

Add a Network Object

- For more information, see Add a Network Object.

Import a CSV File with Network Objects

- For more information, see Import CSV File of Network Objects.

Manage a Network Object

For more information see

- Edit a Network Object
- Duplicate a Network Object
- Delete a Network Object

View Network Objects and Groups

- For more information, see View Network Objects and Groups.

Add a Network Object

Provides instructions for completing the Add a Network Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Cisco Secure Access, a Network Object represents a network resource—a single IPv4 address, IPv4 or IPv6 CIDR block, range of IPv4 addresses, wildcard mask, or fully-qualified domain name (FQDN).

You can add a Network Object individually in Secure Access or import comma-separated values (CSV) files of network objects. For information about importing network objects in Secure Access, see Import CSV File of Network Objects.

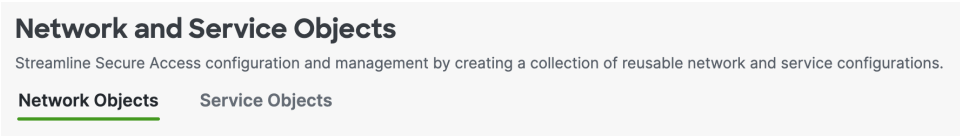
You can include Network Objects in Network Object Groups. For information about Network Object Groups, see Add a Network Object Group.

Before you begin

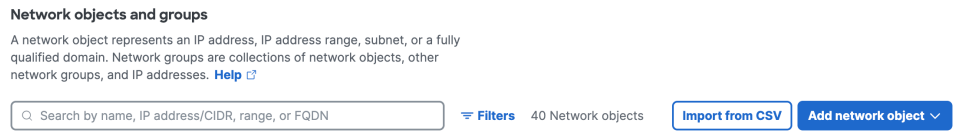
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups** , and then click **Add network object**.

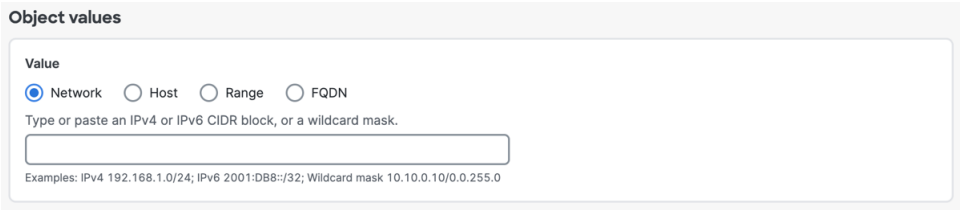


3. On **Add Network Object**, navigate to **General**.



   a) For **Name**, enter a unique name for the Network Object. Secure Access supports a sequence of 1–255 alphanumeric, space, hyphen, and underscore characters.
   b) (Optional) For **Description**, enter text that describes the Network Object.

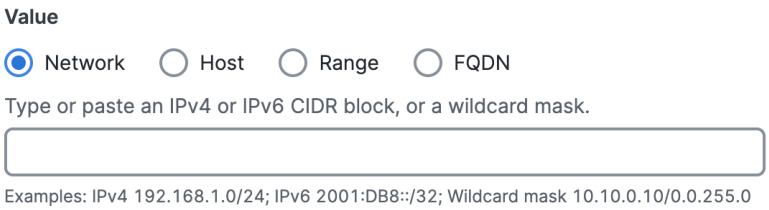
4. Navigate to **Object values**.



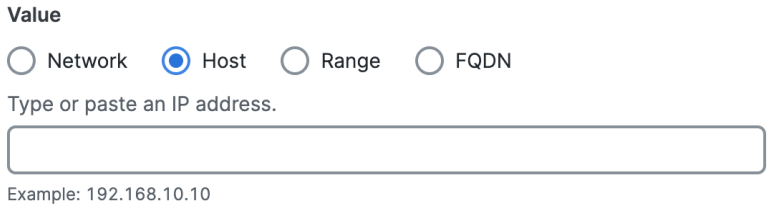
5. For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

   You must choose the type of the Network Object and enter the IP address information.

   a) Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.

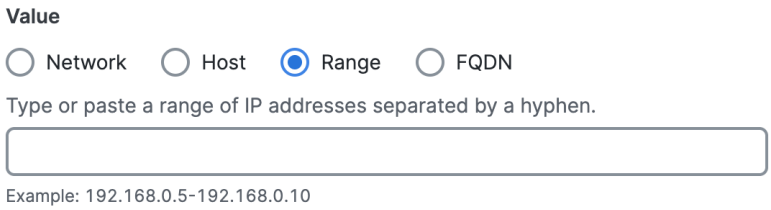
   

   b) Click **Host**, and then enter an IPv4 address.

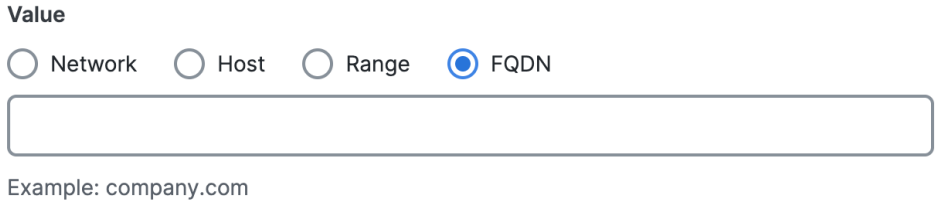
   

   c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (**-**).

   For example: **192.168.0.0-192.168.0.10**.

   d) Click **FQDN**, and then enter a fully-qualified domain name (FQDN).

6. Click **Add Network Object**.

About Importing a CSV File of Network Objects

Describes About Importing a CSV File of Network Objects in Cisco Secure Access. You can import comma-separated values (CSV) files that contain the information required to add Network Objects in Cisco Secure Access.

You can import comma-separated values (CSV) files that contain the information required to add Network Objects in Cisco Secure Access. A Network Object represents a single IPv4 address, IPv4 or IPv6 CIDR block, range of IPv4 addresses, wildcard mask, or fully-qualified domain name (FQDN). For information about adding a single Network Object in Secure Access, see Add a Network Object.

When you upload the Network Objects in a CSV file, Secure Access first validates the required attributes for adding each network resource. If the file contains errors, Secure Access displays the errors and provides suggestions for correcting the errors. If the CSV file is valid, Secure Access adds all of the Network Objects.

During the import of the Network Objects, you can choose to add a Network Object Group and include all of the Network Objects in the group. For information about Network Object Groups, see Add a Network Object Group.

After you add the Network Objects in Secure Access, these resource are available for you to select in the Network Object Groups and on the internet and private access rules in the Access policy. For information about reusable source and destination components, see Components for Internet Access Rules and Components for Private Access Rules.

Guidelines: Import Network Objects in Secure Access

- Secure Access provides a template that you can download and use to create a CSV file with Network Objects. For more information see Download the CSV File Template.
- Review the recommendations for adding or importing Network and Service Objects in your organization. For more information, see General Limits for Network and Service Objects.
- Secure Access adds all valid network objects in a CSV file or none if the data for the network objects is invalid.
- Secure Access does not add duplicate network objects—network objects that have the same name and are already found in the organization.
- A Network Object is defined by the type of the network resource and fully-qualified domain name (FQDN) or IP address information.

Upload CSV File with Network Objects

Provides instructions for completing the Upload CSV File with Network Objects workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

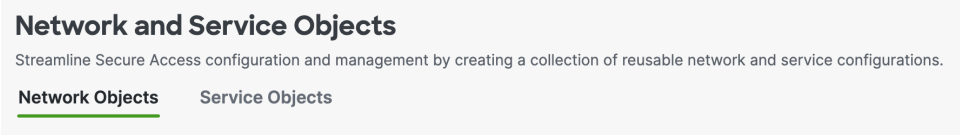
Upload a CSV file with Network Objects to Secure Access.

Before you begin

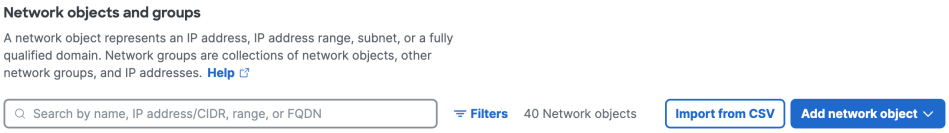
- Full Admin user role. For more information, see Manage Accounts.

Procedure

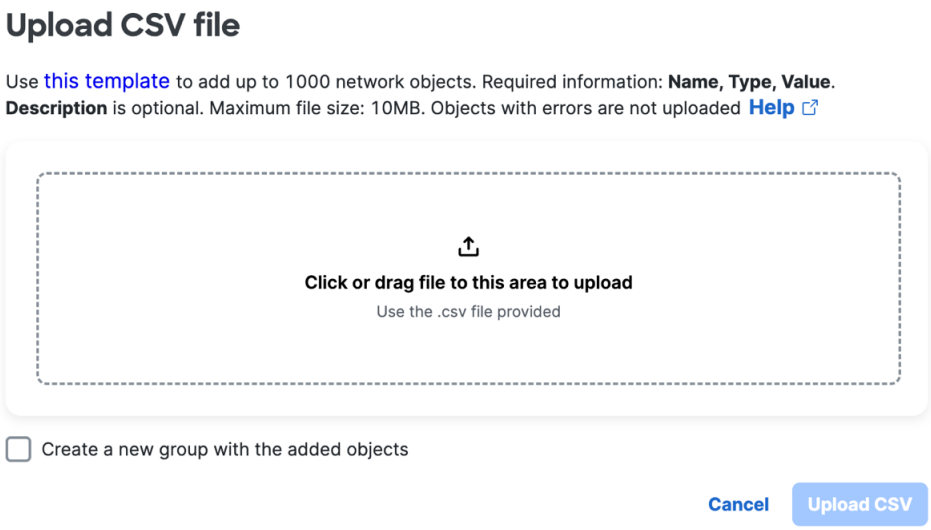
1. Navigate to **Resources > Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups** , and then click **Import from CSV**.



3. For **Upload CSV file**, click or drag a CSV file with the network objects to the area in Secure Access.
   a) Download the CSV file template. Click on **this template** to download a CSV file that you can use to upload the network objects.



4. Check **Create a new group with the added objects** to include the network objects from the CSV file to a network object group.
   a) For **Name**, enter a unique name for the Network Object Group that will be added in Secure Access.
   b) (Optional) For **Description**, enter a description for the Network Object Group.



5. Click **Upload CSV** to validate and upload the CSV file with the network objects.

   Secure Access checks if the CSV file is valid.

   - If the CSV file is valid, Secure Access adds all of the network objects.
   - If the CSV file is invalid, Secure Access provides information about the invalid fields. You can correct the invalid fields and upload the network objects again.

   a) Click **Upload** to validate the CSV file again and upload the network objects.

Examples of Valid CSV Files

Describes Examples of Valid CSV Files in Cisco Secure Access and outlines CSV File with Network Object of FQDN Type, CSV File with Network Object of Host Type, and CSV File with Network Object of Network Type. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

CSV File with Network Object of FQDN Type

```
name,description,type,value
name110,about the test network object 7,fqdn,cisco.com
```

CSV File with Network Object of Host Type

```
name,description,type,value
name111,description1,host,77.160.180.229
```

CSV File with Network Object of Network Type

```
name,description,type,value
name122,description122,network,192.68.1.0/24
```

CSV File with Network Object of Range Type

```
name,description,type,value
name123,,range,10.10.0.0-10.10.2.0
```

Edit a Network Object

Provides instructions for completing the Edit a Network Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit the properties of a Network Object in Secure Access.

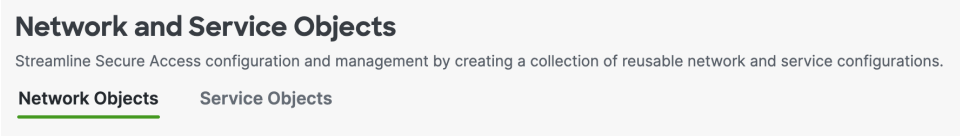
> **Note**
>
> If an VPN profile references a Network Object, you cannot edit the Network Object.

Before you begin

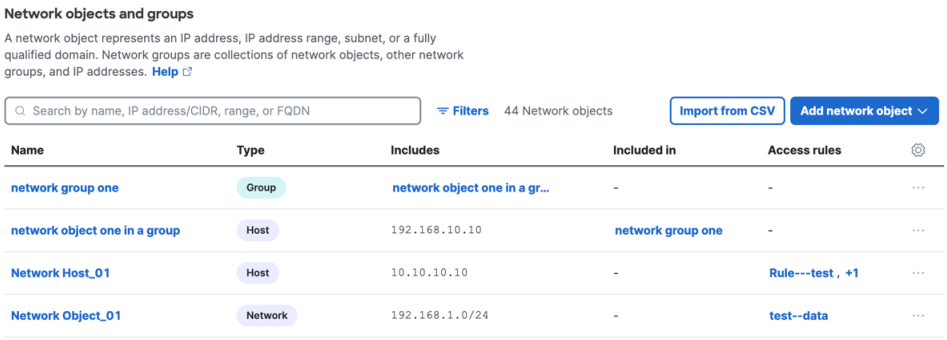
- Full Admin user role. For more information, see Manage Accounts.

Procedure

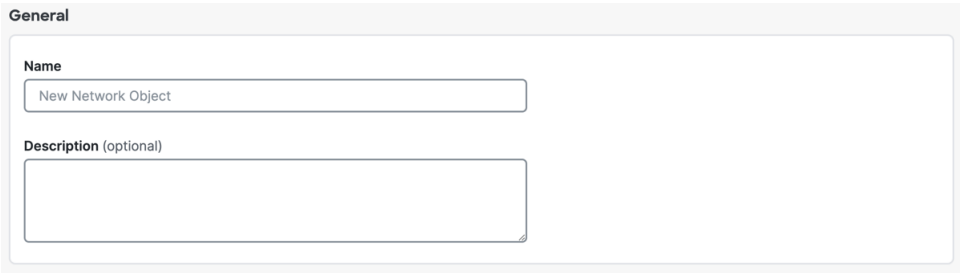
1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**.
3. Navigate to the Network Objects and Groups table.
   a) Navigate to a Network Object in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Name** column, click on the name of a Network Object, and then click **Edit**.

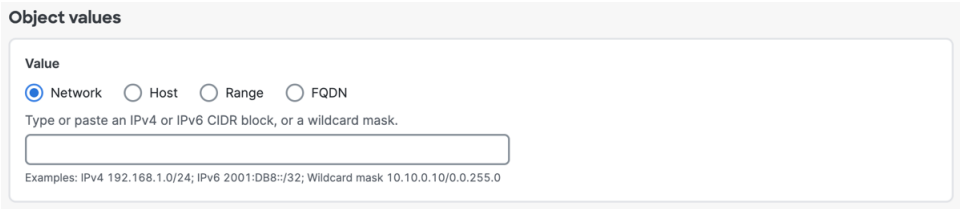


4. Navigate to **General**.



   a) For **Name**, enter a unique name for the Network Object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) (Optional) For **Description**, enter text that describes the Network Object.

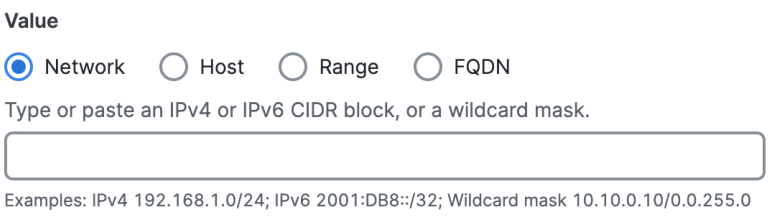
5. Navigate to **Object values**.



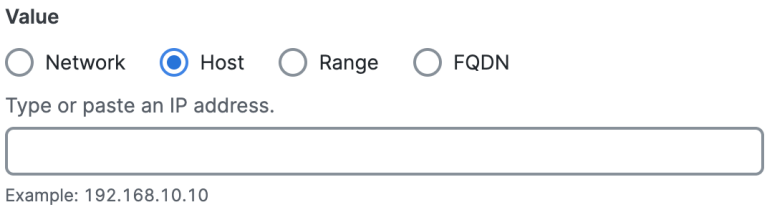
6. For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

> **Note**
>
> You must choose the type of the Network Object and enter the IP address information.

   a) Click **Network**, and then enter an IPv4 CIDR block, IPv6 address, or Wildcard mask.

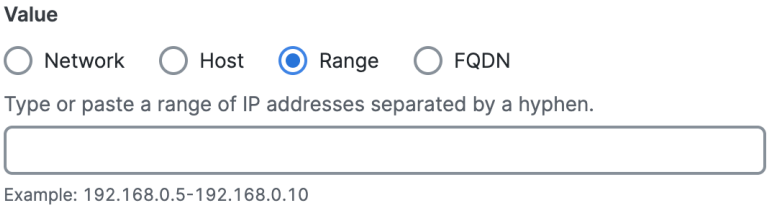


   b) Click **Host**, and then enter an IPv4 address.

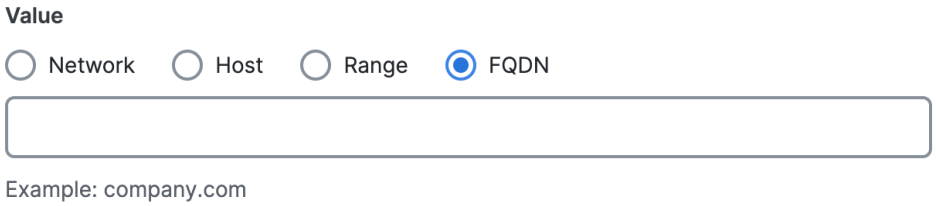


c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (-).

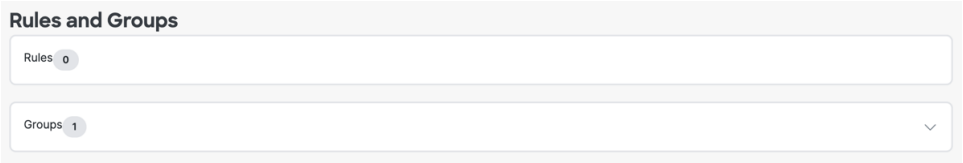
For example: **192.168.0.0-192.168.0.10**.



d) Click **FQDN**, and then enter a fully-qualified domain name (FQDN).



7. Navigate to **Rules and Groups**.



a) For **Rules**, expand a rule, and then click on the name of a rule to edit the rule in the Access policy.

For more information about the Access policy, see Manage the Access Policy.



b) For **Groups**, expand a Network Object Group, and then click on the name of group to edit the group.

For more information about Network Object Groups, see Get Started with Network Object Groups.

8. Click **Save changes**.

Duplicate a Network Object

Provides instructions for completing the Duplicate a Network Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Create a new Network Object in Secure Access from an existing Network Object.

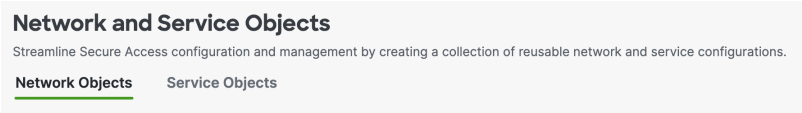
You must provide a unique name for the new Network Object.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**.
3. In the table, navigate to the **Name** column, click on the name of a Network Object, and then click **Duplicate**.
4. For **Name**, enter a unique name for the Network Object.
5. Click **Duplicate** to confirm the addition of the Network Object.



Delete a Network Object

Provides instructions for completing the Delete a Network Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Remove the Network Object in Secure Access.

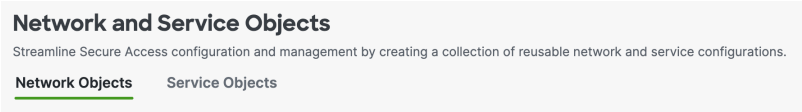
> **Note**
>
> If an VPN profile references a Network Object, you cannot delete the Network Object.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

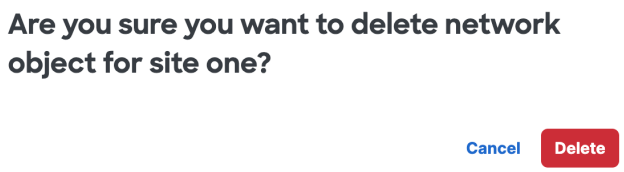
Procedure

1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**.
3. Remove a Network Object.
   a) In the table, navigate to an item in the table, click on the ellipsis (**...**), and then choose **Delete**.
   b) In the table, navigate to the **Name** column, click on the name of a Network Object, and then click **Delete**.

4. Click **Delete** to confirm the removal of the Network Object.



Get Started with Network Object Groups

Describes Get Started with Network Object Groups in Cisco Secure Access. To get started, add Network Object Groups in Secure Access.

To get started, add Network Object Groups in Secure Access. After you add a Network Object Group, you can view, edit, duplicate, or delete the group in Secure Access.

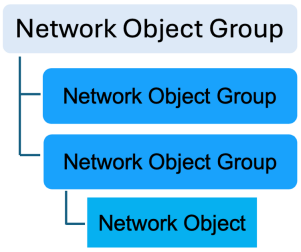
You can select the Network Object Groups and Network Objects in the groups as destination components on the internet and private access rules in the Access policy.

You can also select the Network Object Groups and Network Objects in the groups as source components on private access rules in the Access policy.

For more information, see Components for Internet Access Rules and Components for Private Access Rules.

Guidelines: Add Network Object Groups in Secure Access

- Review the recommendations for adding Network and Service Objects in your organization. For more information, see General Limits for Groups.
- A Network Object Group must have a unique name for all Network Object Groups in the organization.
- A Network Object Group can include Network Objects and other Network Object Groups. Secure Access supports three levels of nested groups.



- Secure Access does not support circular dependencies of groups in Network Object Groups.

Add a Network Object Group

- For more information, see Add a Network Object Group.

Manage a Network Object Group

- View Objects, Groups and Values in a Network Object Group
- Edit a Network Object Group
- Duplicate a Network Object Group

- Delete a Network Object Group

View Network Objects and Groups

- For more information, see View Network Objects and Groups.

Add a Network Object Group

Provides instructions for completing the Add a Network Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Cisco Secure Access, a Network Object Group is a collection of Network Objects and other Network Object Groups.

When you add a Network Object Group, select Network Objects to add to the group, add a non-reusable network value, or create new Network Objects.

You can also create new Network Objects and add these resources to the group and add composite network information in the Network Object Group. Composite network information is not reusable in the organization.

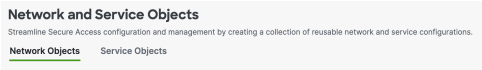
After you add a Network Object Group in Secure Access, you can view the details for the resource. For more information, see View Network Objects and Groups.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

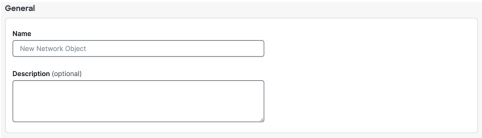
1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**, and then click **Add network object group**.

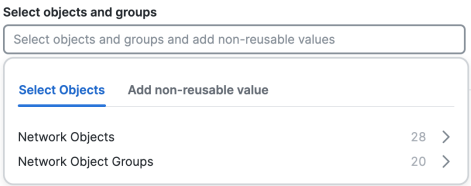


3. On **Add New Network Object Group**, navigate to **General**.

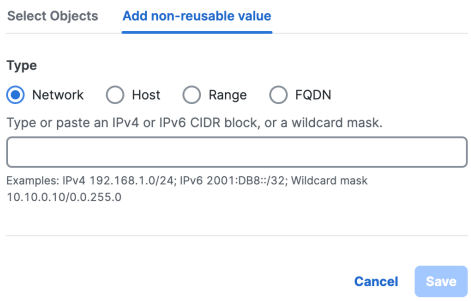


   a) For **Name**, enter a unique name for the Network Object Group. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) For **Description**, enter text that describes the Network Object Group.

4. Navigate to **Group values**, and then add values to the Network Object Group.
5. Click on **Select objects and groups and add non-reusable values**.
6. Click **Select objects**, and then choose the Network Objects and Network Object Groups.

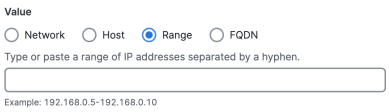


7. Click **Add non-reusable value**, choose the type of the network resource, enter the information for the non-reusable network resource, and then click **Save**.



a) Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.
b) Click **Host**, and then enter an IPv4 address.
c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (-).

For example: **192.168.0.0-192.168.0.10**



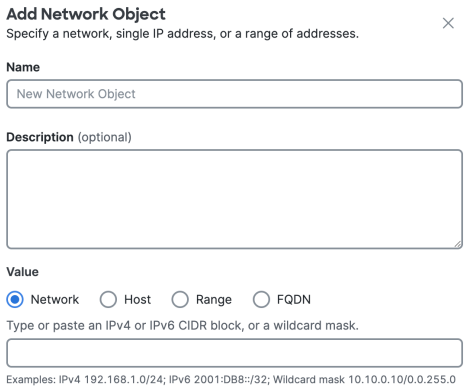
d) Click **FQDN**, and then enter a domain name.

8. Click **+ Create Object**, enter the information for the new network resource, and then click **Add**.



a) For **Name**, enter a unique name for the Network Object.

Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.



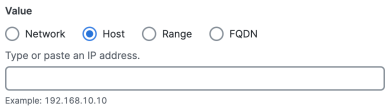
b) (Optional) For **Description**, enter text that describes the Network Object.
c) For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

You must choose the type of the Network Object and enter the IP address information or fully-qualified domain name (FQDN).

d) Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.

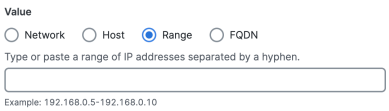


e) Click **Host**, and then enter an IPv4 address.



f) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (**-**).

For example: **192.168.0.0-192.168.0.10**.



g) Click **FQDN**, and then enter a domain name.



View Objects, Groups and Values in a Network Object Group

Provides instructions for completing the View Objects, Groups and Values in a Network Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View the objects, groups and values that are included in the Network Object Group.

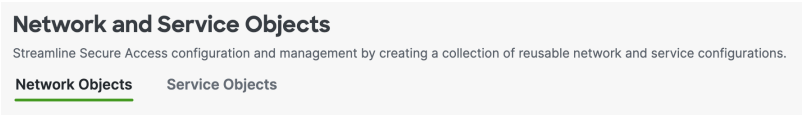
Before you begin

- A minimum user role of Read Only. For more information, see Manage Accounts.

Procedure

---

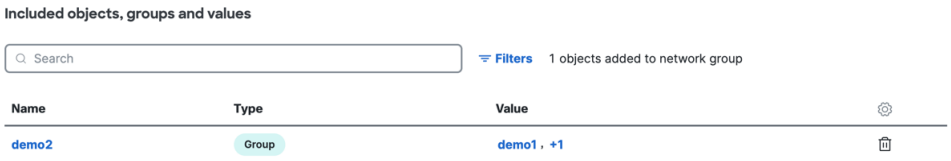
1. Navigate to **Resources** > **Network and Service Objects**.



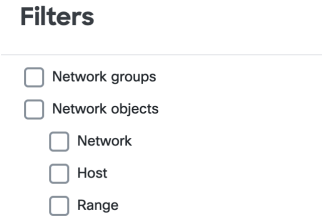
2. On **Network Objects**, navigate to **Network objects and groups**.
3. Navigate to the Network Objects and Groups table.
   a) Navigate to a group in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Name** column, click on the name of a Network Object Group, and then click **Edit**.
4. Navigate to **Group Values**, and then navigate to **Included objects, groups and values**.

   Secure Access displays the properties for the objects in the Network Object Group.

   - **Name**–The name of the object or group.
   - **Type**–The type of the Network Object or **Group**.
   - **Value**–The value of the object, for example the network addresses or the groups that are included in the Service Object Group.



5. (Optional) In the search bar, enter a sequence of characters to query for the name of the included objects, groups and values.
6. (Optional) Click **Filters**, choose the Network Objects, Network Object Groups, and types of the Network Objects.



Edit a Network Object Group

Provides instructions for completing the Edit a Network Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit the properties of a Network Object Group in Secure Access.

> **Note**
>
> If an VPN profile references a Network Object Group, you cannot edit the Network Object Group.

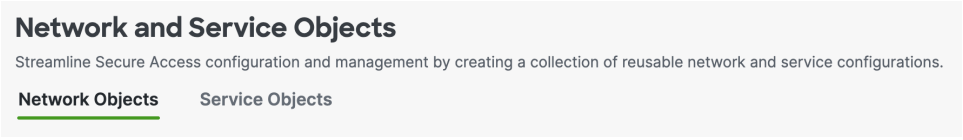
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

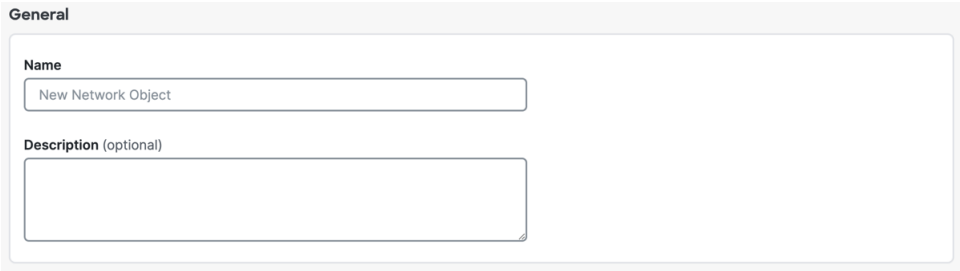
Procedure

---

1. Navigate to **Resources** > **Network and Service Objects**.

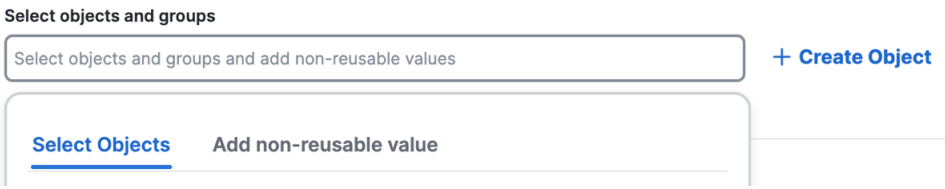


2. On **Network Objects**, navigate to **Network objects and groups**.
3. Edit a Network Object Group.
   a) In the table, navigate to a Network Object Group in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) In the table, navigate to the **Name** column, click on the name of a Network Object Group, and then click **Edit**.
4. For the Network Object Group, navigate to **General**.

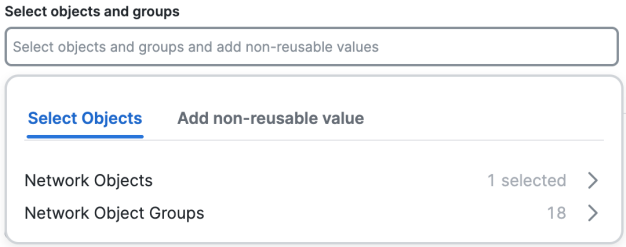


a) For **Name**, enter a unique name for the Network Object Group. Secure Access supports a sequence of 1–255 alphanumeric, space, hyphen, and underscore characters.
b) For **Description**, enter text that describes the Network Object Group.

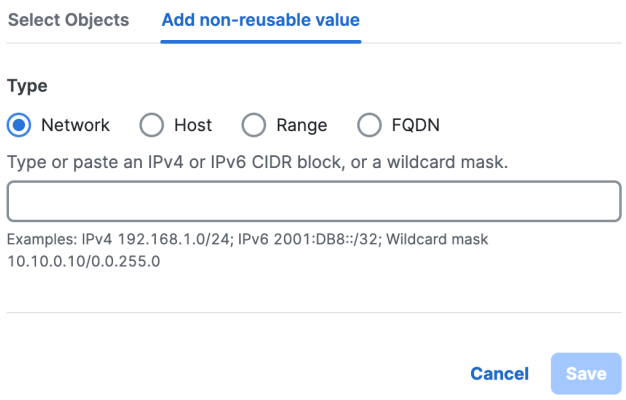
5. Navigate to **Group Values**, navigate to **Select objects and groups**, and then click on **Select object or groups and add non-reusable values**.



6. Click **Select objects**, choose the objects and groups from the lists of the configured Network Objects and Network Object Groups.

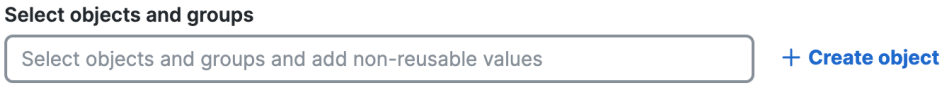


7. Click **Add non-reusable value**, choose the type of the network resource, enter the information for the non-reusable network resource, and then click **Save**.

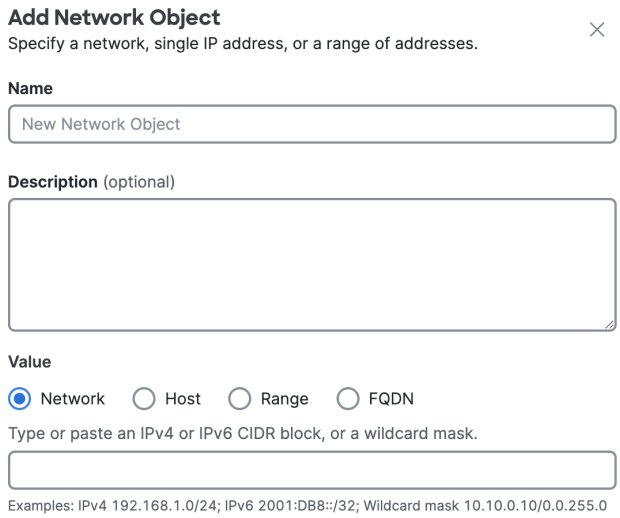


a) Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.
b) Click **Host**, and then enter an IPv4 address.
c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (**-**). For example: **192.168.0.0-192.168.0.10**.
d) Click **FQDN**, and then enter a domain name.

8. Click **+ Create Object**, enter the information for the new network resource, and then click **Add**.



a) For **Name**, enter a unique name for the Network Object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.

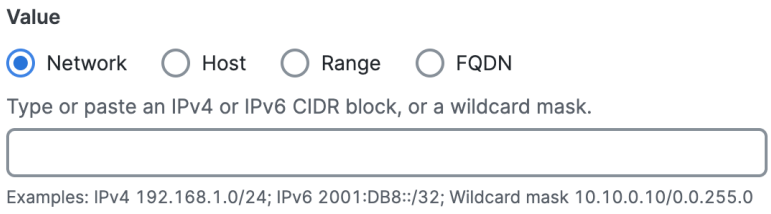


b) (Optional) For **Description**, enter text that describes the Network Object.

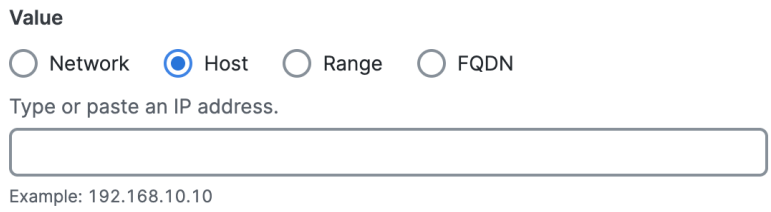
c) For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

> **Note**
>
> You must choose the type of the Network Object and enter the IP address information.

- Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.

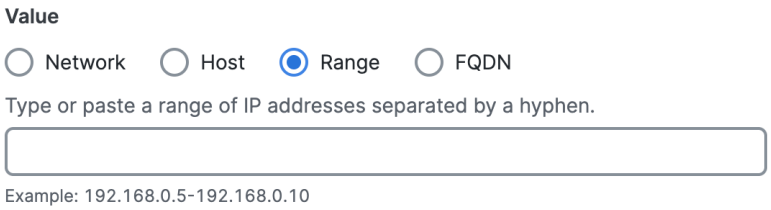


- Click **Host**, and then enter an IPv4 address.

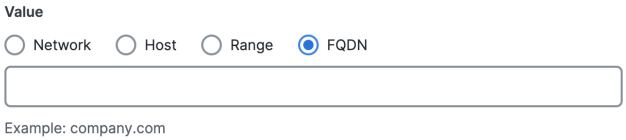


- Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (**-**).

  For example: **192.168.0.0-192.168.0.10**.



- Click **FQDN**, and then enter a domain name.



9. Delete an included object, group and values.
   a) Navigate to **Group values**, and then navigate to **Included objects, groups and values**.



   b) Navigate to an object in the table, click on the trash can icon to remove the object.
10. Click **Save changes**.

Duplicate a Network Object Group

Provides instructions for completing the Duplicate a Network Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Create a new Network Object Group in Secure Access from an existing Network Object Group.

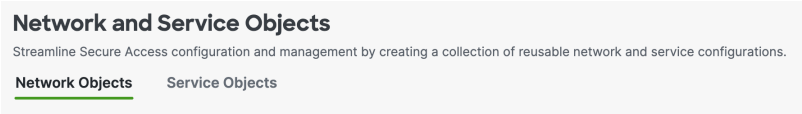
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**.
3. Duplicate a Network Object Group. In the table, navigate to the **Name** column, click on the name of a Network Object Group, and then click **Duplicate**.
4. For **Name**, enter a unique name for the new Network Object Group.
5. Click **Duplicate** to confirm the addition of the Network Object Group.



Delete a Network Object Group

Provides instructions for completing the Delete a Network Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Remove the Network Object Group in Secure Access.

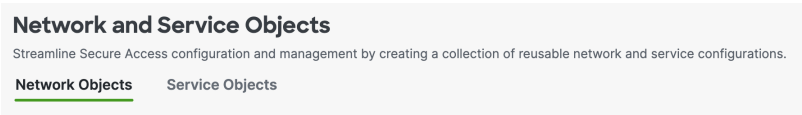
> **Note**
>
> If an VPN profile references a Network Object Group, you cannot delete the Network Object Group.

Before you begin

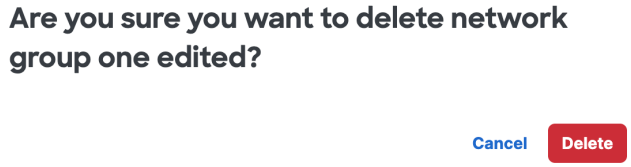
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Network Objects**, navigate to **Network objects and groups**.
3. Edit a Network Object Group.
   a) In the table, navigate to a Network Object Group in the table, click on the ellipsis (**...**), and then choose **Delete**.
   b) In the table, navigate to the **Name** column, click on the name of a Network Object Group, and then click **Delete**.
4. Click **Delete** to confirm the removal of the Network Object Group.



View Network Objects and Groups

Provides instructions for completing the View Network Objects and Groups workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

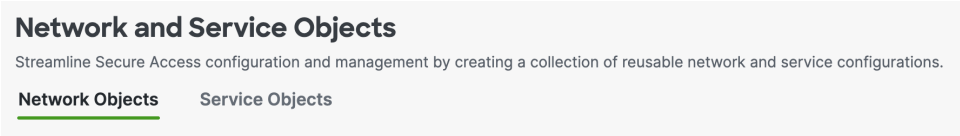
After you add Network Objects and Groups in Cisco Secure Access, you can view the details about the resources.

Before you begin

- A minimum user role of Read Only. For more information, see Manage Accounts.

Procedure

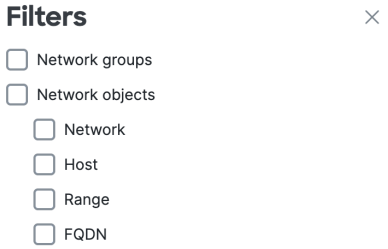
1. Navigate to **Resources** > **Network and Service Objects**.



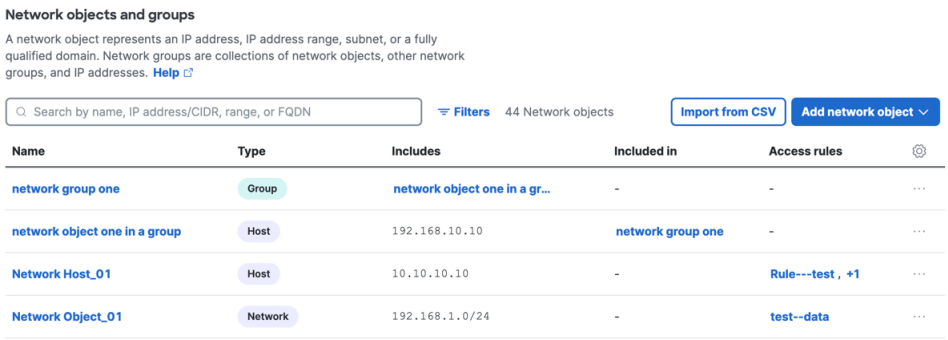
2. On **Network Objects**, navigate to **Network objects and groups**.
3. (Optional) Search for the Network Objects in the organization. In the search bar, enter a sequence of characters to query for the name of the Network Objects.



4. (Optional) Filter for the Network Objects in the organization. Click **Filters**, choose the Network Objects, Network Object Groups, and types of the Network Objects.



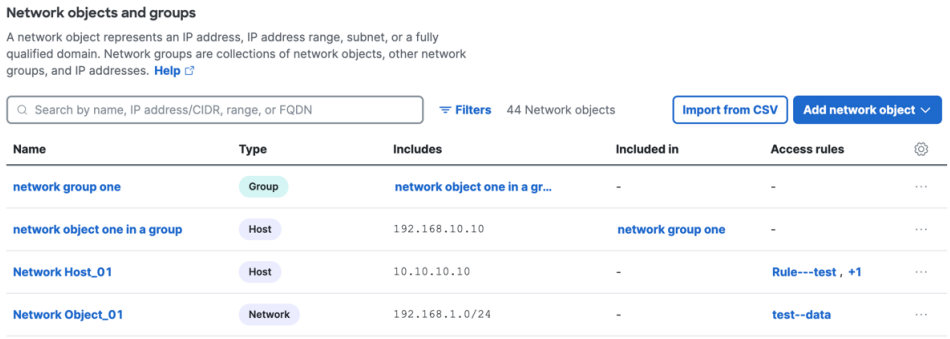
5. In the table, Secure Access displays the properties for the Network Objects and Groups in the organization.



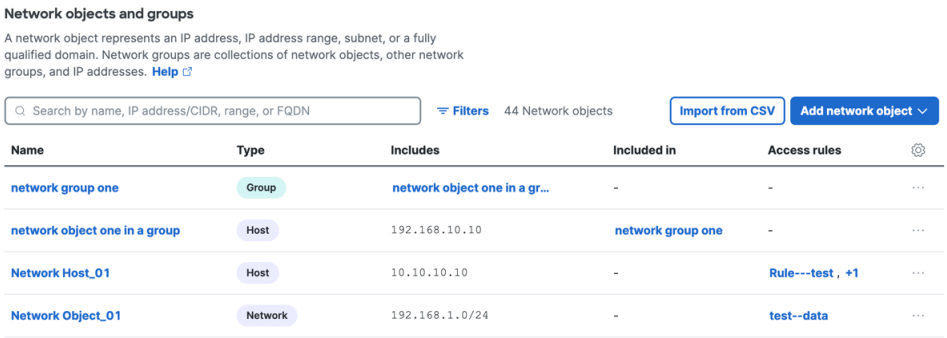
- **Name**–The name of the Network Object or Network Object Group.
- **Type**–The type of the Network Object or Network Object Group.
  - For a Network Object, the type is: **FQDN**, **Host**, **Network**, or **Range**.
  - For a Network Object Group, the type is **Group**.
- **Includes**–The values of the Network Object or references to the objects that are included in the Network Object Group.

- For a Network Object, the value is: the fully-qualified domain name (FQDN), IP addresses or wildcard mask for the Network Object.
- For a Network Object Group, the value is the list of Network Objects or Network Object Groups, which the group includes.

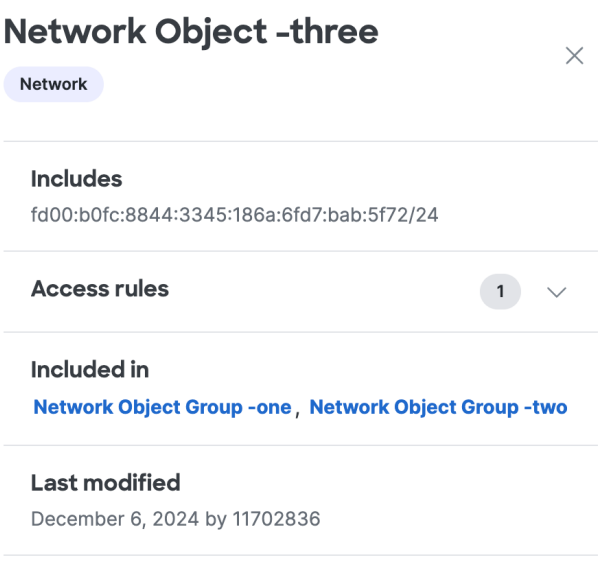
- **Included in**–The list of Network Object Groups that include the Network Object or Network Object Group.
  - For a Network Object, the value is the list of Network Object Groups that include the resource.
  - For a Network Object Group, the value is the list of Network Objects or Network Object Groups, which are included in the group.
- **Access rules**–The list of rules that have the Network Object or Network Object Group selected on the rules.



6. (Optional) In the table, navigate to the **Name** column.
   a) Click on the name of a Network Object or Network Object Group in the table to view the details about the resource.



   b) View the details about the resource.



Manage Service Objects and Groups

Describes Manage Service Objects and Groups in Cisco Secure Access. In Cisco Secure Access, you can add a reusable Service Object and configure the resource with the ports and protocols of a service.

In Cisco Secure Access, you can add a reusable Service Object and configure the resource with the ports and protocols of a service.

A Service Object Group is a collection of Service Objects and other Service Object Groups.

Get Started with Service Objects

Describes Get Started with Service Objects in Cisco Secure Access and outlines About Service Objects, Guidelines: Add Service Objects in Secure Access, and Add a Service Object. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To get started, add Service Objects in Secure Access. After you add a Service Object, you can view, edit, duplicate, or delete the resource.

You can select the Service Objects as destination components on the internet and private access rules in the Access policy. For more information, see Components for Internet Access Rules and Components for Private Access Rules.

About Service Objects

- A Service Object is defined by the protocols and ports of a service (internet or private destination).
- A Service Object supports the TCP, UDP, or ICMP protocol. You can also select **Any** to indicate that the Service Object defines the traffic on any protocol.
- A Service Object must have a name that is unique for all Service Objects in the organization.

Guidelines: Add Service Objects in Secure Access

- A Service Object is defined by the ports and protocol information for the service. For more information, see About Service Objects.

- Review the recommendations for adding Network and Service Objects in your organization. For more information, see General Limits for Objects.
- A Service Object must have a name that is unique for all Service Objects in the organization.

> **Note**
>
> At this time, if you create a service object configured with an internet destination that is a non-standard web port, the HTTP and HTTPS requests from the web or from the SWG are automatically standardized as if they are requests from ports 80 and 443 respectively. Because the requests are normalized, the service object does **not** match against the traffic if you visit a website with a non-standard destination.

Add a Service Object

- For more information, see Add a Service Object.

Import CSV File with Service Objects

- For more information, see Import CSV File of Service Objects.

Manage a Service Object

After you add a Service Object in Cisco Secure Access, you can edit, duplicate, or remove the resource.

- Edit a Service Object
- Duplicate a Service Object
- Delete a Service Object

View Service Objects and Groups

- For more information, see View Service Objects and Groups.

Add a Service Object

Provides instructions for completing the Add a Service Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Cisco Secure Access, a Service Object represents a port, range of ports, specific protocols, or any protocols of a service.

You can add a Service Object individually in Secure Access or import comma-separated values (CSV) files of service objects. For information about importing network objects in Secure Access, see Import CSV File of Service Objects.

You can include Service Objects in Service Object Groups. For information about Service Object Groups, see Add a Service Object Group.

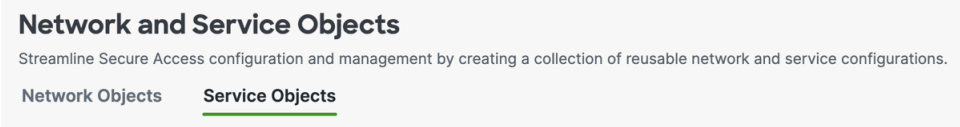
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

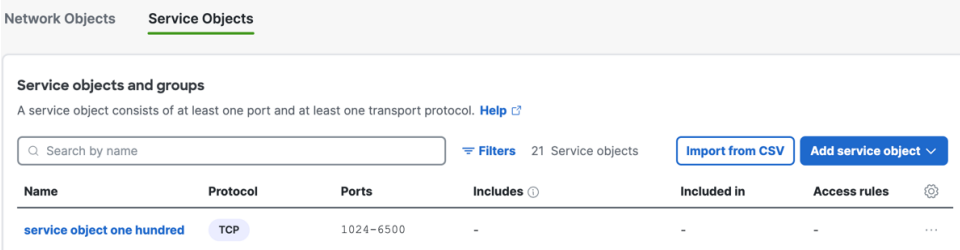
> **Note**
>
> At this time, if you create a service object configured with an internet destination that is a non-standard web port, the HTTP and HTTPS requests from the web or from the SWG are automatically standarized as if they are requests from ports 80 and 443 respectively. Because the requests are normalized, the service object does **not** match against the traffic if you visit a website with a non-standard destination.

Procedure

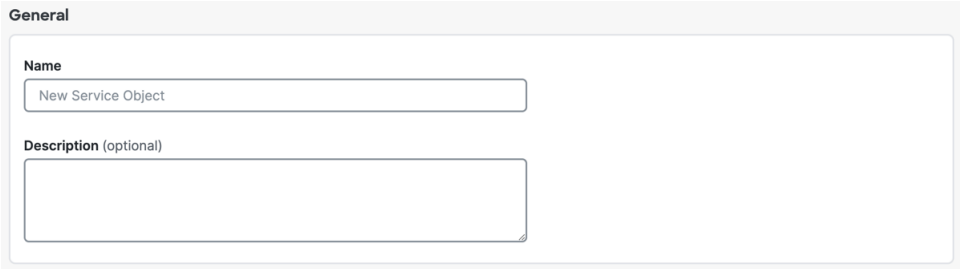
1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Service Objects**, navigate to **Service objects and groups**, and then click **Add service object**.



3. Navigate to **General**.



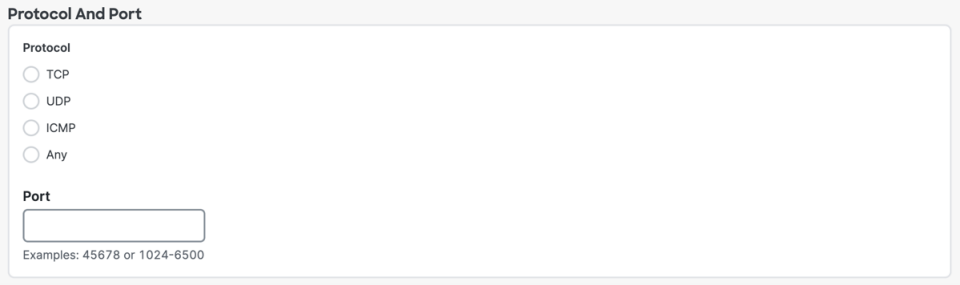
   a) For **Name**, enter a unique name for the Service Object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) For **Description**, enter text that describes the Service Object.

4. Navigate to **Protocol And Port**.
   a) For **Protocol**, choose a protocol for the Service Object.

   > **Note**
   >
   > Select **Any** to add any protocols for the Service Object.

   b) For **Port**, enter a port or range of ports.

      Separate the range of ports with a hyphen (**-**), for example, **1024-6500**.



5. Click **Add Service Object**.

About Importing a CSV File of Service Objects

Describes About Importing a CSV File of Service Objects in Cisco Secure Access. You can import comma-separated values (CSV) files that contain the information required to add Service Objects in Cisco Secure Access.

You can import comma-separated values (CSV) files that contain the information required to add Service Objects in Cisco Secure Access. A Service Object represents a port, range of ports, or one of the supported transport protocols or any protocols. For information about adding a single Service Object in Secure Access, see Add a Service Object.

When you upload the Service Objects in a CSV file, Secure Access first validates the required attributes for adding each Service Object. If the file contains errors, Secure Access displays the errors and provides suggestions for correcting the errors. If the CSV file is valid, Secure Access adds all of the new Service Objects.

During the import of the Service Objects, you can choose to add a Service Object Group and include all of the Service Objects in the group. For information about Service Object Groups, see Add a Service Object Group.

After you add the Service Objects in Secure Access, these resources are available for you to select in the Service Object Groups and on destinations for the internet and private access rules in the Access policy. For information about reusable destination components, see Components for Internet Access Rules and Components for Private Access Rules.

Guidelines: Import Service Objects in Secure Access

- Secure Access provides a template that you can download and use to create a CSV file with service objects. For more information see Download the CSV File Template.
- Review the recommendations for adding Network and Service Objects in your organization. For more information, see General Limits for Network and Service Objects.
- Secure Access adds all valid Service Objects in a CSV file or none if the data for the Service Objects is invalid.
- A Service Object is defined by the ports and protocol information for the service. For more information, see About Service Objects.

Upload CSV File with Service Objects

Provides instructions for completing the Upload CSV File with Service Objects workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Upload a CSV file with the service objects to Secure Access.

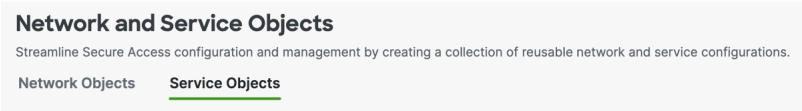
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

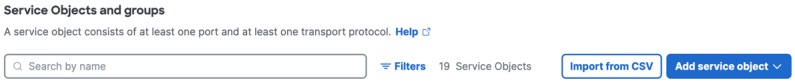
Procedure

---

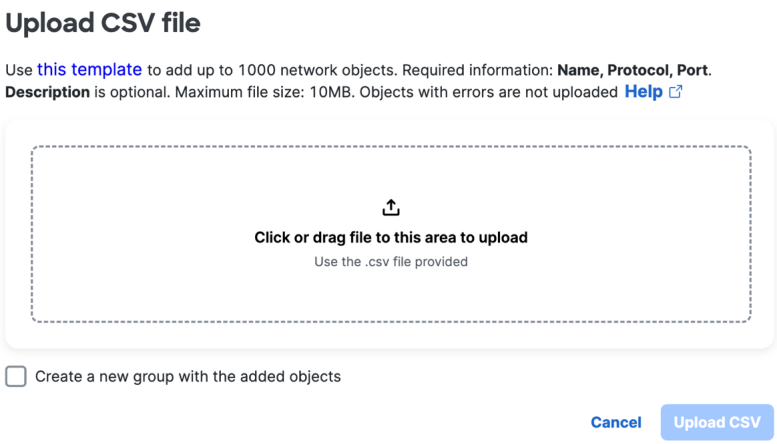
1. Navigate to **Resources** > **Network and Service Objects**.



2. On **Service Objects**, navigate to **Service objects and groups** , and then click **Import from CSV**.



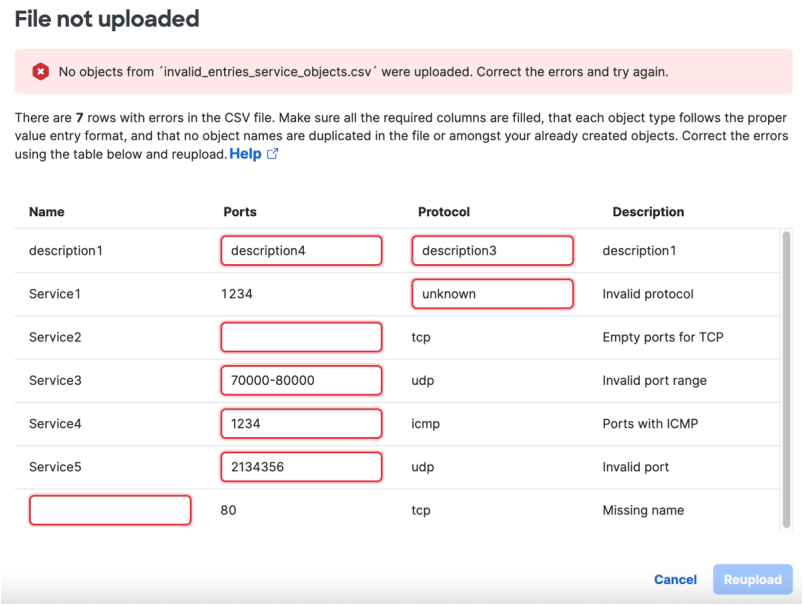
3. For **Upload CSV file**, click or drag a CSV file with the service objects to the area in Secure Access. Download the CSV file template. Click on **this template** to download a CSV file that you can use to upload the network objects.



4. Check **Create a new group with the added objects** to include the service objects from the CSV file to a service object group.
   a) For **Name**, enter a unique name for the Service Object Group that will be added in Secure Access.
   b) (Optional) For **Description**, enter a description for the Service Object Group.
5. Click **Upload CSV** to validate and upload the CSV file with the service objects.

   Secure Access checks if the CSV file is valid.

   - If the CSV file is valid, Secure Access adds all of the service objects.
   - If the CSV file is invalid, Secure Access provides information about the invalid fields. You can correct the invalid fields and upload the service objects again.



a) Click **Upload** to validate the CSV file again and upload the service objects.

Examples of Valid CSV Files

Describes Examples of Valid CSV Files in Cisco Secure Access and outlines CSV File with Service Object and UDP Protocol, CSV File with Service Object and TCP Protocol, and CSV File with Service Object and ICMP Protocol. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

CSV File with Service Object and UDP Protocol

```
name,description,protocol,port
name110,about the test service object 7,udp,9000
```

CSV File with Service Object and TCP Protocol

```
name,description,protocol,port
name111,description1,tcp,9000
```

CSV File with Service Object and ICMP Protocol

```
name,description,protocol,port
name112,description for 112,icmp
```

CSV File with Service Object and Any Protocols and Port Range

```
name,description,protocol,port
name113,description for 113,any,1024-6500
```

Edit a Service Object

Provides instructions for completing the Edit a Service Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

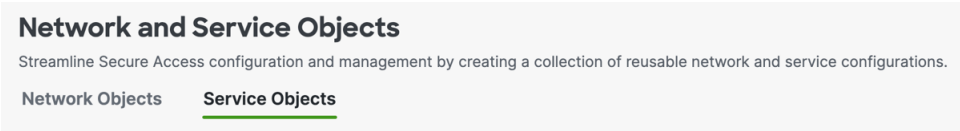
Edit a Service Object in Secure Access.

Before you begin

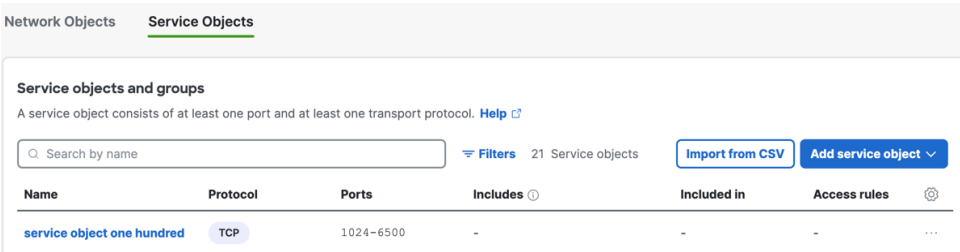
- Full Admin user role. For more information, see Manage Accounts.

Procedure

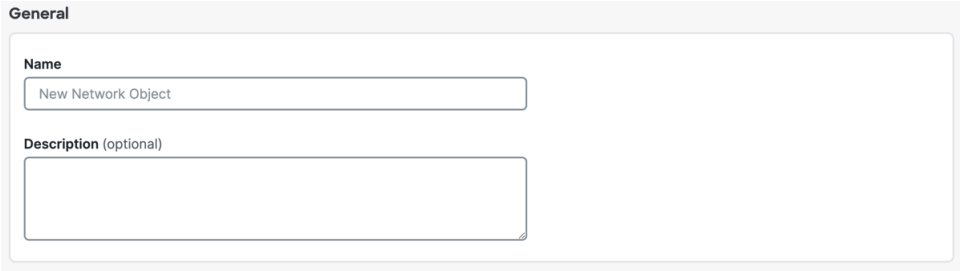
1. Navigate to **Resources** > **Network and Service Objects**.



2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
   a) Navigate to a Service Object, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Name** column, click on the name of a Service Object, and then click **Edit**.



4. Navigate to **General**.



   a. For **Name**, enter a unique name for the Service Object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.

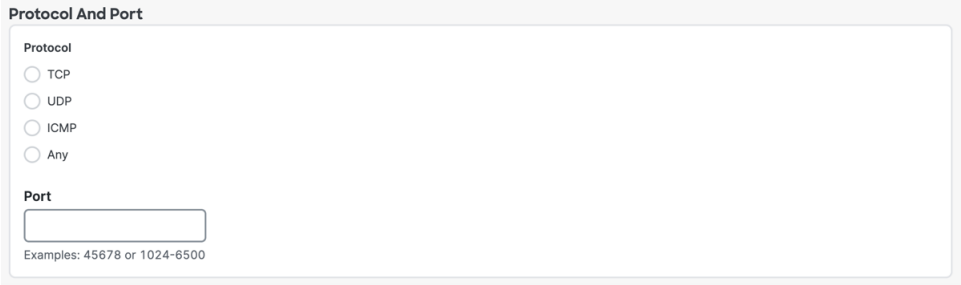
   b. (Optional) For **Description**, enter text that describes the Service Object.

5. Navigate to **Protocol And Port**.
   a) For **Protocol**, choose a protocol for the Service Object.

      Select **Any** to add any protocol for the Service Object.

   b) For **Port**, enter a port or range of ports.

      Separate the range of ports with a hyphen (**-**), for example: **1024-6500**.



6. Navigate to **Rules and Groups**.
   a. For **Rules**, expand a rule, and then click on the name of a rule to edit the rule. For more information, see Manage the Access Policy.



   b. For **Groups**, expand a Service Object Group, and then click on the name of group to edit the group. For information about Service Object Groups, see Get Started with Service Object Groups.

7. Click **Save changes**.

Duplicate a Service Object

Provides instructions for completing the Duplicate a Service Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Create a new Service Object in Secure Access from an existing Service Object.

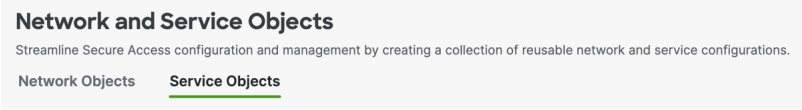
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Resources** > **Network and Service Objects**.



2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table. Navigate to the **Name** column, click on the name of a Service Object, and then click **Duplicate**.
4. For **Name**, enter a unique name for the new Service Object.
5. Click **Duplicate** to confirm the addition of the Service Object.



Delete a Service Object

Provides instructions for completing the Delete a Service Object workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

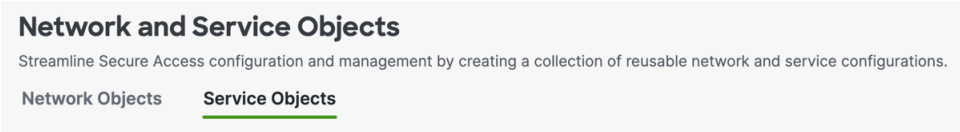
Remove a Service Object in Secure Access.

Before you begin

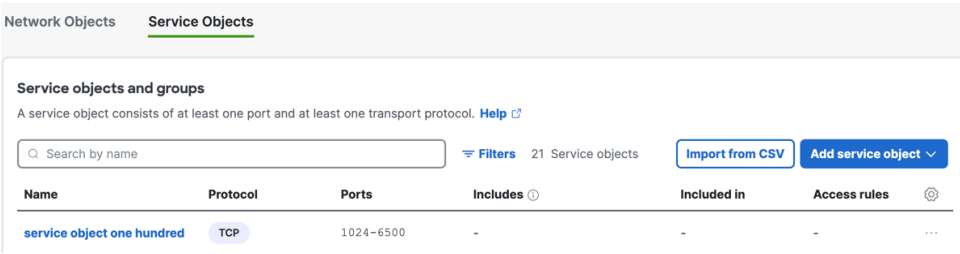
- Full Admin user role. For more information, see Manage Accounts.

Procedure

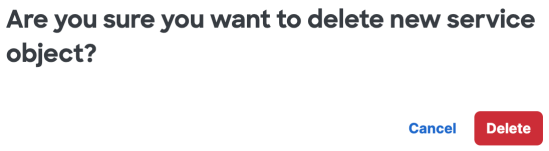
1. Navigate to **Resources** > **Network and Service Objects**.



2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
   a) In the table, navigate to an item in the table, click on the ellipsis (**...**), and then choose **Delete**.
   b) In the table, navigate to the **Name** column, click on the name of a Service Object, and then click **Delete**.



4. Click **Delete** to confirm the removal of the Service Object.



Get Started with Service Object Groups

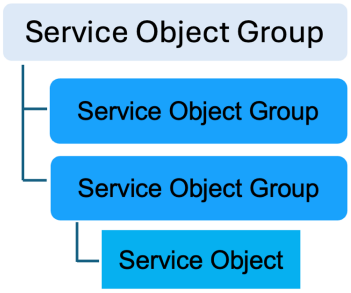
Describes Get Started with Service Object Groups in Cisco Secure Access. To get started, add Service Object Groups in Secure Access.

To get started, add Service Object Groups in Secure Access. After you add a Service Object Group, you can view, edit, duplicate, or delete the group.

You can select the Service Object Groups and Service Objects in the groups as destination components on the internet and private access rules in the Access policy. For more information, see Components for Internet Access Rules and Components for Private Access Rules.

Guidelines: Add Service Object Groups in Secure Access

- Review the recommendations for adding Network and Service Objects in your organization. For more information, see General Limits for Groups.
- A Service Object Group must have a unique name for all Service Object Groups in the organization.
- A Service Object Group can include Service Objects and other Service Object Groups. Secure Access supports three levels of nested groups.



- Secure Access does not support circular dependencies of groups in Service Object Groups.

Add Service Object Groups

- For more information, see Add a Service Object Group.

Manage a Service Object Group

After you add a Service Object Group in Cisco Secure Access, you can edit, duplicate, or remove the resource.

- View Objects, Groups and Values in a Service Object Group
- Edit a Service Object Group
- Duplicate a Service Object Group
- Delete a Service Object Group

View Service Objects and Groups

- For more information, see View Service Objects and Groups.

Add a Service Object Group

Provides instructions for completing the Add a Service Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Cisco Secure Access, a Service Object Group is a collection of Service Objects and other Service Object Groups. After you add a Service Object Group in Secure Access, you can view the details for the resource. For more information, see View Service Objects and Groups.

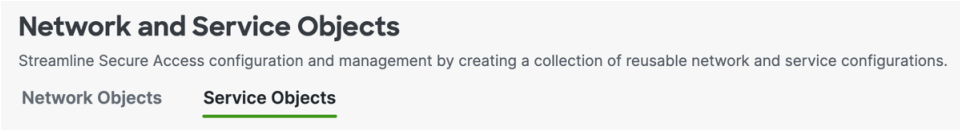
When you configure a Service Object Group, select the Service Objects and other Service Object Groups to include in the group. You can create new Service Objects and add these resources to the group. You can also add composite service information in the Service Object Group. Composite service information is not reusable in the organization.

Before you begin

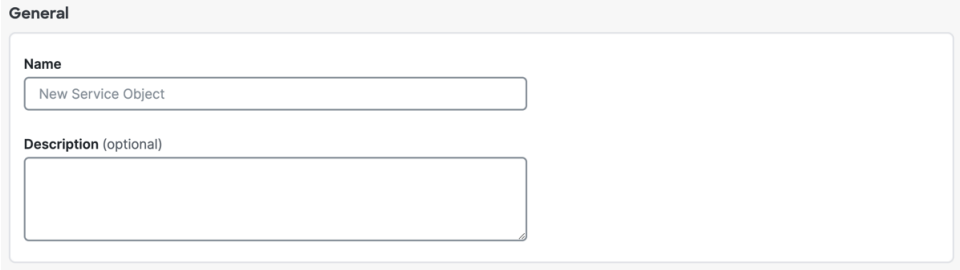
- Full Admin user role. For more information, see Manage Accounts.

Procedure

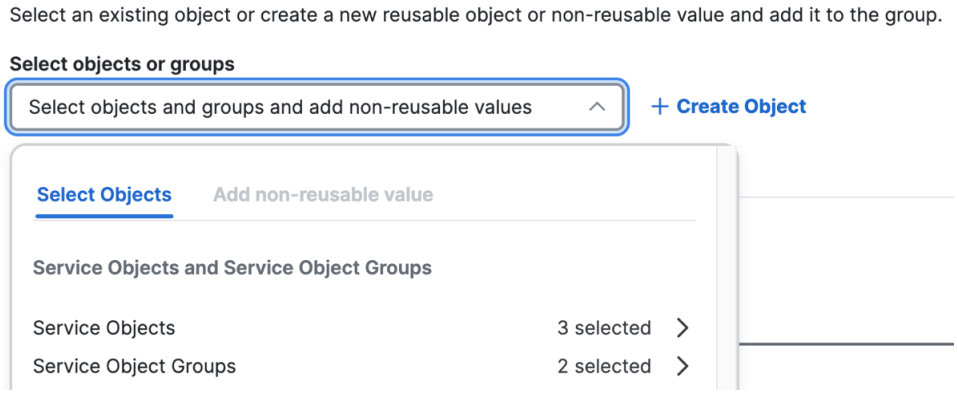
1. Navigate to **Resources** > **Network and Service Objects**.



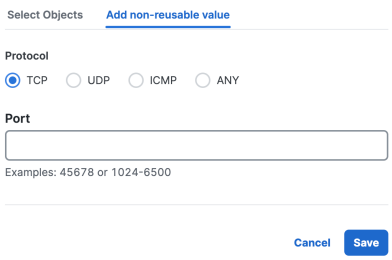
2. On **Service Objects**, navigate to **Service objects and groups**, and then click **Add service object group**.
3. On **Add New Service Object Group**, navigate to **General**.



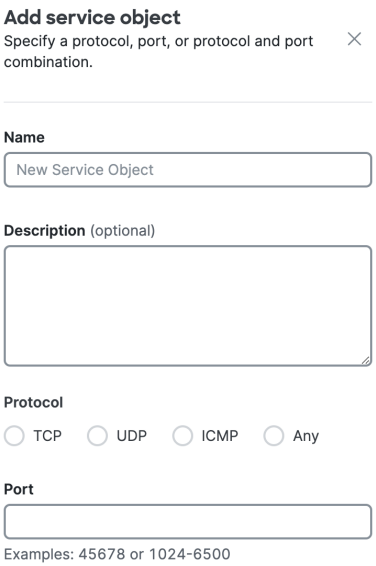
4. For **Name**, enter a unique name for the Service Object Group. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
5. For **Description**, enter text that describes the Service Object Group.
6. Navigate to **Group Values**, and then navigate to **Select objects or groups**.



   a) Click **Select objects and groups and add non-reusable values**.
   b) Click **Select objects**, choose from the lists of configured Service Objects and Service Object Groups.
   c) Click **Add non-reusable value**.
   d) Choose a protocol–**TCP**, **UDP**, **ICMP**, or **ANY**.
   e) Enter a port or range of ports.
   f) Click **Save**.



7. Click **+ Create Object**.
   a) For **Name**, enter a unique name for the Service Object.
      Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) For **Description**, enter text that describes the Service Object.
   c) For **Protocol**, choose a protocol for the Service Object. Select **Any** to add any protocols for the Service Object.
   d) For **Port**, enter a port or range of ports.
      Separate the range of ports with a hyphen (**-**), for example, **1024-6500**.
   e) Click **Add**.



8. Click **Add Service Group**.

View Objects, Groups and Values in a Service Object Group

Provides instructions for completing the View Objects, Groups and Values in a Service Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View the objects, groups and values that are included in the Service Object Group.

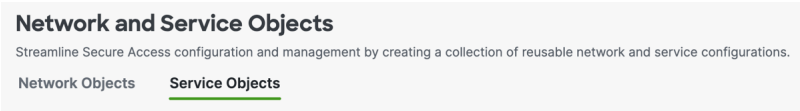
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

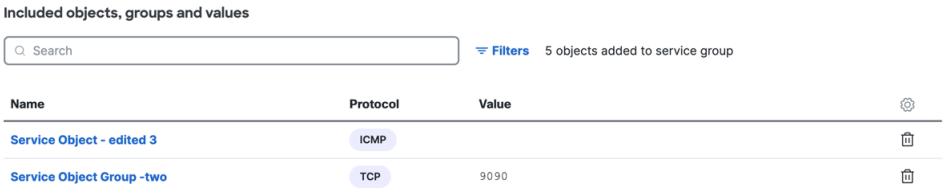
1. Navigate to **Resources** > **Network and Service Objects**.



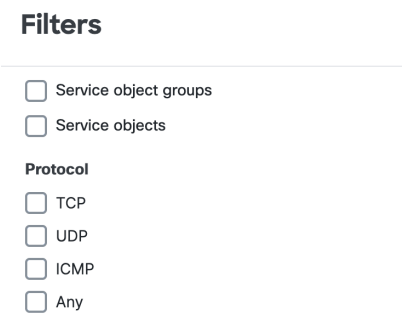
2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
   a) Navigate to a group in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Name** column, click on the name of a Service Object Group, and then click **Edit**.
4. Navigate to **Group Values**, and then navigate to **Included objects, groups and values**.

   Secure Access displays the properties for the objects in the Service Object Group.

   - **Name**–The name of the object or group.
   - **Protocol**–The protocol for the Service Object or **Group**.
   - **Value**–The value of the object, for example range of ports or name of the groups that are included in the Service Object Group.



5. (Optional) In the search bar, enter a sequence of characters to query for the name of the included objects, groups and values.
6. (Optional) Click **Filters**, choose the Service Objects, Service Object Groups, and protocols of the Service Objects.



Edit a Service Object Group

Provides instructions for completing the Edit a Service Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit a Service Object Group in Secure Access.

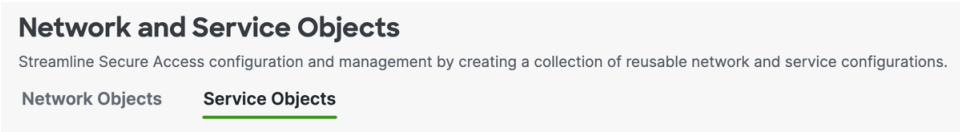
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

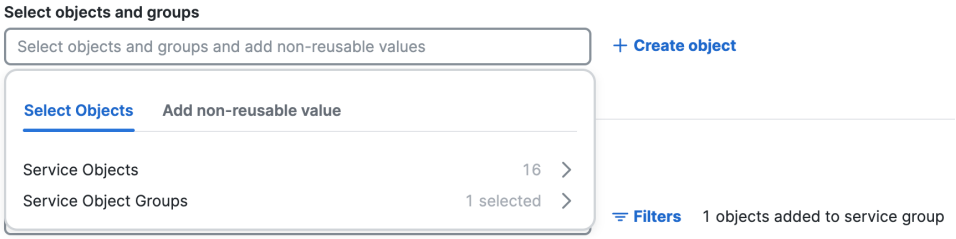
1. Navigate to **Resources** > **Network and Service Objects**.



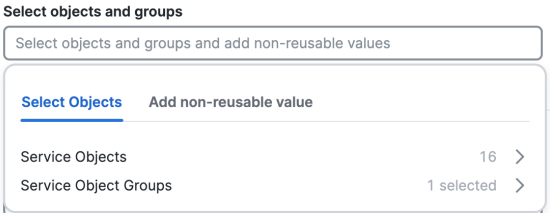
2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
   a) Navigate to a group in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Name** column, click on the name of a Service Object Group, and then click **Edit**.
4. Navigate to **General**.
   a) For **Name**, enter a name for the Service Object Group.
   Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.

   > **Note**
   >
   > You must enter a valid name for the Service Object Group that is unique for all Service Object Groups in the organization.

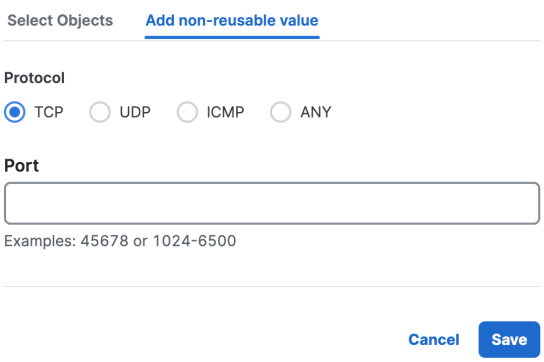
   b) For **Description**, enter text that describes the Service Object Group.
5. Navigate to **Group Values**, and then navigate to **Select objects and groups**.



6. Click **Select objects and groups and add non-reusable values**.
7. Click **Select objects**, and then choose from the lists of configured Service Objects and Service Object Groups.



8. Click **Add non-reusable value**.
   a) Choose a protocol, either **TCP**, **UDP**, **ICMP**, or **ANY** to add any protocols.
   b) Enter a port or range of ports.
   c) Click **Save**.



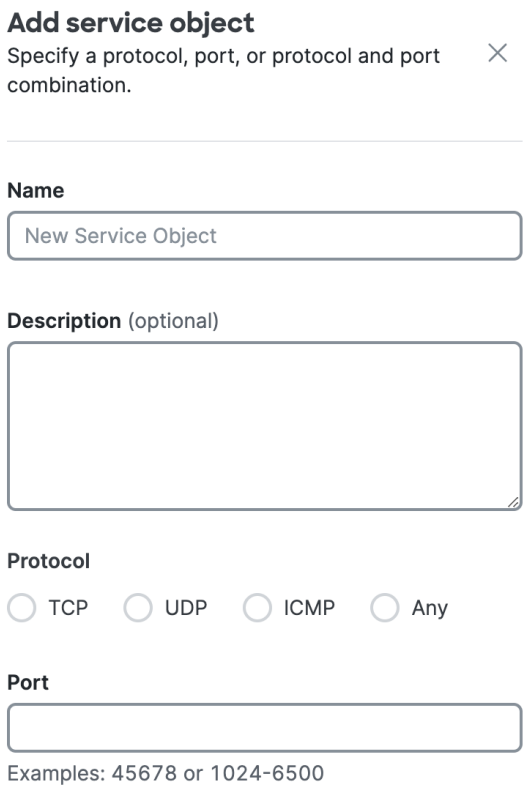
9. Click **+ Create Object**.
   a) For **Name**, enter a name for the Service Object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) For **Description**, enter text that describes the Service Object.
   c) For **Protocol**, choose a protocol for the Service Object.

      Select **Any** to add any protocols for the Service Object.

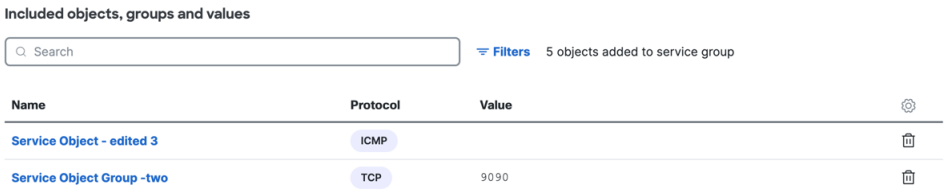
   d) For **Port**, enter a port or range of ports.

      Separate the range of ports with a hyphen (**-**), for example, **1024-6500**.

   e) Click **Add**.



10. Delete an included object, group and values.
    a) Navigate to **Group values**, and then navigate to **Included objects, groups and values**.



b) Navigate to an object in the table, click on the trash can icon to remove the object.

11. Click **Save changes**.

Duplicate a Service Object Group

Provides instructions for completing the Duplicate a Service Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Create a new Service Object Group in Secure Access from an existing Service Object Group.

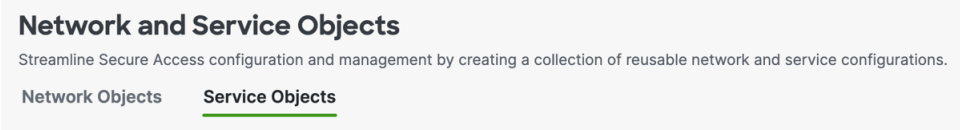
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

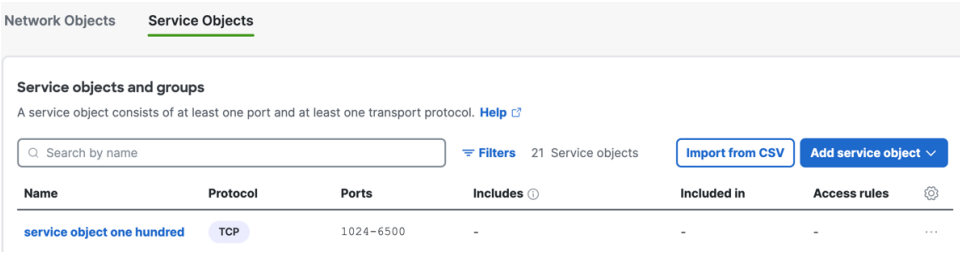
Procedure

---

1. Navigate to **Resources** > **Network and Service Objects**.



2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
4. Navigate to the **Name** column, click on the name of a Service Object Group, and then click **Duplicate**.



5. For **Name**, enter a unique name for the new Service Object Group.
6. Click **Duplicate** to confirm the addition of the Service Object Group.



Delete a Service Object Group

Provides instructions for completing the Delete a Service Object Group workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

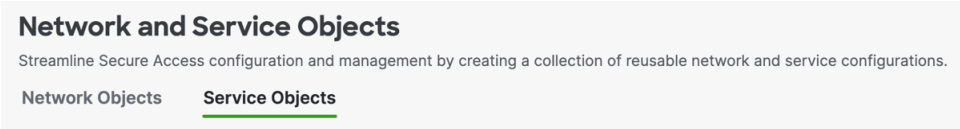
Remove the Service Object Group in Secure Access.

Before you begin

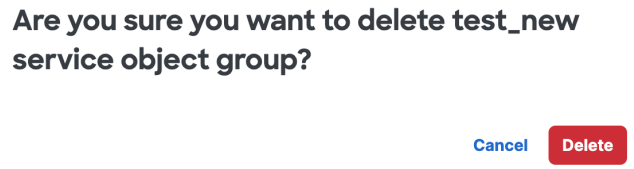
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Network and Service Objects**.



2. Click **Service Objects**, and then navigate to **Service objects and groups**.
3. Navigate to the Service Objects and Groups table.
   a) Navigate to a Service Object Group in the table, click on the ellipsis (**...**), and then choose **Delete**.
   b) Navigate to the **Name** column, click on the name of a Service Object Group, and then click **Delete**.
4. Click **Delete** to confirm the removal of the Service Object Group.



View Service Objects and Groups

Provides instructions for completing the View Service Objects and Groups workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

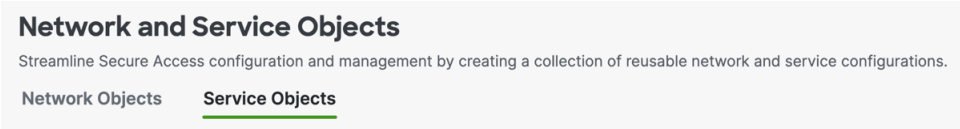
After you add Service Objects and Groups in Cisco Secure Access, you can view the details about the resources.

Before you begin

- A minimum user role of Read Only. For more information, see Manage Accounts.

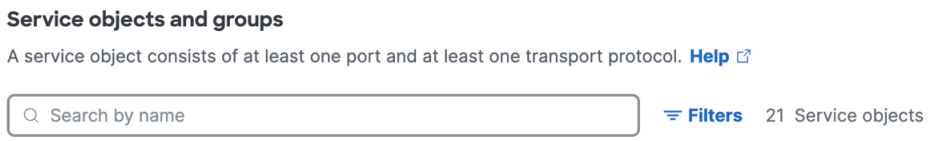
Procedure

1. Navigate to **Resources** > **Network and Service Objects**.

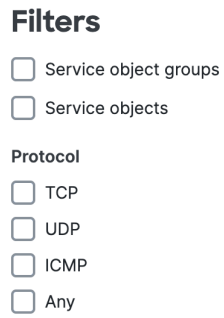


2. On **Service Objects**, navigate to **Service objects and groups**.

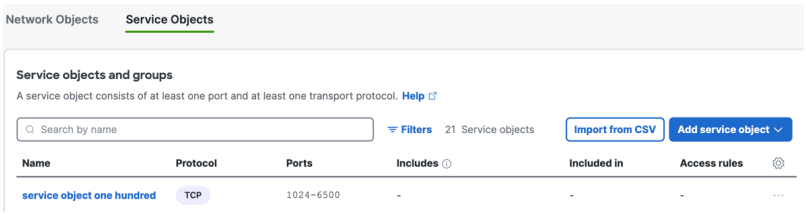
3. (Optional) Search for the Service Objects in the organization. In the search bar, enter a sequence of characters to query for the name of the Service Objects.



4. (Optional) Filter for the Service Objects in the organization. Click **Filters**, choose the Service Objects, Service Object Groups, and protocols of the Service Objects.

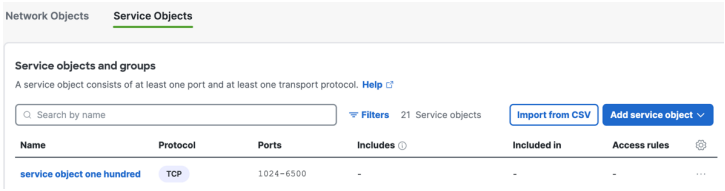


5. In the table, Secure Access displays the properties for the Service Objects and Groups in the organization.

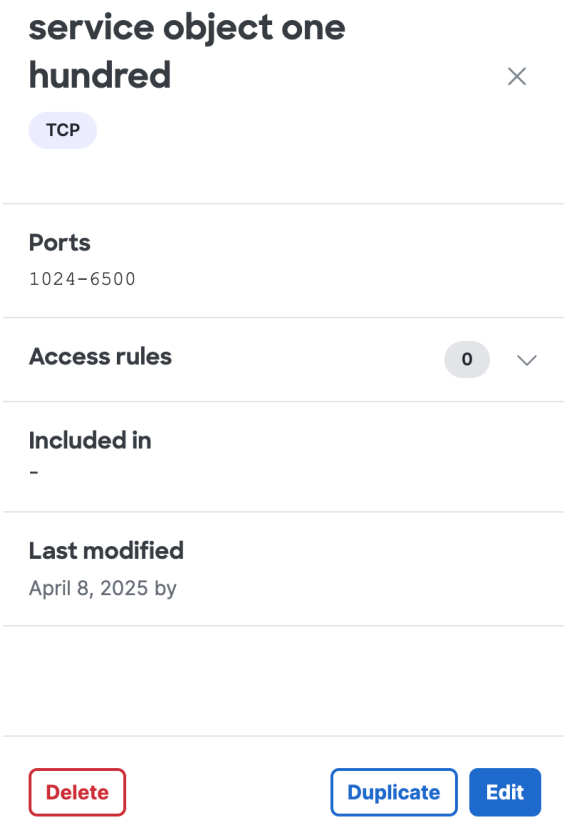


- **Name**–The name of the Service Object or Service Object Group.
- **Protocol**–The protocol of the Service Object or value of the Service Object Group.
  - For a Service Object, the value of the protocol is: **TCP**, **UDP**, **ICMP**, or **ANY**.
  - For a Service Object Group, the value is: **Group**.
- **Ports**–The ports of the Service Object or value of the Service Object Group.
  - For a Service Object, the value of the port or range of ports.
  - For a Service Object Group, the value is none.
- **Includes**–The values of the Service Object or references to the objects that are included in the Service Object Group.
  - For a Service Object, the value is none.
  - For a Service Object Group, the value is the list of Service Objects or Service Object Groups, which the group includes.
- **Included in**–The list of Service Object Groups that include the Service Object or Service Object Group.
  - For a Service Object, the value is the list of Service Object Groups that include the resource.
  - For a Service Object Group, the value is the list of Service Objects or Service Object Groups, which are included in the group.
- **Access rules**–The list of rules that have the Service Object or Service Object Group selected on the rules.

6. (Optional) In the table, navigate to the **Name** column.
   a) Click on the name of a Service Object or Service Object Group in the table to view the details about the resource.



b) View the details about the Service Object or Service Object Group.



17 Manage API Keys

Topics:

- Manage API Keys
- About Secure Access API Keys
- About Key Admin API Keys

Provides an overview of Manage API Keys in Cisco Secure Access, including Manage API Keys, About Secure Access API Keys, and About Key Admin API Keys. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage API Keys

Describes Manage API Keys in Cisco Secure Access. The Secure Access API keys and Key Admin API keys enable you to interact programmatically with the Cisco Secure Access platform.

The Secure Access API keys and Key Admin API keys enable you to interact programmatically with the Cisco Secure Access platform. You can create an API key and secret for each API key and manage your organization's API keys in Secure Access.

- **API Key**—An intent-based Secure Access API key with a configurable key name, description, expiration date, and key access scopes. The API key description is optional.
- **KeyAdmin API key**—An API key that you can use in a program or script to create and manage your organization's Secure Access API keys. The KeyAdmin API key has a configurable key name, description, and expiration date, and key access scopes. The key access scopes are limited to the management of Secure Access API keys. The API key description is optional.

Your API key and API secret are credentials that enable you to authenticate to Secure Access and create short-lived API access tokens. API keys, passwords, secrets, and tokens allow access to your private data. You should never share your credentials with another user or organization.

About Secure Access API Keys

Describes About Secure Access API Keys. The Secure Access API enables you to create, manage, and protect the users, user devices, network connections, and private resources in your organization.

The Secure Access API enables you to create, manage, and protect the users, user devices, network connections, and private resources in your organization.

In REST client, you can use your Secure Access API key credentials to authenticate with Secure Access and generate a short-lived API access token. Then, with your generated access token, make your first API request to the Secure Access API. You must include your access token in every API request. For more information, see Secure Access API Authentication.

You can create any number of granular, multi-scoped Secure Access API keys. When you create an API key, choose a unique key name, description, key expiration date, and API key scopes and permissions. The API key description and expiration date are optional. If you do not set an expiration date when you add the key, Secure Access sets your API key to never expire. For each key scope and API resource, choose either **Read-Only** or **Read/Write** API key permissions.

Once you add an API key to Secure Access, you can refresh your key's credentials, update the key's name, description, expiration date, and key scopes, and delete the API key.

Manage Your Secure Access API Keys

- Add an API Key
- Refresh an API Key
- Update an API Key
- Delete an API Key

Add an API Key

Provides instructions for completing the Add an API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

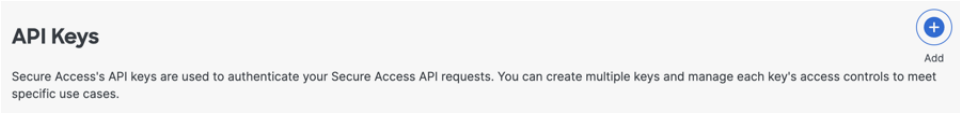
Add API keys in your Secure Access organization. Configure each API key with a unique name, description, API key scopes, and expiry date.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

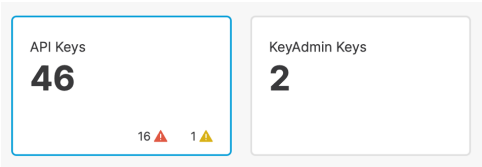
Procedure

1. Navigate to **Admin** > **API Keys**.



2. Click **API Keys** and then click **Add**.

   The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.

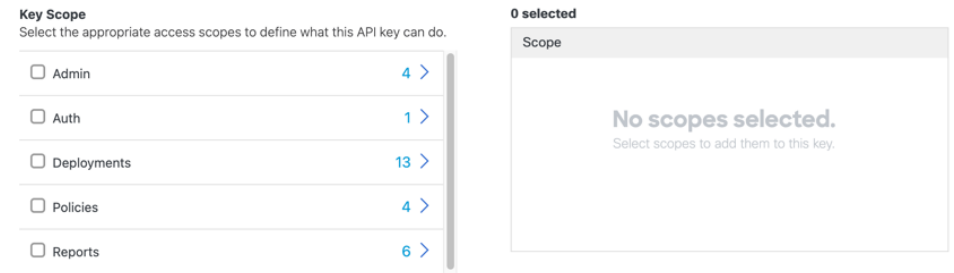


3. Enter a name and description for the key.

   A name must contain less than 256 characters. The key description is optional.



4. Select the key scopes and expand a key scope to view the resources. Check each resource in a key scope to enable access to the resource.

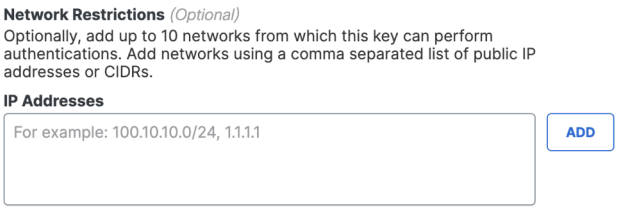


5. Choose **Read-Only** or **Read / Write** for the selected scope and resource.
6. For **Expiry Date**, choose an expiration date or choose **Never expire**.



7. (Optional) For **Network Restrictions**, enter a comma-separated list of public IP addresses or CIDRs, then click **Add**.

> **Note**
>
> You can add up to ten networks to your API key. You can only use your API key to authenticate requests for clients on the selected networks.



8. Click **Create Key**.
9. Copy and save your **API Key** and **Key Secret**.
10. Click **Accept and Close**.



Refresh an API Key

Provides instructions for completing the Refresh an API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

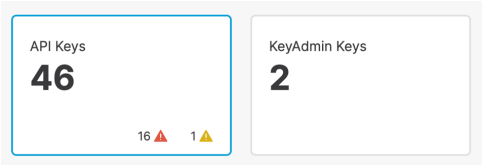
Refresh an API key in your Secure Access organization.

Before you begin

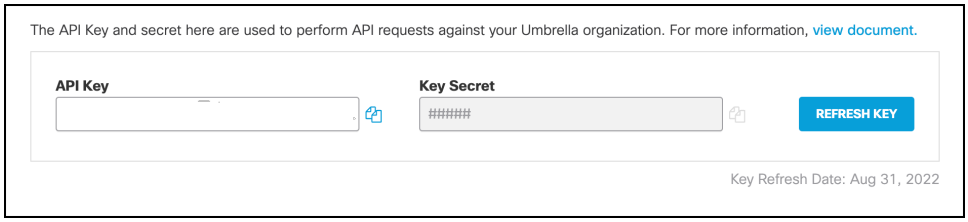
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **API Keys**, and then expand an API key.



3. Click **Refresh Key**.



4. Copy and save your **API Key** and **Key Secret**.

5. Click **Accept and Close**.



Update an API Key

Provides instructions for completing the Update an API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

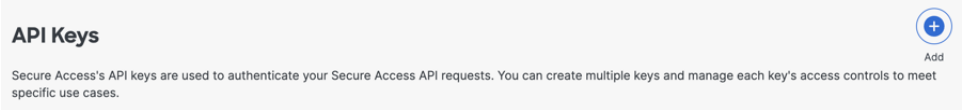
Modify your Secure Access API keys. You can modify one setting or multiple settings on each API key.

Before you begin

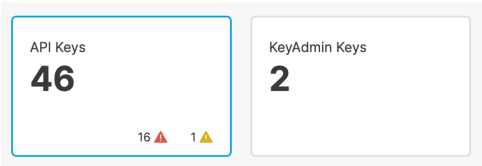
- Full Admin user role. For more information, see Manage Accounts.

Procedure

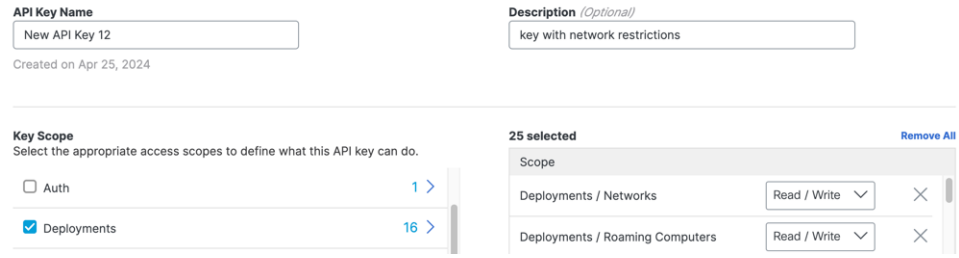
1. Navigate to **Admin** > **API Keys**.



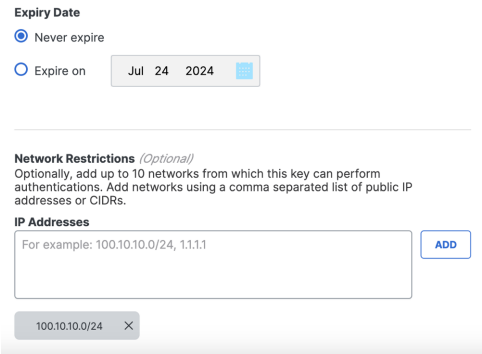
2. Click **API Keys**, and then expand an API key.



3. Modify the **API Key Name**, **Description**, and selected scopes and permissions in **Key Scope**.



4. Modify the **Expiry Date**.
5. For **Network Restrictions**, update the list of IP addresses or CIDRs. Click on the **X** to remove a network address.



6. Click **Save**.

Delete an API Key

Provides instructions for completing the Delete an API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Delete an API key in your Secure Access organization.

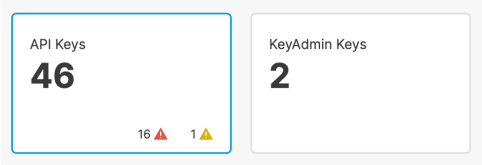
> **Note**
>
> Before deleting any key, carefully examine the Key ID. Do not delete any key that starts with the **MDM-** prefix (for example, `MDM-2026-09-02-10:05:22`).
>
> Keys with the **MDM-** prefix are Deployment Keys. Before attempting any management of these keys, navigate to **Connect** > **End User Connectivity** > **Internet Security** to verify if any devices are associated with the key. Deleting a Deployment Key that is currently in use will result in a high-impact service disruption, including the immediate disconnection of existing roaming devices and the failure of all new device registrations and synchronizations. If you need to manage a key with the **MDM-** prefix, please contact Cisco Technical Support.

Before you begin

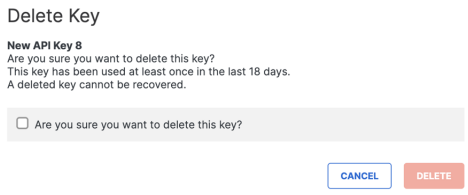
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **API Keys**.
2. Click **API Keys**, and then expand an API key.



3. Click **Delete**.
   a) In the dialog window, click **Delete** to remove the API key from your organization.



About Key Admin API Keys

Describes About Key Admin API Keys in Cisco Secure Access. The Secure Access Key Admin API enables you to create and manage Secure Access API keys programmatically.

The Secure Access Key Admin API enables you to create and manage Secure Access API keys programmatically. In a REST client, use your KeyAdmin API key credentials to authenticate with Secure Access and generate a short-lived API access token. Then, make Key Admin API requests with your access token to create Secure Access API keys for your organization. You must include your access token in every API request. For more information, see Secure Access API Authentication.

You can create any number of Key Admin API keys for your organization. When you create a Key Admin API key, choose a unique key name, description, permissions, and key expiry date. If you do not set an expiration date when you add the key, Secure Access sets your Key Admin API key to never expire.

Once you add a KeyAdmin API key to Secure Access, you can refresh your key's credentials, update the key's name, description, expiration date, and permissions, and delete the API key.

> ⚠ **Caution**
>
> If your organization uses a multi-organization setup, ensure that you generate API keys from the specific organization where the key will be used. Using a parent organization API key to generate client credentials for a child organization can cause virtual appliances to sync with the parent organization, which may lead to DNS outages or the loss of internal domain synchronization for the child organization.

Use Cases

- Programmatically create Secure Access API keys.
- Programmatically manage the Secure Access API keys in your organization–refresh API key credentials, update API key properties, or delete API keys.
- Use the Key Admin API to manage the organization's Secure Access API keys.

Manage Your Secure Access Key Admin API Keys

- Add a Key Admin API Key
- Refresh a Key Admin API Key
- Update a Key Admin API Key
- Delete a Key Admin API Key

Add a Key Admin API Key

Provides instructions for completing the Add a Key Admin API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

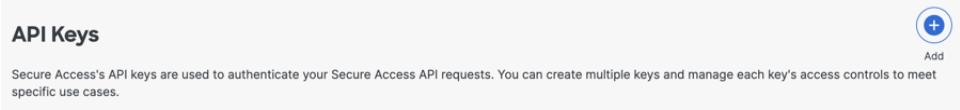
Add Key Admin API keys in your Secure Access organization. Configure each Key Admin API key with a unique name, description, permissions, and expiry date.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

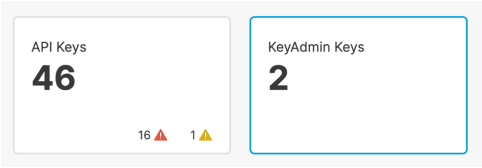
Procedure

1. Navigate to **Admin** > **API Keys** .



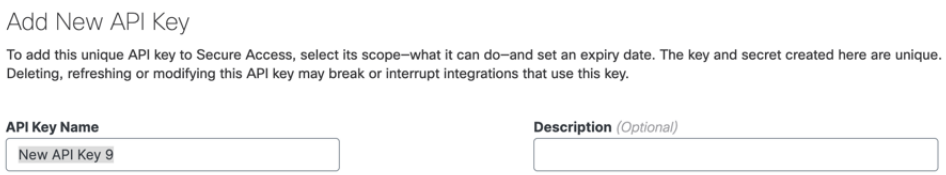
2. Click **KeyAdmin Keys** and then click **Add**.

   The number of expired API keys appears next to the red triangle. The number of API keys that expire within 30 days appears next to the yellow triangle.

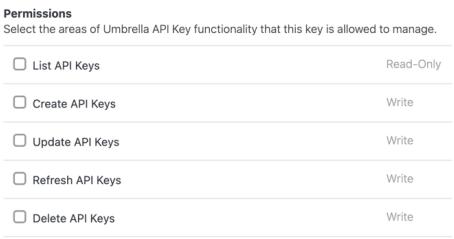


3. Enter a name and description for the key.

   A name must contain less than 256 characters. The key description is optional.



4. Select the permissions for the key.

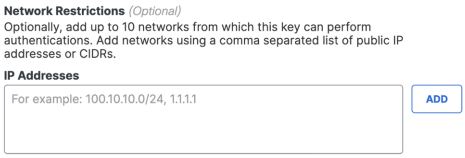


5. For **Expiry Date**, choose the expiration date for the key, or choose **Never expire**.



6. (Optional) For **Network Restrictions**, enter a comma-separated list of public IP addresses or CIDRs, then click **Add**.

> **Note**
>
> You can add up to ten networks to your API key. You can only use your API key to authenticate requests for clients on the selected networks.



7. Click **Create Key**.
8. Copy and save your **KeyAdmin Key** and **Key Secret**.
9. Click **Accept and Close**.



Refresh a Key Admin API Key

Provides instructions for completing the Refresh a Key Admin API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

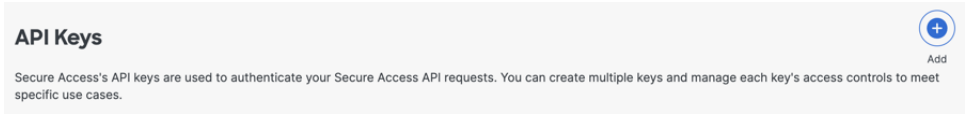
Refresh a Key Admin API key in your Secure Access organization.

Before you begin

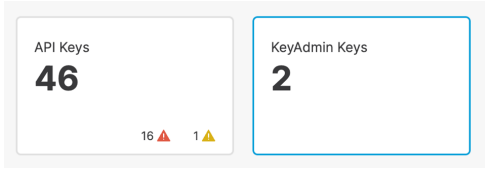
- Full Admin user role. For more information, see Manage Accounts.

Procedure

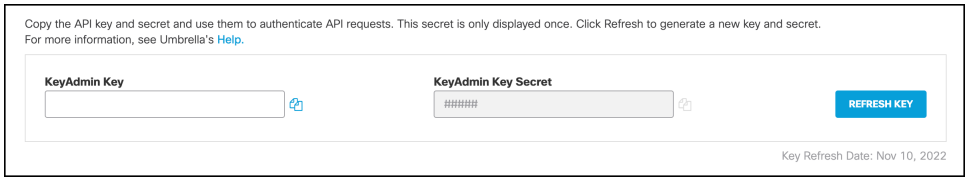
1. Navigate to **Admin** > **API Keys**.



2. Click **KeyAdmin Keys**, and then expand an API key.



3. Click **Refresh Key**.



4. Copy and save your **KeyAdmin Key** and **Key Secret**.
5. Click **Accept and Close**.



Update a Key Admin API Key

Provides instructions for completing the Update a Key Admin API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

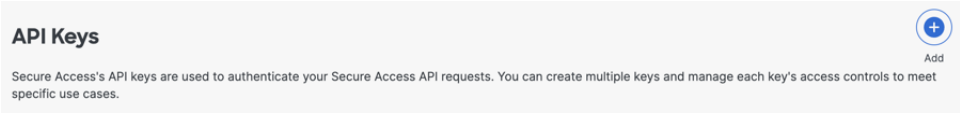
Modify your Key Admin API keys in Secure Access. You can modify one setting or multiple settings on each API key.

Before you begin

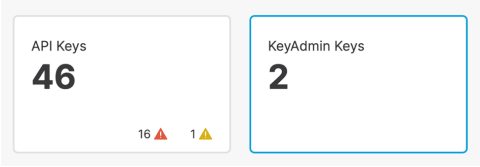
- Full Admin user role. For more information, see Manage Accounts.

Procedure

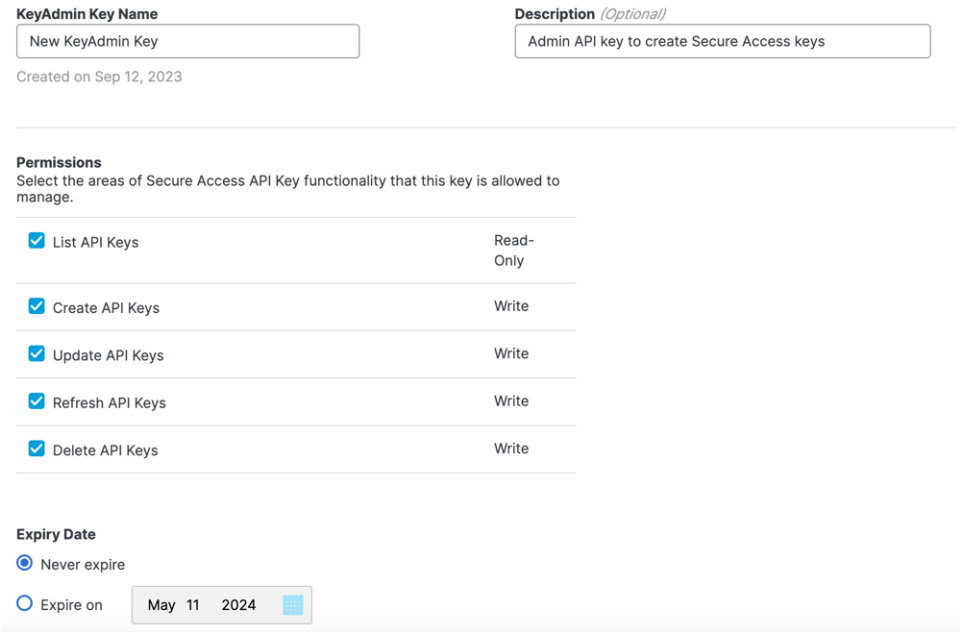
1. Navigate to **Admin** > **API Keys**.



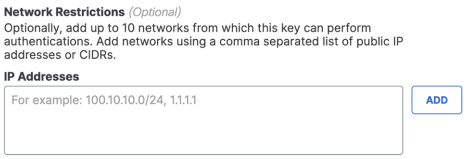
2. Click **KeyAdmin Keys**, and then expand an API key.



3. Modify the **KeyAdmin Key Name**, **Description**, **Permissions**, and **Expiry Date**.



4. For **Network Restrictions**, update the list of IP addresses or CIDRs. Click on the **X** to remove a network address.



5. Click **Save**.

Delete a Key Admin API Key

Provides instructions for completing the Delete a Key Admin API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

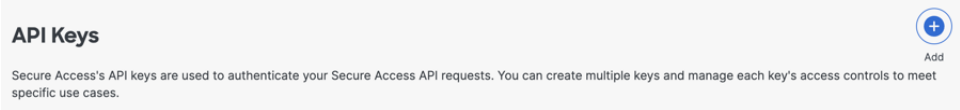
Delete a Key Admin API key in your Secure Access organization.

Before you begin

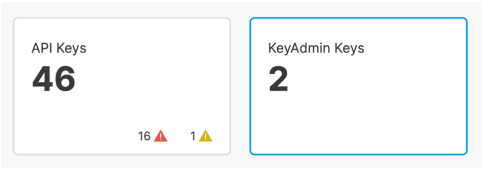
- Full Admin user role. For more information, see Manage Accounts.

Procedure

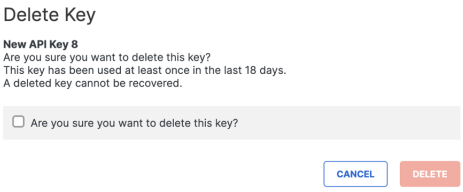
1. Navigate to **Admin** > **API Keys**.



2. Click **KeyAdmin Keys**, and then expand an API key.



3. Click **Delete**. In the dialog window, click **Delete** to confirm the removal of the Key Admin API key.



Part III

Identity and Access

Topics:

- Users, Groups, and Endpoint Devices
- User Directories and Device Management
- Advanced User Configuration Settings
- Identity Providers
- Provision Users, Groups, and Endpoint Devices from Active Directory
- User Authentication Profiles
- Integrations with Open ID Connect Identity Providers
- Integrations with SAML Identity Providers
- Access Policies
- Internet Access Rules
- Internet and SaaS Resources
- Private Access Rules
- IPS Profiles
- Security Profiles
- App Risk Profiles
- Threat Categories
- Traffic Decryption
- Schedules for Access Rules
- Virtual Private Networks and Proxy Settings
- Zero Trust Access
- Endpoint Security

Provides information, guidelines, and steps for how to configure and manage users, identities, access control, and authentication.

18 Users, Groups, and Endpoint Devices

Topics:

- Manage Users, Groups, and Endpoint Devices
- Unenroll Devices for Client-Based Zero Trust Access
- Disconnect Remote Access VPN Sessions

Provides an overview of Users, Groups, and Endpoint Devices in Cisco Secure Access, including Manage Users, Groups, and Endpoint Devices, Unenroll Devices for Client-Based Zero Trust Access, and Disconnect Remote Access VPN Sessions. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Users, Groups, and Endpoint Devices

Describes Manage Users, Groups, and Endpoint Devices in Cisco Secure Access. Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs).

Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs). Once integrated with Secure Access, you can protect and monitor the connections for the users and devices to internet and private destinations by configuring Access rules in the organization's policy.

- You can integrate multiple cloud IdPs with Secure Access.
- Endpoint device integration requires devices provisioned by an on-premise Active Directory domain controller (DC) and Cisco AD Connector version 1.14.4 or newer. For more information, see Connect Active Directory to Secure Access and Configure Updates on AD Connectors.

In addition to integrations with identity providers for provisioning users and groups, we recommend that you configure user authentication profiles. Authentication profiles describe integrations with single sign-on (SSO) IdPs. SSO IdPs authenticate users that connect through the Secure Access Secure Web Gateway (SWG) or with Secure Access Zero Trust Access.

- You can set up multiple authentication profiles in Secure Access.
- An authentication profile describes the association between a provisioning IdP and an SSO IdP.

After you add user directory integrations and set up user authentication profiles, Secure Access displays the users and groups that you provisioned in the organization.

Get Started with User Configuration Management

First, configure a user directory integration with Secure Access. The directory integration provisions users and groups into Secure Access.

Then, set up SSO authentication for users that connect to the web through the Secure Web Gateway or communicate with private destinations through Zero Trust Access.

Step 1 – Manage User Directories

- Provision the organization's users and groups into Secure Access. For more information, see Configure User Directory Integrations.
- Manage the integrated user directories. for more information, see Manage User Directories.

Step 2 – Manage User Authentication Profiles

- Configure integrations with SSO authentication providers in Secure Access. For more information, see Add User Authentication Profiles.
- Manage the added user authentication profiles. for more information, see Manage User Authentication Profiles.

Get Started with Endpoint Device Management

Configure your on-premise Active Directory integration and provision your identity endpoints in Secure Access, see Manage Active Directory Integration.

View Provisioned Users and Groups

After you provision users, group, and endpoint devices in Secure Access, you can view the information about these identities.

- View User Details
- View Group and Organizational Unit Details
- View Endpoint Device Details

Manage Remote Access VPN and Zero Trust Device Connections

In Secure Access, manage the user connections.

- Disconnect Remote Access VPN Sessions
- Unenroll Devices for Client-Based Zero Trust Access

Manage End-User Connectivity

Describes Manage End-User Connectivity in Cisco Secure Access. Secure Access provides secure connectivity to the internet and your digital resources.

Secure Access provides secure connectivity to the internet and your digital resources. To route network traffic from endpoints securely, you can:

- Manage the DNS servers deployed in your organization
- Manage private resources configured for Zero Trust access
- Manage client IP address ranges and profiles used by virtual private networks (VPNs)
- Protect or bypass traffic to certain internet resources
- Configure comprehensive endpoint internet security settings

DNS Servers

Add DNS servers to resolve DNS requests for certain domains from remote clients. For more information, see Manage DNS Servers.

Traffic Steering for Cisco Secure Client Connections

View traffic steering rules for zero trust connections. For certain private resource configurations, you can specify subdomains to exclude from zero trust access. For more information , see Traffic Steering for Client-Based Zero Trust Connections.

Virtual Private Networks Settings and Profiles

Configure VPN settings and profiles. For more information, see Manage Virtual Private Networks.

Internet Security

Steer traffic from endpoints to Secure Access or directly to the internet. For more information, see Manage Internet Security.

View Users Provisioned in Secure Access

Provides instructions for completing the View Users Provisioned in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

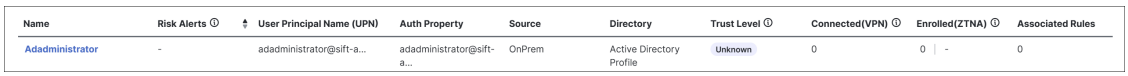
After an administrator provisions users in Cisco Secure Access, you can view details about the users including information about the access rules that apply to the users.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and click **Users**.
   Secure Access displays a table of users provisioned in your organization. You can use filters to refine your search, including components like VPN or ZTNA, and ZTNA filters for active or inactive connections.
2. The table includes the following columns:
   - **Name**–The first and last names of the user.
   - **Risk Alerts**–The number of risk categories detected for the user in last seven days.
   - **User Principal Name (UPN)**–The User Principal Name for the user.
   - **Auth Property**–The property that Secure Access uses to authenticate the users in the organization.
   - **Source**–The method or identity provider (IdP) that provisioned the user.
   - **Directory**–The name of the user directory for the (IdP) integration.
   - **Trust Level**–The trust level of users provisioned by an IdP. This column is available as a table filter and within the User Details component. Trust Level in Secure Access requires integration with Cisco Identity Intelligence via Security Cloud Control. For more information, see Integrate Cisco Identity Intelligence. When enabled, eligible users will have Trust Levels from the following range of values:
     - **Trusted**–Indicates the user has an exceptional level of safety.
     - **Favorable**–Indicates the user has a minimum level of safety.
     - **Neutral**–Indicates the user has been evaluated and has neither positive nor negative behavior.
     - **Questionable**–Indicates the user is displaying behavior that may indicate risk or may be undesirable.
     - **Untrusted**–Indicates the user is displaying behavior that is exceptionally high risk, malicious, or undesirable.
     - **Unknown**–Indicates the user was not yet evaluated, or insufficient data is available to assert a trust level.
   - **Connected (VPN)**–The number of connections with Secure Access virtual private network (VPN) from the user's devices.
   - **Enrolled (ZTNA)**–The number of connections with Secure Access Zero Trust Access from the user's devices.
   - **Associated Rules**–The number of access rules that include the user.
3. Navigate to a user.



View User Details

View user details.

Get the information about a user provisioned in the Secure Access organization.

Before you begin

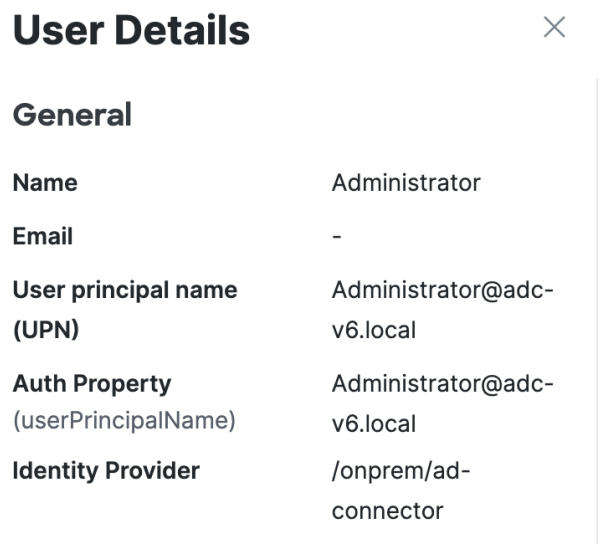
- Ensure you have at least a Read-only user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and click **Users**.
2. Select a user, and then click their name to view the details.

   The attributes for the user include:

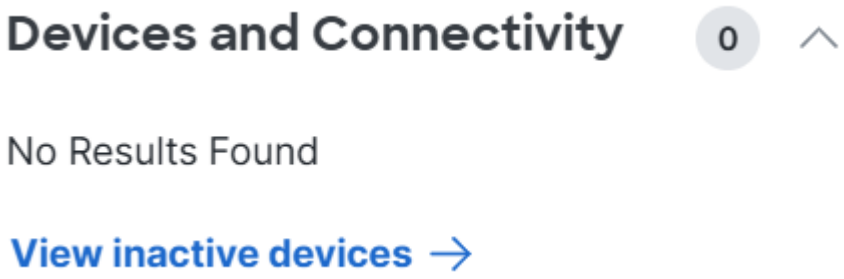
   - **Name**–The name of the user.
   - **Email**–The email of the user.
   - **User Principal Name**–The User Principal Name for the user.
   - **Auth Property**–The name and value of the property that Secure Access uses to authenticate the users in the organization.
   - **Identity Provider**–The identity provider that manages the user account.



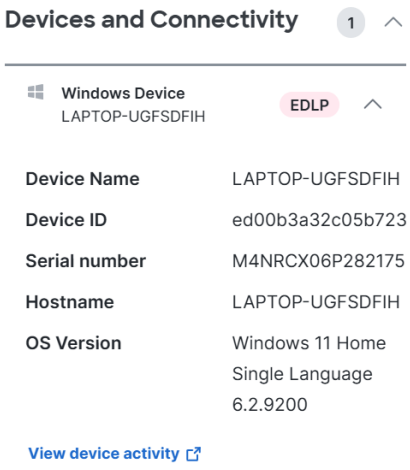
   The number and information of user devices connected.

   - **Connection**–The type of connection
   - **IP address**–The IP address of the device.
   - **OS Version**–The version of the device's operating system.

   If the user has not enrolled in any device, the **Devices and Connectivity** area will not show any device details.

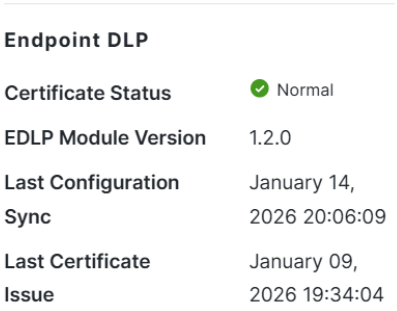


In the **Devices and Connectivity** area, you can view the number of Endpoint Data Loss Prevention (DLP) devices that you have enrolled. Each device shows the details such as device name, device identification number, serial number, hostname, operating system version.



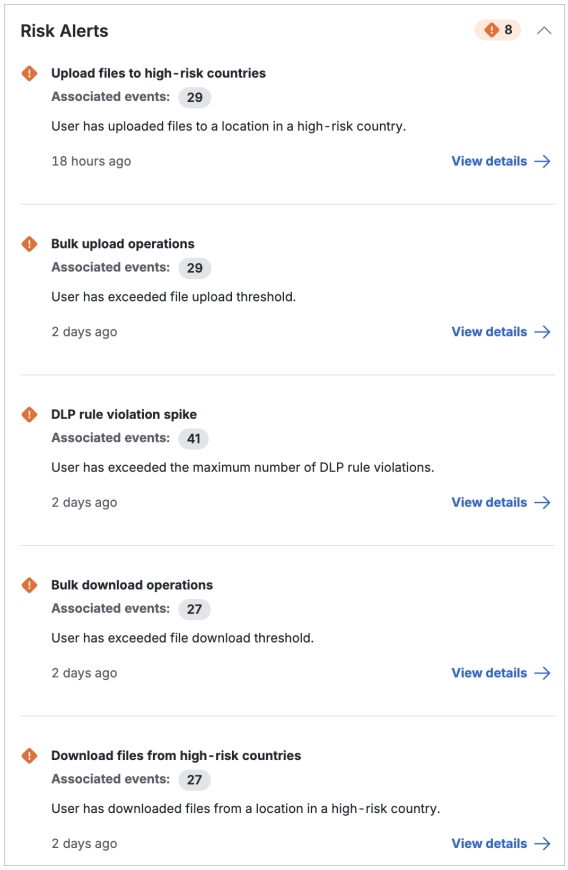
When you click the **View device activity** link, you will be directed to the Data Loss Prevention report, which displays a list of devices that are currently active.

You can also check the certificate status, module version of Endpoint DLP, date and time when the Endpoint DLP device was last configured, and date and time when the certificate was last issued.

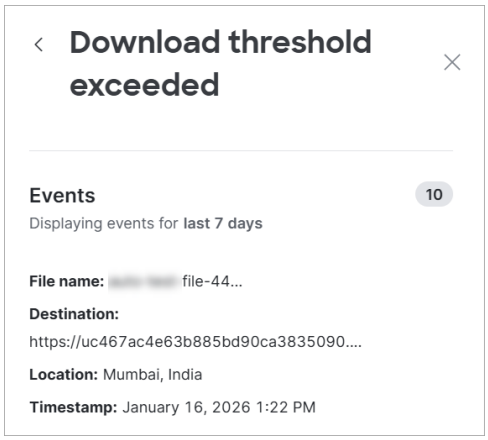


If you want to cancel the enrollment, click **Unenroll device**.

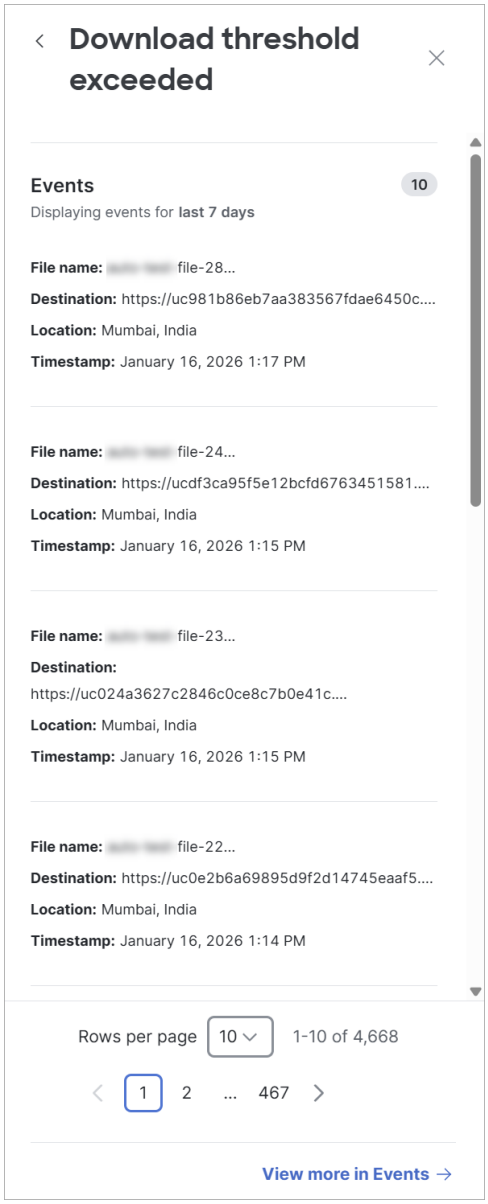
The **Risk Alerts** section displays alerts upto past thirty days for the user. The alerts appear based on their categories. It also displays the number of associated events for each alert category.



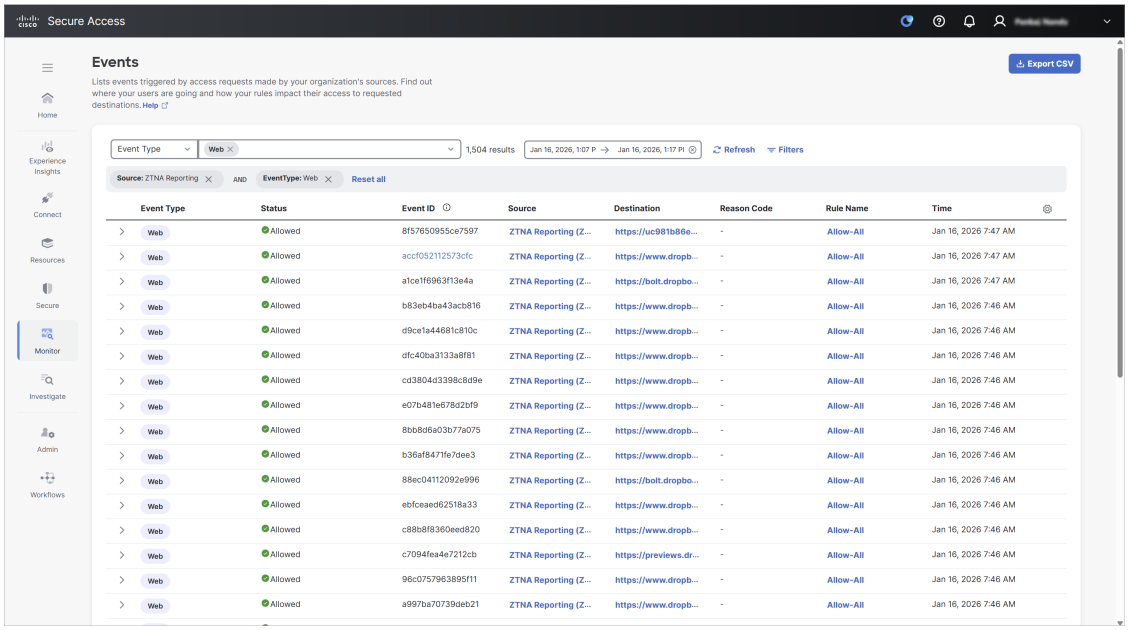
To view details for each risk alert, click **View details** to display details of each event for the risk alert category.



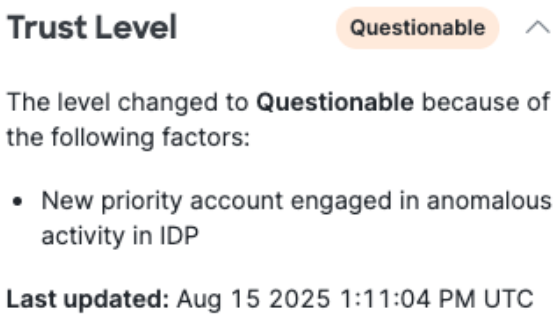
To view all the events that are associated with a risk alert, click **View more in Events**.



This opens the **Events** page and automatically applies necessary filters to display the events for that specific risk alert. For more information on Events, see Events Report.

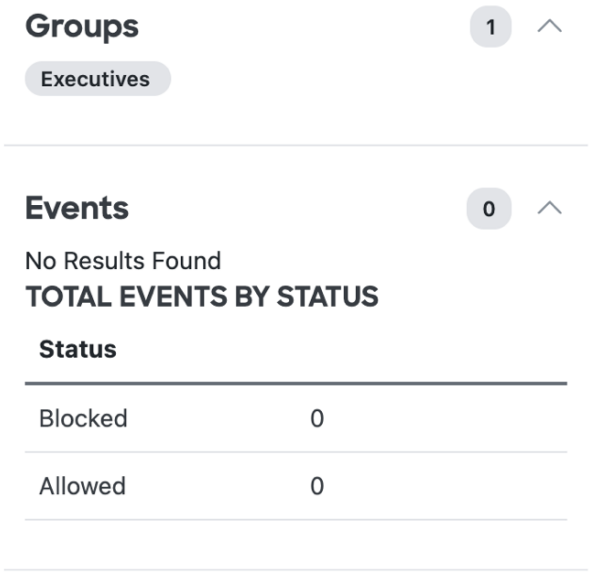


The **Trust Level** section displays the user's current trust level, an explanation of that trust level, and the date and time the trust level was last updated.

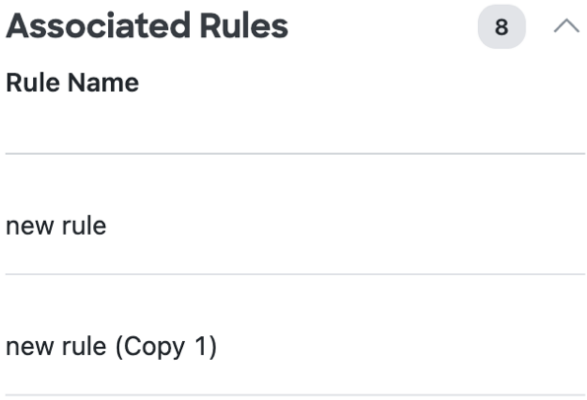


For a description of each possible trust level value (Trusted, Favorable, Neutral, Questionable, Untrusted, Unknown), refer to View Users Provisioned in Secure Access. For more information, see Integrate Cisco Identity Intelligence with Secure Access.

- **Groups**–The number of groups that include the user and the name of the groups.
- **Events**–The number of events created by the user and the status of the events.



The Secure Access rules in the Access policy applicable to the user.



Export Users to CSV

Describes how to apply filters to the Users list and export the data to a CSV file.

The robust filtering and search capabilities on the **Users, Groups, and Endpoint Devices** page help you quickly narrow down and analyze significant security and network activities. You can use a combination of basic search box filters and advanced filter options to focus on specific events. Export the results for troubleshooting, record keeping, and more.

Before you begin

You must use at least one filter and apply it to the table before you can export the information into a .csv.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**.
2. Click the **Users** tab.
3. Beside the search bar, click **Filters** and launch the pop-up window for selections. You have the following options in drop-down menus:

- Directory – Select the directory type currently configured for your users.
- Risk alert – Select the risk alert you want to filter on.
- Trust level – Select the trust level you want to filter on.
- (Optional) VPN Filters – Check this box to only show active VPN sessions. Note that using this option disables the other filter options listed above.
- VPN profile - Select the VPN profile you want to filter on.

4. Filters are automatically applied. Once you have modified the filter selections, review the table. Click on the **Name** of an entry to examine the details of the user, such as devices and connectivity, device ID, OS version, VPN access information and more.
5. To export the table, click **Export CSV**.
6. Enter an **Exported Report Name**. This is what the file is saved as once it is exported locally.
7. Enter the **Results Row Limit** to limit the exported report to a certain number of rows. There is a maximum limit of 1,000,000 rows allowed per report; if you do not express a specific value for your report and the number of rows from your filter exceeds the max number, the report is truncated to 1,000,000 rows by default.
8. Click **Export**. Alternatively, click **Cancel** to not save the report.

View Group and Organizational Unit Details

View the provisioned groups in Secure Access.

View the provisioned groups in Secure Access.

Administrators can use Identity Providers (IdPs) that are integrated with Secure Access to provision IdP groups and Google Chromebook Organizational Units (OUs) in Secure Access. Once groups and OUs are provisioned, you can view their details and access rules that apply to users and endpoint devices in the groups or OUs.

Before you begin

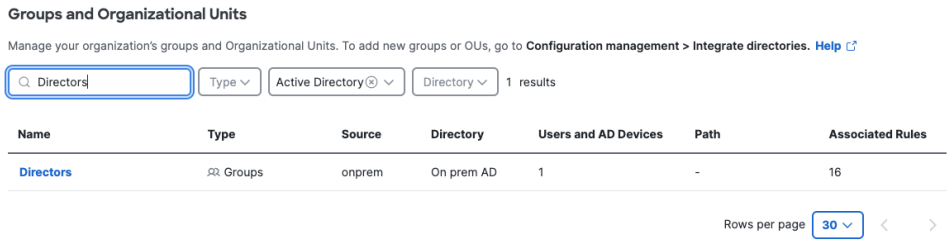
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, then click **Groups and Organizational Units**.

   Secure Access lists the provisioned groups and OUs.

   - **Name**–The name of the group or OU.
   - **Type**–Group or OU.
   - **Source**–The method or identity provider (IdP) that provisioned the group or OU.
   - **Directory**–The name of the IdP that provisioned the group or OU.
   - **Users and AD Devices**–The number of users in the group or OU.
   - **Path**–The path for the OU.
   - **Associated Rules**–The Access rules that include the group or OU.



2. Click on the name of a group to view the details about the group or OU.

Group Details

Describes Group Details in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Information about the user group.

- **Name**–The name of the group.
- **Identity Provider**–The source of the provisioned group.
- **Users**–The number of users in the group and the group label.
- **Devices**–The number of endpoint devices in the group and the group label.
- **Events**–Number of user or device connection events by connection status (Blocked or Allowed).
- **Associated Rules**–The number and names of access rules applied to users in the group.

Organizational Unit Details

Describes Organizational Unit Details in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Information about the OU.

- **Name**–The name of the OU.
- **Identity Provider**–The source of the provisioned OU.
- **Path**–The directory path of the OU.
- **Users**–The number, names, and email addresses of users in the OU.
- **Child OUs**–The number and names of child OUs of the OU.
- **Associated Rules**–The number and names of access rules applied to users in the OU.

View Details for Endpoint Devices

Provides instructions for completing the View Details for Endpoint Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

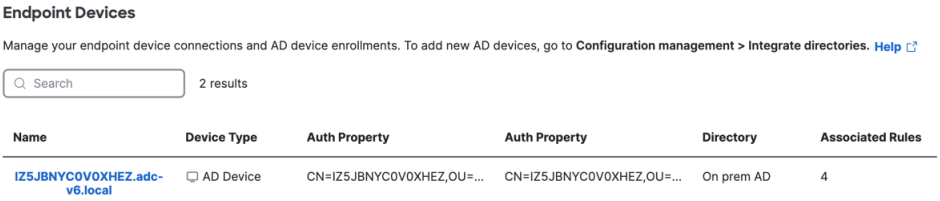
After an administrator provisions endpoint devices in Cisco Secure Access, you can view details about the devices including information about the access rules that apply to the endpoint devices.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.
- An Active Directory integration with Cisco AD Connector version 1.14.4 or newer. For more information, see Manage Active Directory Integration, Connect Active Directory to Secure Access, and Configure Updates on AD Connectors.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Endpoint Devices**. Secure Access lists the devices provisioned in the organization.
   - **Name**–The AD display name of the device.
   - **Device Type**–The type of identity provider (IdP) integration that provisioned the device. Secure Access supports the **AD Device** type only.
   - **Auth Property**–The value of the property used to authenticate the device in Secure Access.
   - **Directory**–The name of the Active Directory IdP.
   - **Associated Rules**–The number of access rules that apply to the device.
2. Navigate to an endpoint device.



View a Configured AD Device

Provides instructions for completing the View a Configured AD Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

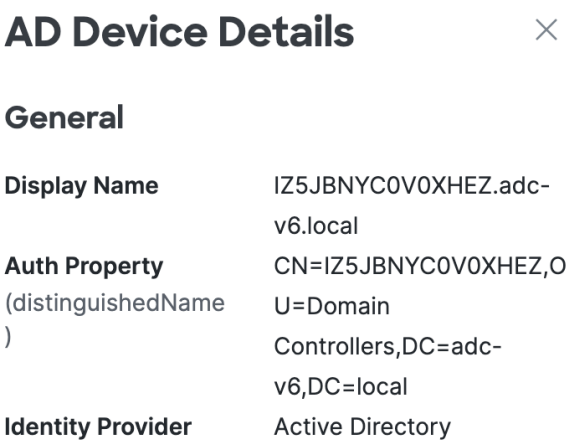
Click a device name to view the details about the device.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.
- An Active Directory integration with Cisco AD Connector version 1.14.4 or newer. For more information, see Manage Active Directory Integration, Connect Active Directory to Secure Access, and Configure Updates on AD Connector.

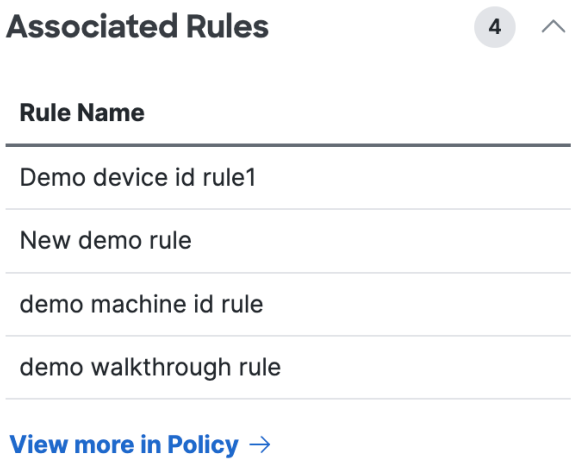
Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Endpoint Devices**.
2. Navigate to an endpoint device, and then click the name of the device.
   a) View the general properties for the endpoint device.
      - **Display Name**–The AD display name of the device.
      - **Auth Property**–The name and value of the property that Secure Access uses to authenticate the device.
      - **Identity Provider**–The name of the identity provider that manages the user device.



b) View the information about the access rules that apply to the endpoint device.

- The number of access rules that apply to the endpoint device.



- **Rule Name**–The name of the access rules that apply to the endpoint device.
  - Click **View more in Policy** to navigate to the Access Policy in Secure Access.

Export User Data to CSV

Describes how to apply filters on the Users page and export user data to a CSV file for troubleshooting and monitoring.

You can filter, view, and export User data into a .csv file for troubleshooting and monitoring purposes. The robust filtering and search capabilities on the **Users, Groups, and Endpoint Devices** page help you quickly narrow down and analyze significant security and network activities. You can use a combination of basic search box filters and advanced filter options to focus on specific events. Export the results for troubleshooting, record keeping, and more.

> **Note**
>
> You must use at least one filter and apply it to the table before you can export the information into a .csv.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**.
2. Click the **Users** tab.
3. Beside the search bar, click **Filters** and launch the pop-up window for selections. You have the following options in drop-down menus:
   - Directory – Select the directory type currently configured for your users.
   - Risk alert – Select the risk alert you want to filter on.
   - Trust level – Select the trust level you want to filter on.
   - (Optional) VPN Filters – Check this box to only show active VPN sessions. Note that using this option disables the other filter options listed above.
   - VPN profile - Select the VPN profile you want to filter on.
4. Filters are automatically applied. Once you have modified the filter selections, review the table. Click on the **Name** of an entry to examine the details of the user, such as devices and connectivity, device ID, OS version, VPN access information and more.
5. To export the table, click **Export CSV**.
6. Enter an **Exported Report Name**. This is what the file is saved as once it is exported locally.
7. Enter the **Results Row Limit** to limit the exported report to a certain number of rows. There is a maximum limit of 1,000,000 rows allowed per report; if you do not express a specific value for your report and the number of rows from your filter exceeds the max number, the report is truncated to 1,000,000 rows by default.
8. Click **Export**. Alternatively, click **Cancel** to not save the report.

Unenroll Devices for Client-Based Zero Trust Access

Provides instructions for completing the Unenroll Devices for Client-Based Zero Trust Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After a user enrolls their device for zero trust access on the Cisco Secure Client, the device appears in Secure Access. The user's device can create secure zero trust sessions and connect to their organization's private resources.

If you need to remove a user device that has zero trust access enabled from the organization, you can unenroll the user's device on Secure Access. The unenroll administrative action has these consequences:

- Prevents new zero trust connections from the device.
- The user device cannot create any new zero trust sessions to private resources.
- Invalidates the device's zero trust certificate.
- Blocks all current active zero trust access (ZTA) sessions associated with the enrollment.

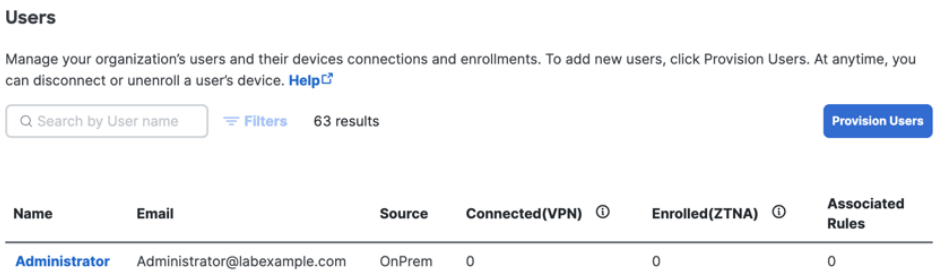
Unenroll user devices on Secure Access that have enabled zero trust access on the Secure Client.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A user device that has enrolled in zero trust access on the Cisco Secure Client.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**.
2. Click **Users** to view the users provisioned in the organization.
3. Click on the **Name** of a user that has configured **Enrolled (ZTNA)**.



4. For **User Details**, navigate to **Client-based ZTA**, and then click **Unenroll ZTNA**.
5. Click **Unenroll ZTNA**, and then confirm the removal of the user device.

Reenroll the User Device on the Secure Client

Describes Reenroll the User Device on the Secure Client in Cisco Secure Access. After you unenroll a device on Secure Access, the end user can reenroll their device to enable zero trust access from the Cisco Secure Client.

After you unenroll a device on Secure Access, the end user can reenroll their device to enable zero trust access from the Cisco Secure Client. For more information, see Invite Users to Enroll in Zero Trust Access for Secure Client.

Disconnect Remote Access VPN Sessions

Provides instructions for completing the Disconnect Remote Access VPN Sessions workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Disconnect users on Secure Access that have established remote access VPN sessions on the Secure Client.

After a user connects to your network on the Cisco Secure Client from a remote location, using a computer or other supported iOS or Android device connected to the Internet, the device appears on Secure Access.

You can disconnect a user's remote access VPN session from Secure Access. The disconnect administrative action has these consequences:

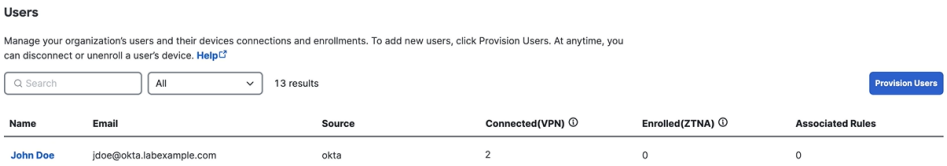
- Prevents new remote access VPN sessions from the device. The user device can not access private resources.
- Revokes the device's certificate.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A user device that has a remote access VPN connection on the Cisco Secure Client to your network from a remote location.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**.
2. Click **Users** to view the users provisioned in the organization.
3. Click on the **Name** of a user that has configured **Connected(VPN)**.



4. For **User Details**, navigate to **Device Connectivity**, and scroll through the device list to find the session you want to disconnect.
5. Under **VPN Access** click **Disconnect device**.
6. Click **Disconnect** to confirm the removal of the user device.

19 User Directories and Device Management

Topics:

- Manage User Directories and Device Management
- Configure User Directory Integrations
- Manage Cloud Identity Providers
- Manage API Keys for Provisioning Identities
- Manage Active Directory Integration
- Manage Google Workspace Account
- Manage Imported Users and Groups

Provides an overview of User Directories and Device Management in Cisco Secure Access, including Manage User Directories and Device Management, Configure User Directory Integrations, and Manage Cloud Identity Providers. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage User Directories and Device Management

Describes Manage User Directories and Device Management in Cisco Secure Access. Cisco Secure Access supports the provisioning of users, groups, and endpoint devices through integrations with identity providers (IdPs).

Cisco Secure Access supports the provisioning of users, groups, and endpoint devices through integrations with identity providers (IdPs). Once you provision, you can view the directories that were added in the organization. You can also modify or delete a directory integration.

About Configuring Multiple Cloud Provisioning IdPs

The integration of a user directory in Secure Access manages the provisioning of the organization's users and groups from the identity provider (IdP) to Secure Access. You can integrate multiple cloud IdPs with Secure Access. For more information, see Add a Cloud Identity Provider.

Configure User Directory Integrations

Add the user directory integrations for the organization and configure advance settings for the directories.

- Configure User Directory Integrations
- Manage Advanced Configuration Settings

Manage User Directory Integrations

After you add the user directory integrations for the organization, you can view, edit, or delete a user directory.

- Manage Cloud Identity Providers
- Manage Active Directory Integration
- Manage Google Workspace Integration
- Manage Imported Users and Groups

Configure Active Directory Endpoint Device Management

The Active Directory integration in Secure Access includes the option to provision endpoint devices from an on-premise Active Directory domain controller (DC). For more information, see Manage Active Directory Integration.

Configure User Directory Integrations

Provision users and groups in Secure Access by integrating a user directory.

To start provisioning users, groups, and endpoint devices into Cisco Secure Access, integrate a user directory with Secure access. A user directory represents an integration with an identity provider (IdP).

You can provision users and groups in Secure Access through a cloud identity provider (IdP), Active Directory (AD) integration, Google Workspace integration for Google Chromebook users, and a CSV file that includes the organization's users and groups information. You can provision endpoint devices through an Active Directory (AD) integration.

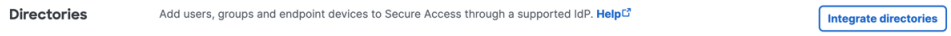
> **Note**
>
> You can add multiple user directory integrations for various cloud IdPs.

Before you begin

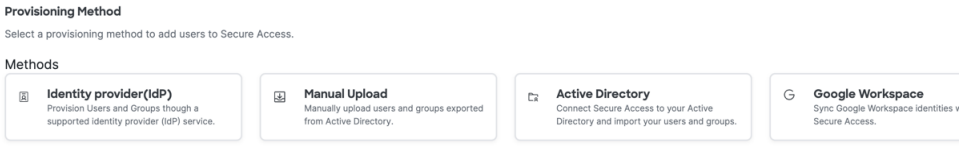
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
2. On the **Configurations** tab, click **Integrate directories**.



3. For **Provisioning Method**, select a user directory integration and complete the steps to provision users and groups for the organization.
   a) Click **Identity provider (IdP)**. Follow the steps to integrate a cloud IdP. For more information, see Add a Cloud Identity Provider.
   b) Click **Manual Upload**. Follow the steps to manually upload users and groups. For more information, see Import Users and Groups from CSV File.
   c) Click **Active Directory**. Follow the steps to integrate AD with Secure Access. For more information, see Provision Users and Groups from Active Directory.
   d) Click **Google Workspace**. Follow the steps to manage the Google Workspace user account for the users on Google Chromebooks in the organization. For more information, see Manage Google Workspace Account.



What to do next

- Manage User Authentication Profiles
- Manage Advanced User Configuration Settings
- Authenticate Active Directory Devices

View Directories

Provides instructions for completing the View Directories workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

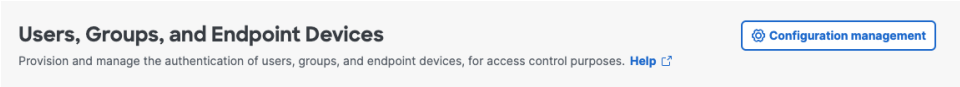
After you add user directory integrations in Secure Access, you can view the list of directories configured for the organization.

Before you begin

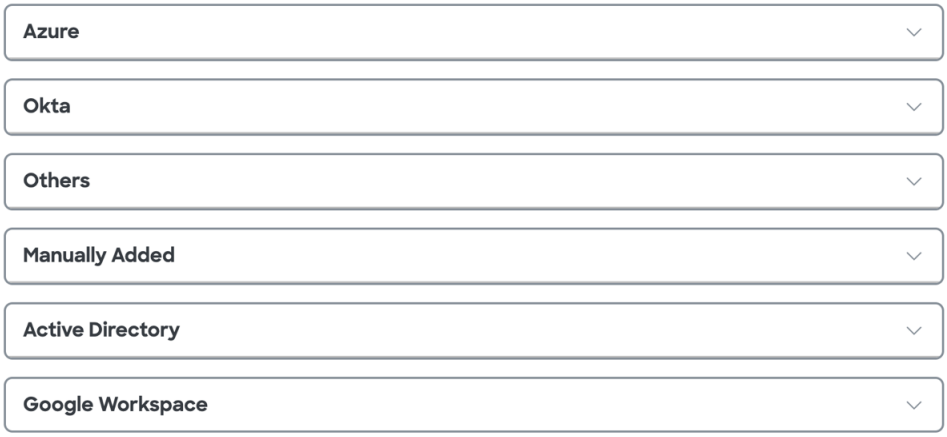
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.



2. On the **Configurations** tab, navigate to **Directories**, and then expand a user directory.



Manage Cloud Identity Providers

Describes Manage Cloud Identity Providers in Cisco Secure Access. Cisco Secure Access supports the provisioning of users and groups through integrations with identity providers (IdPs).

Cisco Secure Access supports the provisioning of users and groups through integrations with identity providers (IdPs). Once you provision users and groups, you can view, edit, or delete the configured user directory integration.

Add Identity Providers

- For more information, see Add a Cloud Identity Provider.

View Identity Providers

- For more information, see View Integrated Cloud Identity Providers.

Edit an Identity Provider Integration

- For more information, see Edit an Identity Provider Integration.

Delete an Identity Provider Integration

- For more information, see Delete an Identity Provider Integration.

Add a Cloud Identity Provider

Provides instructions for completing the Add a Cloud Identity Provider workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add an IdP integration in Secure Access and configure the provisioning of users and groups on the IdP.

Provide a label for the IdP integration, generate an SCIM token, and save the token to your local system.

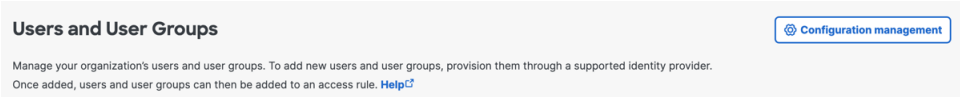
Copy and save the Secure Access Identity API URL, and then use the Secure Access SCIM token and URL to configure the integration with an IdP.

Before you begin

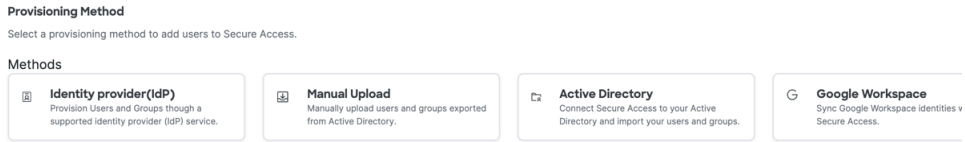
- Full Admin user role. For more information, see Manage Accounts.

Procedure

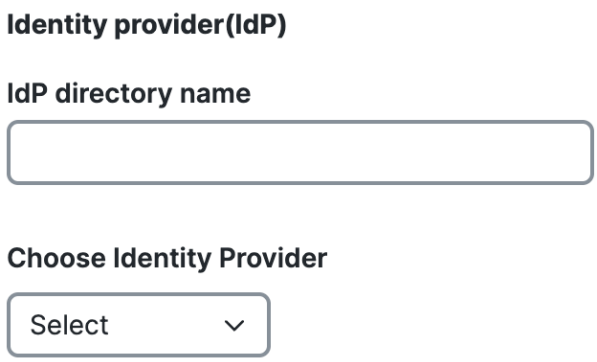
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



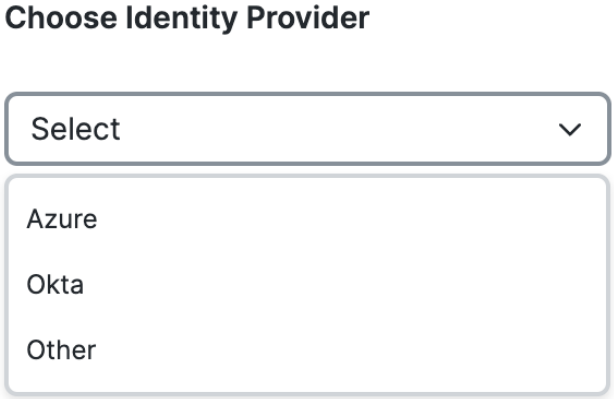
2. On the **Configurations** tab, click **Integrate directories**, and then click **Identity provider (IdP)**.



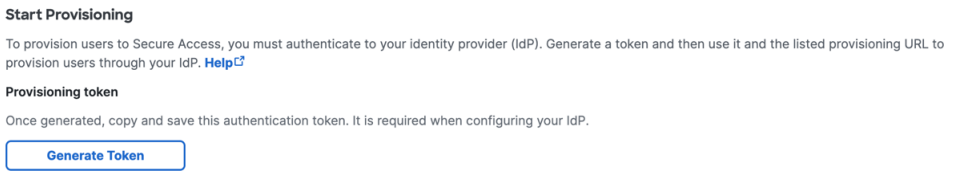
3. For **IdP directory name**, enter a descriptive label for the IdP integration.



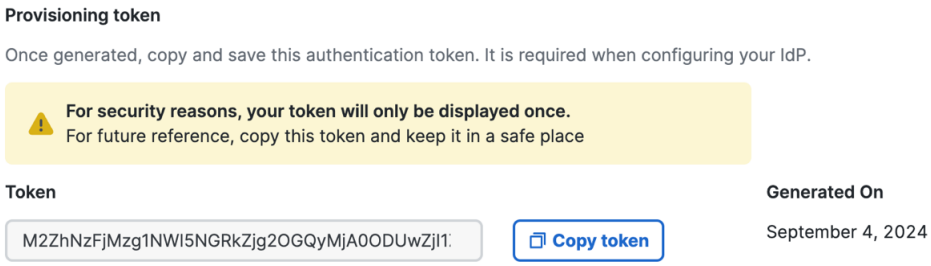
4. For **Choose Identity Provider**, select an IdP or **Other**, and then click **Next**.



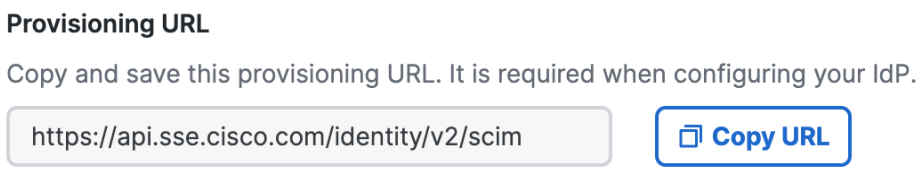
5. For **Provisioning Token**, click **Generate Token** to create the SCIM token for the integration with the IdP and Secure Access.



6. Click **Copy token**, and then save the SCIM token to your local system.



7. For **Provisioning URL**, click **Copy URL** to get the Secure Access identity provisioning URL. Save the URL to your local system.



8. For **Configure your IdP portal**, set up an IdP for the organization. For more information, see Configure Identity Providers.
9. Click **Done**.

What to do next

Configure a user authentication profile for users in the organization to use single sign-on (SSO) when connecting to web and private destinations. For more information, see Add User Authentication Profiles.

View an Integrated Cloud Provider

Provides instructions for completing the View an Integrated Cloud Provider workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a cloud IdP, view the settings on the configured user directory.

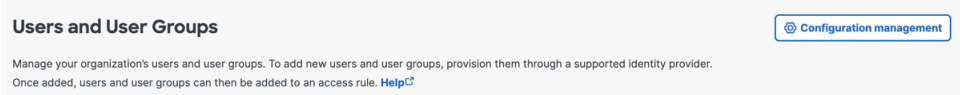
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

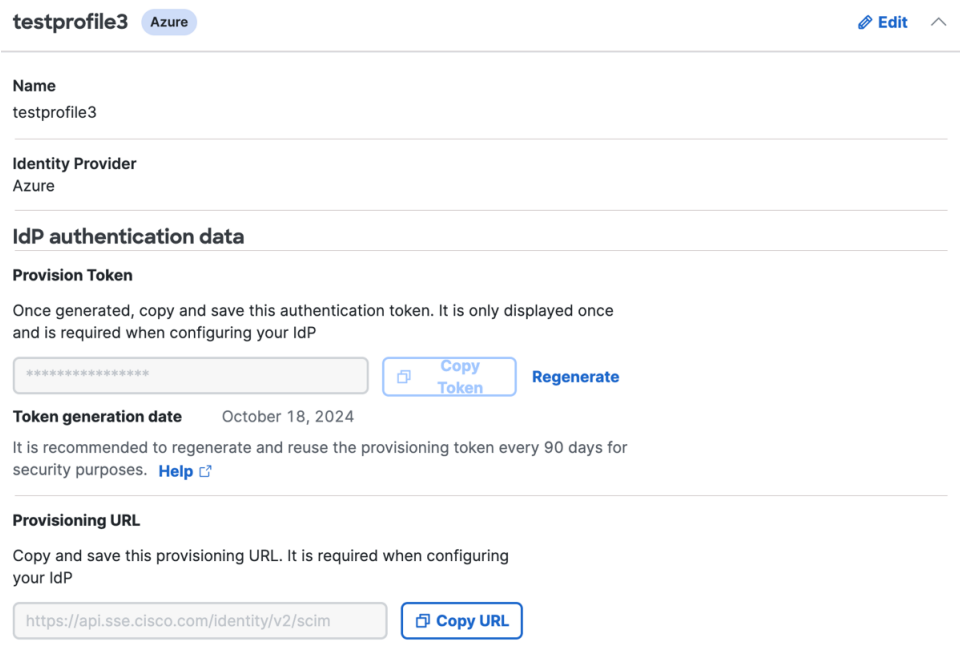
Procedure

---

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. On the **Configurations** tab, navigate to **Directories**, and then expand a user directory.
   - **Name**–The label for the user directory integration.
   - **Identity Provider**–The type of cloud identity provider that is integrated.
   - **Provision Token**–The SCIM token for the user directory integration.
   - **Token generation date**–The date when the provisioning token was created.
   - **Provisioning URL**–The URL of the Secure Access service provider.



Edit an Identity Provider Integration

Provides instructions for completing the Edit an Identity Provider Integration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access supports the provisioning of users and groups through integrations with identity providers (IdPs).

Once you provision an IdP integration, you can edit the configured settings on the integration. Secure Access supports the provisioning of multiple instances of various IdPs. For more information, see Manage User Directories.

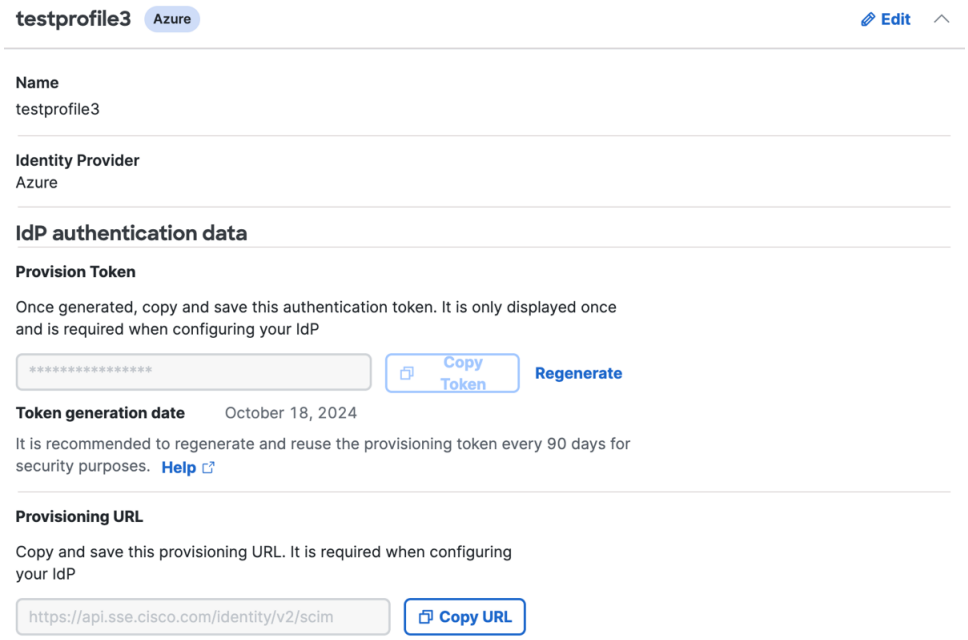
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. On the **Configurations** tab, navigate to **Directories**, and then expand a user directory. You can modify the name of the IdP integration and regenerate the SCIM token.

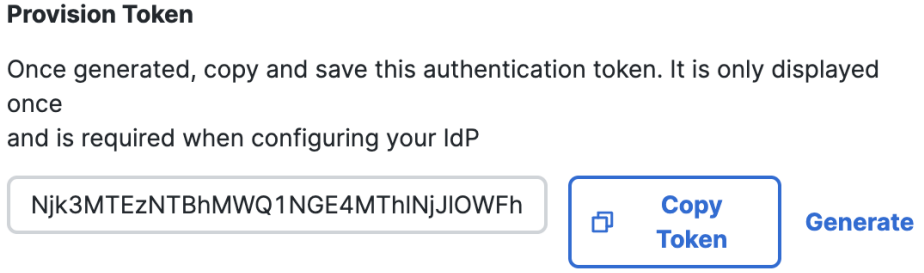
2. Click **Edit**.



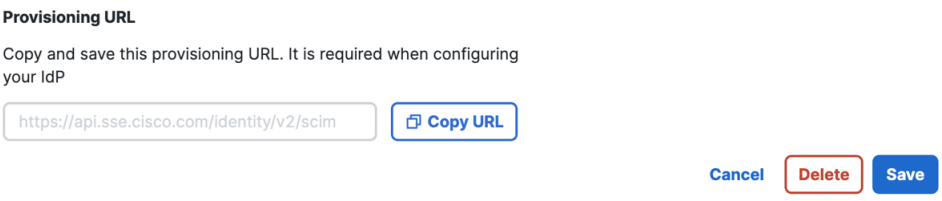
3. For **Name**, update the name of the IdP integration.



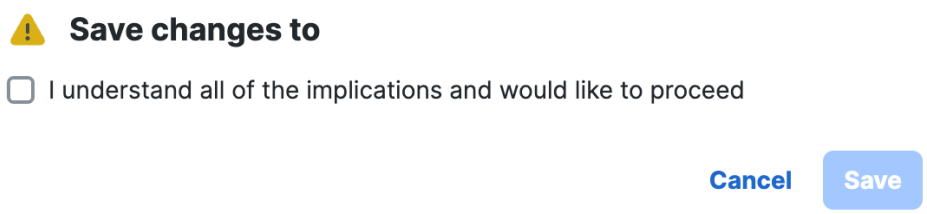
4. For **Provision Token**, you can generate the SCIM token for the IdP integration.



5. For **Provisioning URL**, copy the Secure Access provisioning URL.



6. Click **Save**, and then check **I understand all of the implications and would like to proceed**.



7. Click **Save**.

What to do next

Configure a user authentication profile for users in the organization to use single sign-on (SSO) when connecting to web and private destinations. For more information, see Add User Authentication Profiles.

Delete an Identity Provider Integration

Provides instructions for completing the Delete an Identity Provider Integration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access supports the provisioning of users and groups through integrations with identity providers (IdPs).

Once you integrate an IdP, you can remove the IdP in Secure Access and the provisioned users and groups. For more information, see Manage User Directories.

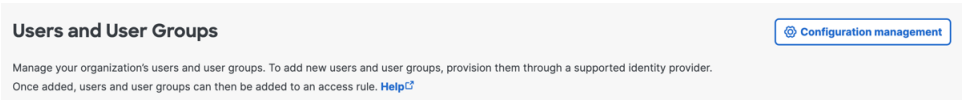
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

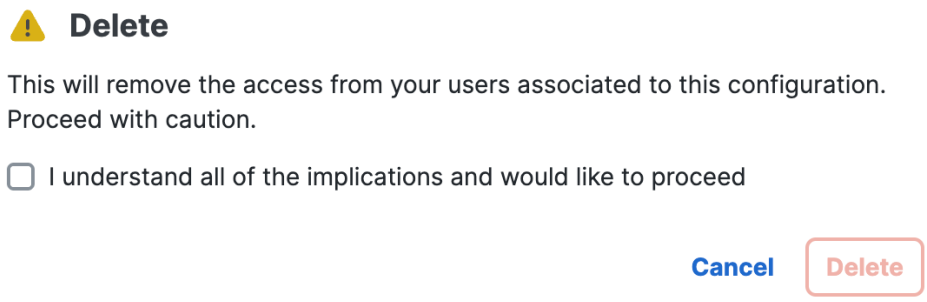
Procedure

---

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.



2. On the **Configurations** tab, navigate to **Directories**, and then expand a user directory.
3. Click **Edit**, and then click **Delete**.



4. Check **I understand all of the implications and would like to proceed**, and then click **Delete**.

Manage API Keys for Provisioning Identities

Describes Manage API Keys for Provisioning Identities in Cisco Secure Access. Cisco Secure Access supports the management of Microsoft Active Directory (AD) endpoint devices and Security Group Tags (SGTs) in Secure Access through the Cisco Secure Access Identities Registration API.

Cisco Secure Access supports the management of Microsoft Active Directory (AD) endpoint devices and Security Group Tags (SGTs) in Secure Access through the Cisco Secure Access Identities Registration API. For more information, see Cisco Secure Access Identities Registration API.

You can also provision users, groups, and endpoint devices by uploading AD identities in comma-separated values (CSV) files. For information about uploading CSV files to Secure Access, see Import Users and Groups from CSV File and Manage Machine Tunnels.

- Add the API Key for Managing Identities
- Refresh the API Key for Managing Identities
- Delete API Keys
- View Details About Provisioned API Keys
- View Details for Identities Provisioned with the API
- View Endpoint Devices
- Verify Context Sharing in Secure Access

Guidelines

Describes Guidelines in Cisco Secure Access. For general information about adding, refreshing, or removing Secure Access API keys, see Manage API Keys.

- For general information about adding, refreshing, or removing Secure Access API keys, see Manage API Keys.
- Generate an API key for provisioning endpoint devices and Security Group Tags (SGTs) in Secure Access on **Connect > Users, Groups, and Endpoint Devices > Integrate Directories**. Secure Access generates the API key with these attributes:
  - The **Deployments / Identities** key scope and **Read / Write** permissions.
    - You can add more API keys in Secure Access to manage the endpoint devices in the organization. Create and manage API keys on the **Admin > API Keys** page.
  - A default expiry date of 90 days. You can modify the API key's expiry date at any time.
  - A default key name of **API Provisioning Key**.
- Secure Access only displays the active endpoint devices in the organization. For more information, see View Endpoint Device Details.
- Use the Cisco Secure Access Identity Endpoints API to update an endpoint device in Secure Access. For more information, see Cisco Secure Access Identities Registration API.

Add the API Key for Managing Identities

Provides instructions for completing the Add the API Key for Managing Identities workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add an API key in Secure Access to manage the endpoint devices and Security Group Tags (SGTs) for the organization.

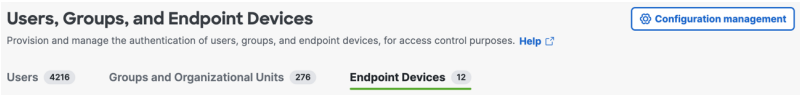
> **Note**
>
> You can add API keys with the **Deployments / Identities** key scope on the **Admin > API Keys** page in Secure Access.

Before you begin

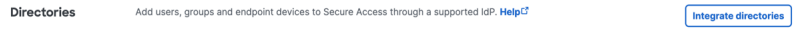
- Full Admin user role. For more information, see Manage Accounts.

Procedure

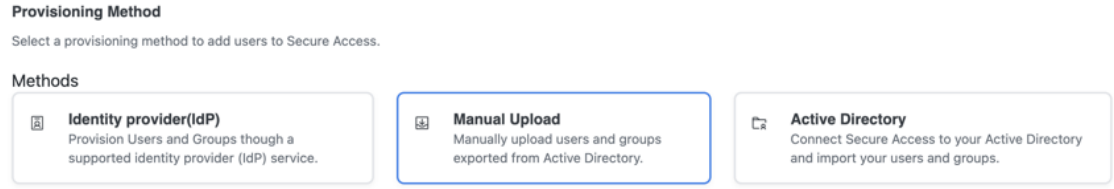
1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.



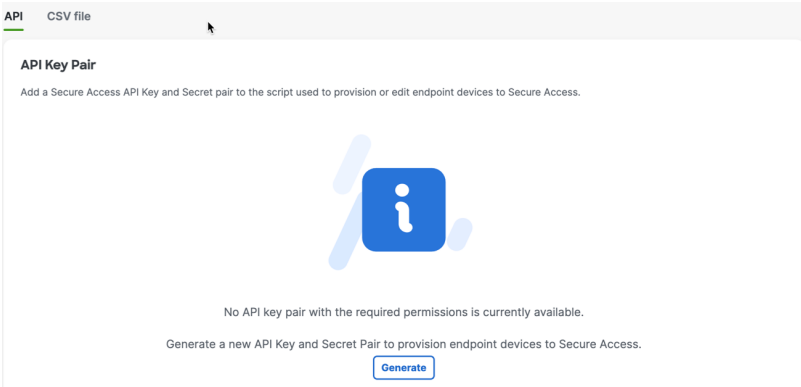
2. On the **Configurations** tab, click **Integrate directories**.



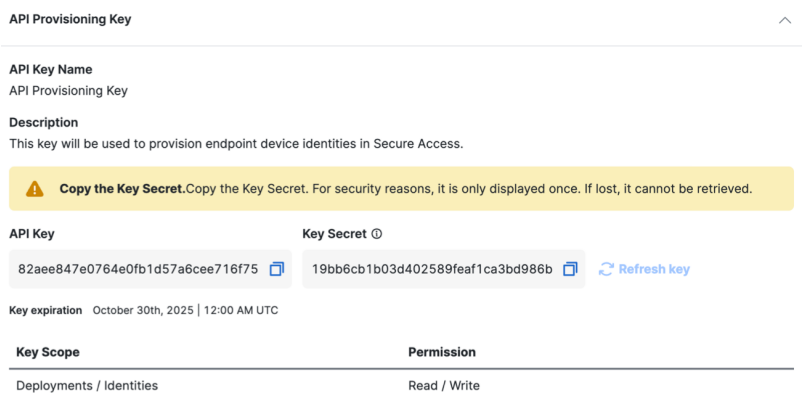
3. For **Provisioning Method**, click **Manual Upload**, and then click **Next**.



4. On **Integrate Directories**, click the **API** tab.



5. Click **Generate** to add an API key and secret.



6. Copy the value of **API Key** and the value of **Key Secret** to your local environment.
7. Click **Done**.

Refresh the API Key for Managing Identities

Provides instructions for completing the Refresh the API Key for Managing Identities workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Refresh the API key used to manage the endpoint devices and Security Group Tags (SGTs) in Secure Access.

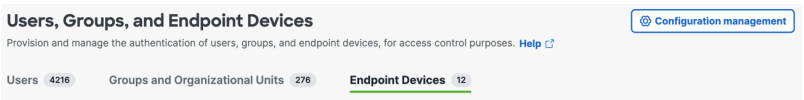
> **Note**
>
> You can refresh any API keys that you added in the organization on the **Admin > API Keys** page in Secure Access.

Before you begin

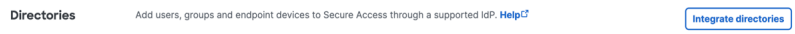
- Full Admin user role. For more information, see Manage Accounts.

Procedure

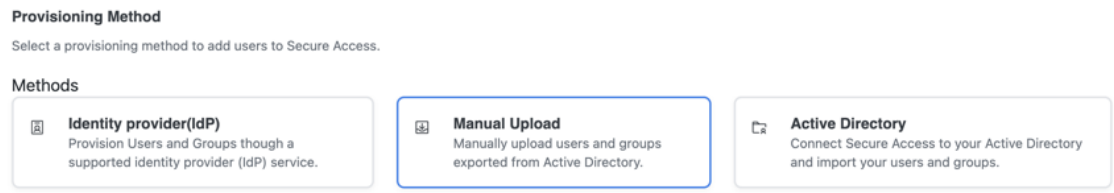
1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.



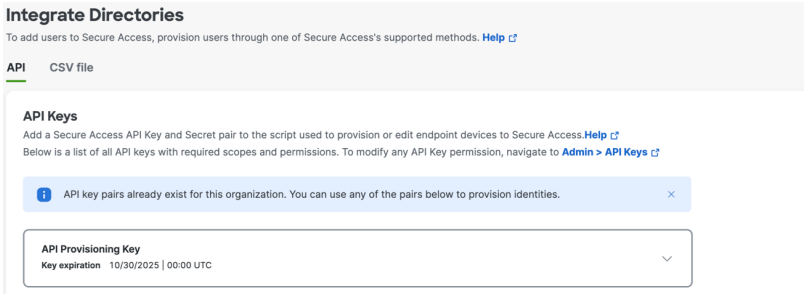
2. On the **Configurations** tab, click **Integrate directories**.



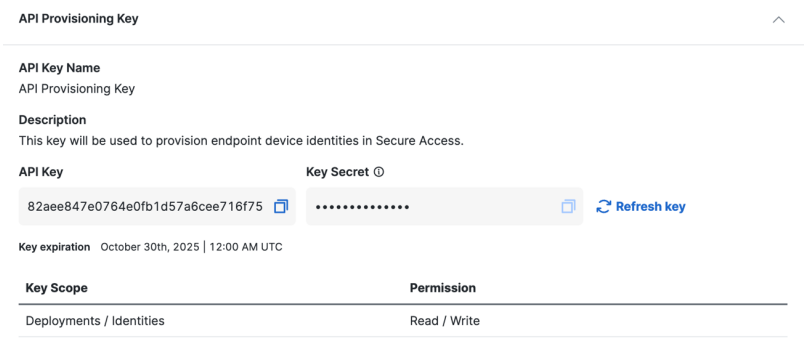
3. For **Provisioning Method**, click **Manual Upload**, and then click **Next**.



4. On **Integrate Directories**, click the **API** tab.



5. Expand an API key, and then click **Refresh key**.



6. Copy the value of **API Key** and the value of **Key Secret** to your local environment.
7. Click **Done**.

Delete API Keys

Describes Delete API Keys in Cisco Secure Access. To remove the API keys that you added in Secure Access, navigate to Admin > API Keys and delete the keys.

To remove the API keys that you added in Secure Access, navigate to **Admin > API Keys** and delete the keys. For more information, see Manage API Keys.

View Details About Provisioned API Keys

Provides instructions for completing the View Details About Provisioned API Keys workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

> **Note**
>
> You can view all API keys added in the organization on the **Admin > API Keys** page in Secure Access. For more information, see Manage API Keys.

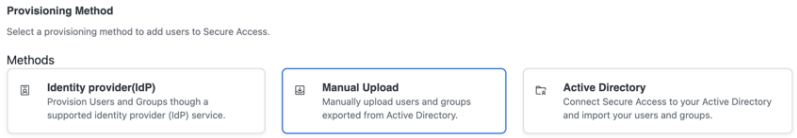
Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

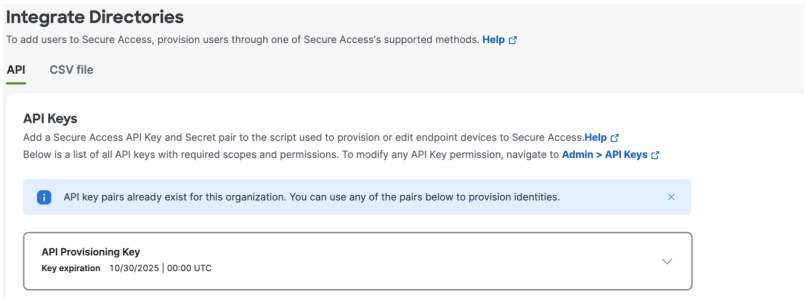
Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

2. On the **Configurations** tab, click **Integrate directories**.
3. For **Provisioning Method**, click **Manual Upload**, and then click **Next**.



4. Navigate to **Integrate Directories**, and then click on the **API** tab.



5. Secure Access displays the list of API keys in the organization configured with the **Deployments/identities** key scope and **Read/Write** key permissions.
6. Expand an API key to view the key details.

View Details for Identities Provisioned with the API

Provides instructions for completing the View Details for Identities Provisioned with the API workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

> **Note**
>
> Secure Access only displays the **API Provisioned** component if the organization provisioned an API key for managing the endpoint devices and Security Group Tags (SGTs).

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
2. On the **Configurations** tab, navigate to **Directories**, and then expand the **API Provisioned** component.

   Secure Access displays the number of identities that the organization provisioned with the Cisco Secure Access Identities Registration API.



View Endpoint Devices

Provides instructions for completing the View Endpoint Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

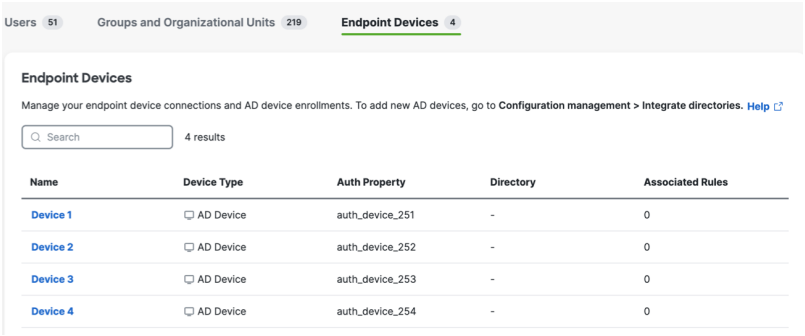
You can view the details about the endpoint devices in Secure Access. For more information, see View Endpoint Device Details.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click on the **Endpoint Devices** tab.



Manage Active Directory Integration

Manage the Active Directory integration for the organization.

Cisco Secure Access supports the provisioning of users and endpoint devices from Active Directory (AD) into Secure Access. Once you provision users and endpoint devices from AD, you can manage the organization's AD user or device directory in Secure Access.

For more information about provisioning of users and groups, see Provision Users, Groups, and Endpoint Devices from Active Directory.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Endpoint device management requires devices provisioned by an on-premise Active Directory domain controller (DC) and Cisco AD Connector version 1.14.4 or newer.

- For more information, see Connect Active Directory to Secure Access, and Configure Updates on AD Connectors.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and click **Configuration management**.
2. On the **Configurations** tab, navigate to **Directories**, and then expand **Active Directory**.

Download the Active Directory Components

Provides instructions for completing the Download the Active Directory Components workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Endpoint device management requires devices provisioned by an on-premise Active Directory domain controller (DC) and Cisco AD Connector version 1.14.4 or newer.
- For more information, see Manage Active Directory Integration, Connect Active Directory to Secure Access, and Configure Updates on AD Connectors.

Procedure

1. For **Active Directory Connector**, click **Download**.
2. For **Windows Configuration Script for Domain Controller**, click **Download**.

Edit the Active Directory Connector Auto-Upgrades

Describes Edit the Active Directory Connector Auto-Upgrades in Cisco Secure Access. For more information, see Configure Updates on AD Connectors.

- For more information, see Configure Updates on AD Connectors.

Edit Authentication Properties for the AD Integration

Describes Edit Authentication Properties for the AD Integration in Cisco Secure Access. For more information, see Edit AD Authentication Properties.

- For more information, see Edit AD Authentication Properties.

Enable DLP Email Notifications for Reporting Managers

Describes Enable DLP Email Notifications for Reporting Managers in Cisco Secure Access. For more information, see Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications.

- For more information, see Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications.

View Active Directory Components

Describes View Active Directory Components in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- For more information, see View AD Components in Secure Access.

Manage Sites for AD Components

Describes Manage Sites for AD Components in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- For more information, see Manage Sites for AD Components.

Delete Active Directory Integration

Describes Delete Active Directory Integration in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- For more information, see Delete AD Components.

Manage Google Workspace Account

Manage the Google Workspace Super Admin account for the organization.

Cisco Secure Access supports the provisioning of users on Google Chromebooks from Google Workspace into Secure Access. You can integrate the Google Workspace Identity Service with Secure Access and manage the identities in Organization Units (OUs). For more information, see Integrate the Google Workspace Identity Service.

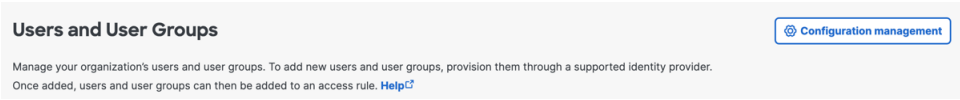
Once you provision users in OUs, you can manage the Google Workspace account in Secure Access and view the provisioned users and groups.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

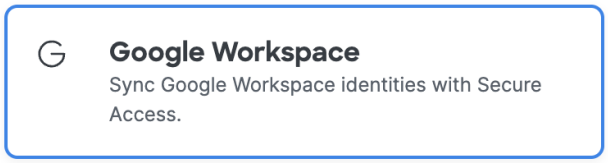
Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.

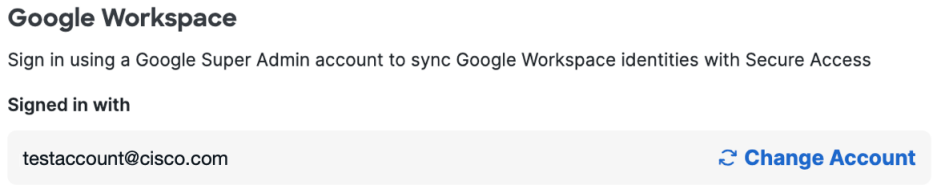


> **Note**
>
> These users and groups are currently intended exclusively for Chromebook (DNS/SWG) identification. The users cannot be utilized for other purposes, such as SAML authentication.

2. On the **Configurations** tab, navigate to **Directories**, and then expand **Google Workspace**.
3. Click **Google Workspace**, and then click **Next**.



4. Click **Change Account**, and then follow the steps to choose a new Google Workspace account through the Cisco User Management app.



5. Click **Done**.

Manage Imported Users and Groups

Describes Manage Imported Users and Groups in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Cisco Secure Access supports manually provisioning users and groups. Upload an CSV file in Secure Access with the organization's users and groups. For more information, see Import Users and Groups from CSV File.

Once you provision users and groups, you can delete the imported CSV file and upload a new CSV file with the users and groups in the organization.

Import Users and Groups from CSV File

Import users into Secure Access from a comma-separated values (CSV) file.

Cisco Secure Access supports provisioning users and groups manually from a comma-separated values (CSV) file. Export your Microsoft Active Directory (AD) users and groups to a CSV file. We recommend using `CSVDE.EXE` from a domain controller.

For each upload, the CSV file can have up to 4000 rows. An import may require ten minutes. Each subsequent CSV file upload replaces the contents of the previous upload. For large numbers of users and groups, we recommend using AD provisioning.

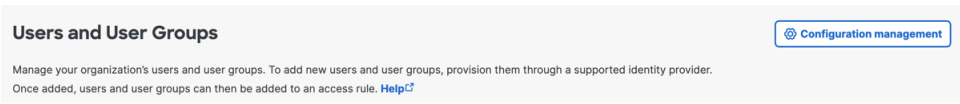
> **Note**
>
> To switch from AD provisioning to CSV import, you must uninstall your Secure Access AD Connectors and delete the AD Connectors in Secure Access. For more information, see Provision Users and Groups from Active Directory.

Before you begin

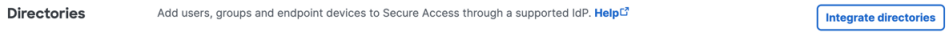
- Full Admin user role. For more information, see Manage Accounts.

Procedure

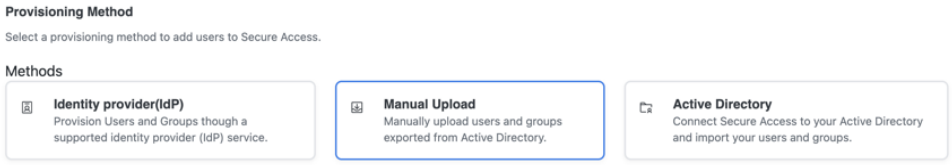
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. On the **Configurations** tab, click **Integrate directories**.

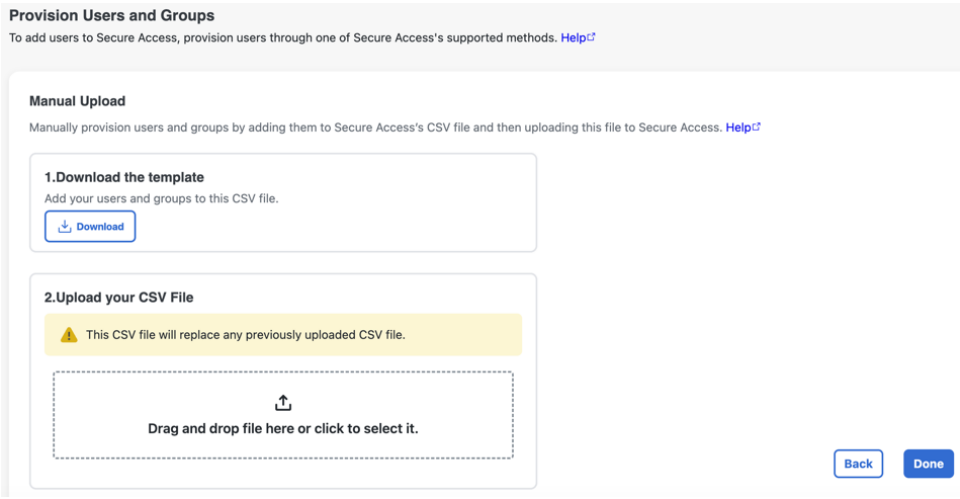


3. For **Provisioning Method**, click **Manual Upload** to provision users or groups in your organization.



4. Click **Download** to save the Secure Access import template to your local system. The template is a CSV file that supports the following format:
5. Add users or groups to the Secure Access CSV template file, and then upload the CSV file to Secure Access. For example:

```
DN,sn,givenName,userPrincipalName,mail,memberOf
last_name1,first_name1,emp20@cisco.com,emp20@cisco.com,adminGroup
last_name2,first_name2,emp2@cisco322.onmicrosoft.com,emp2@cisco322.onmicrosoft.com,adminGroup
last_name3,first_name3,user5@vvaidya.com,user5@vvaidya.com,adminGroup
last_name4,first_name4,employee1@company.com,employee1@company.com,adminGroup
last_name5,first_name5,demouser@company.com,demouser@company.com,adminGroup
```



6. Click **Done**.

CSV File Format

Describes CSV File Format in Cisco Secure Access. The CSV file must include the users and groups information in a comma delimited format.

The CSV file must include the users and groups information in a comma delimited format.

Header row:

```
DN,sn,givenName,userPrincipalName,mail,memberOf
```

Object row:

```
"CN=SMUser,CN=Users,DC=mycompany,DC=local",last_name1,first_name1,smuser@mycompany.com,smuser@mycompany.com,"CN=Group2,CN=Users,DC=mycompany,DC=com"
```

The following characters are not supported:

```
%<([{\\^-=$!|]})?*+>
```

CSV File Fields

Describes CSV File Fields in Cisco Secure Access. A user may belong to multiple groups, which are defined in the memberOf attribute.

Field	Required	Notes	Supported Number of Characters
DN	**No**	"CN=SAMLuser,CN=Users,DC=mycompany,DC=local"	64
sn	**Yes**	The user's surname (family name or last name).	64
givenName	**Yes**	The user's given name (legal first name).	64
userPrincipalName	**Yes**	The `userPrincipalName` corresponds to the principal that Secure Access receives in the SAML assertion, and is often identical to the object's mail attribute. However, this is not always the case. The `userPrincipalName` is constant, but the mail attribute may change. Example: samluser@mycompany.com	64
mail	**Yes**	Only valid email addresses. Example: samluser@mycompany.com	256
memberOf	**No**	"CN=Group2,CN=Users,DC=mycompany,DC=local"	1024

A user may belong to multiple groups, which are defined in the `memberOf` attribute.

An example value of the `memberOf` field:

```
"CN=Group1,CN=Users,DC=dcloud,DC=local;CN=Group2,CN=Users,
DC=dcloud,DC=local;CN=Group3,CN=Users,DC=dcloud,DC=local;
CN=Group4,CN=Users,DC=dcloud,DC=local"
```

View Provisioned Users and Groups in Secure Access

Provides instructions for completing the View Provisioned Users and Groups in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

Navigate to **Connect > Users, Groups, and Endpoint Devices** to view the users and groups provisioned in your organization.

- For more information, see View Users Provisioned in Secure Access.
- For more information, see View Group Details.

Upload a New CSV File with Users and Groups

Provides instructions for completing the Upload a New CSV File with Users and Groups workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

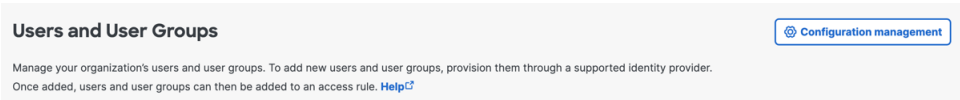
Upload a new CSV file in Secure Access. The new CSV file replaces the previously provisioned users and groups in the organization.

Before you begin

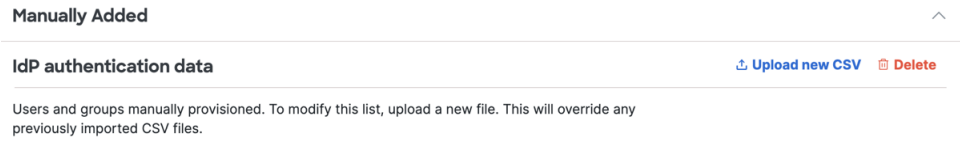
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. On the **Configurations** tab, navigate to **Directories**, and then expand the **Manually Added** user directory.
3. Click **Upload new CSV**, and then upload a CSV file that contains users and groups in your organization.



Delete an Imported CSV File

Provides instructions for completing the Delete an Imported CSV File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

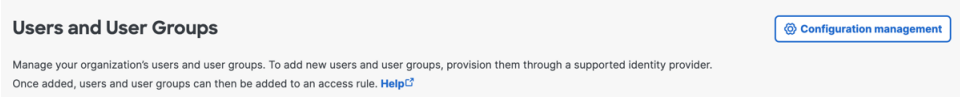
Remove an imported CSV file in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. Click the **Configurations** tab, navigate to **Directories**, and then expand the **Manually Added** user directory.
3. Click **Delete**, and then remove the CSV file that contains the provisioned users and groups in your organization.

---

20 Advanced User Configuration Settings

Topics:

- Manage Advanced Configuration Settings
- Manage IP Surrogates for User Authentication
- Manage Behaviour Analytics Configuration

Provides an overview of Advanced User Configuration Settings in Cisco Secure Access, including Manage Advanced Configuration Settings, Manage IP Surrogates for User Authentication, and Manage Behaviour Analytics Configuration. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Advanced Configuration Settings

Describes Manage Advanced Configuration Settings in Cisco Secure Access. Cisco Secure Access provides the option to configure advanced settings for the cloud identity provider (IdP) integrations, user authentication profiles, and Cisco AD Connectors and Virtual Appliances (VAs).

Cisco Secure Access provides the option to configure advanced settings for the cloud identity provider (IdP) integrations, user authentication profiles, and Cisco AD Connectors and Virtual Appliances (VAs).

- For cloud IdPs, enable the authName option in Secure Access. Then, configure the authName attribute on the IdP. For more information, see Provision Users and Groups in Okta or Provision Users and Groups from Microsoft Entra ID.
- For user authentication profiles, configure IP Surrogates for single sign-on (SSO) authentication providers.
- For the Cisco AD Connectors and Virtual Appliances, configure authentication of API requests for these components.

Set Up Authentication Preferences for Identity Providers

Provides instructions for completing the Set Up Authentication Preferences for Identity Providers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

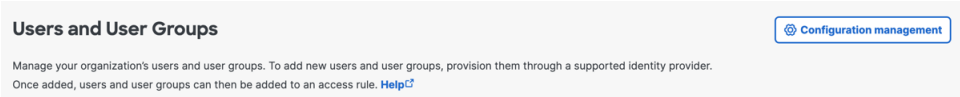
Enable the option to use the **User Principal Name** and **Authentication Name** for the cloud Identity Providers (IdPs) that you integrate with Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

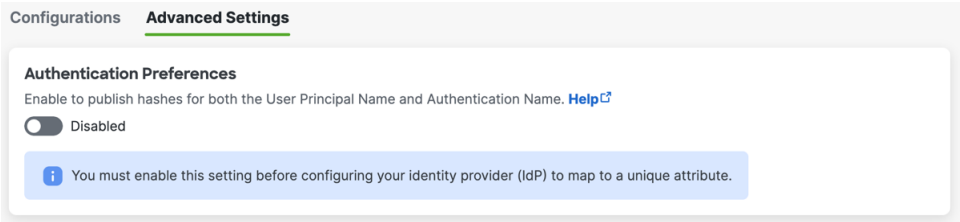
Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. Click the **Advanced Settings** tab, and then navigate to **Authentication Preferences > Public Hashes**
3. Click the toggle to enable the authName attribute.

   You can use the authName attribute to authenticate users in addition to the UPN attribute. The UPN attribute is the primary attribute and is always used to authenticate users.



Set Up IP Surrogates for SSO User Authentication

Describes Set Up IP Surrogates for SSO User Authentication in Cisco Secure Access. Enable IP surrogates for the SSO user authentication providers that you integrate with Secure Access.

Enable IP surrogates for the SSO user authentication providers that you integrate with Secure Access. For more information, see Manage IP Surrogates for SSO Authentication.

Set Up API Authentication

Describes Set Up API Authentication in Cisco Secure Access. Configure authentication for the integrations of the Cisco Active Directory (AD) Connectors and Secure Access Virtual Appliances (VAs) in the organization's environment.

Configure authentication for the integrations of the Cisco Active Directory (AD) Connectors and Secure Access Virtual Appliances (VAs) in the organization's environment. For more information, see Configure Authentication for AD Connectors and VAs.

Manage IP Surrogates for User Authentication

Describes Manage IP Surrogates for User Authentication in Cisco Secure Access. The Cisco Secure Access Secure Web Gateway (SWG) uses a cookie surrogate for Security Assertion Markup Language (SAML) authentication.

The Cisco Secure Access Secure Web Gateway (SWG) uses a cookie surrogate for Security Assertion Markup Language (SAML) authentication. Secure Access checks if a cookie is set in the HTTPS request. If the cookie surrogate is not set in the HTTP header, then Secure Access can not authenticate the user's connections to secure internet destinations.

We recommend using IP surrogates when the user's private IP address is visible, when your network tunnels don't use NAT, or when your networks incorporate a Proxy Chain with the X-Forwarded-For (XFF) request header. If the user's private IP address or an IP address is shared by multiple users, then we recommend using cookie surrogates. You can bypass IP surrogates for the internal networks that you add to an SSO authentication identity provider (IdP) integration.

How HTTPS Inspection Works

Describes How HTTPS Inspection Works in Cisco Secure Access. Before redirecting a web request to an IdP, Secure Access uses HTTPS inspection to determine if a request is from a browser that supports cookies.

Before redirecting a web request to an IdP, Secure Access uses HTTPS inspection to determine if a request is from a browser that supports cookies. Secure Access can establish the identity of a user through the browser cookies and map the user to an IP address. For subsequent requests, Secure Access uses the IP address as a surrogate for the user. Secure Access periodically inspects the cookies in a browser request to ensure the user is mapped to the correct IP address.

Secure Access checks to determine if an IP address has been reassigned; only requests from browsers are checked. This check is affected when browsing in incognito mode or deleting cookies from a browsing session and will require the user to re-authenticate. If the user has not browsed for over 12 hours since the last identity check, the IP is discarded from user to IP mapping until the user re-authenticates. After this, the policy will match either a tunnel or network identity.

Note: When Active Directory IdP users authenticate with a browser installed on a dual stack IPv4/IPv6 device, the IP Surrogates feature will not automatically map both addresses to the user. The user must authenticate twice to map both the IPv4 address and the IPv6 address as user surrogates. Re-authentication will also be enforced separately.

Enable IP Surrogates for User Authentication

Provides instructions for completing the Enable IP Surrogates for User Authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can add internal networks for your integrated SSO authentication IdP that connect on Registered Networks or Network Tunnels through the Secure Access Secure Web Gateway.

The connections on the internal networks bypass the SAML IP surrogate authentication challenge and revert to SAML with cookie surrogates. You should bypass IP surrogates for internal networks from IP surrogates where the IP address is shared by a number of users, such as a virtual desktop deployment. In these cases, where an IP address is shared, we recommend cookie surrogates because they associate the user's browser session to the identity. Internal networks must be defined for the IP address before you can add it to the IP surrogate bypass list.

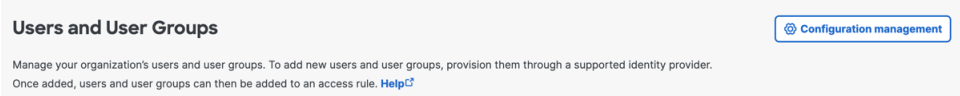
Add an Internal Network to the IP Surrogate for Registered Networks and Network Tunnels in Network Tunnel Groups where the internal IP address is not visible or is shared by multiple users. Once added, the internal networks will bypass the SAML IP surrogate authentication challenge.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- At least one configured user authentication IdP integration. For more information, see Add User Authentication Profiles.
- Internal private IP addresses are visible. IP surrogate needs to be able to see the internal private IPs.
- Proxy networks with XFF or network tunnels without NAT.
- In Secure Access, enable HTTPS inspection.
- Do not delete cookies at the end of a browser session, or browse in incognito mode.

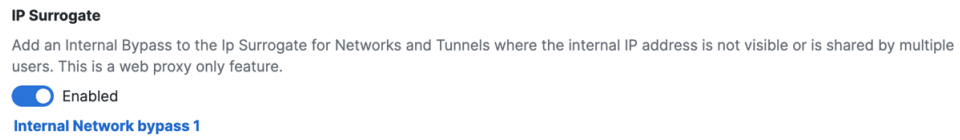
Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. On the **Advanced Settings** tab, toggle on **IP Surrogate**.

   The **Internal Network bypass** option appears.



Add Internal Networks for Bypass

Provides instructions for completing the Add Internal Networks for Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

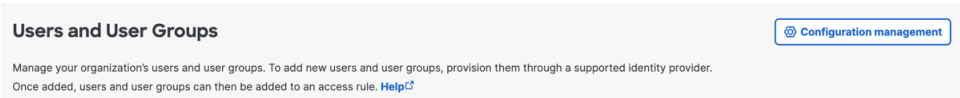
After you enable **IP Surrogate**, add internal networks. The user connections on internal networks bypass the SAML IP surrogate authentication challenge for traffic to the Secure Access Secure Web Gateway.

Before you begin

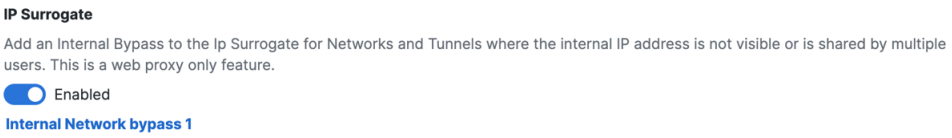
- Full Admin user role. For more information, see Manage Accounts.
- At least one configured user authentication IdP integration. For more information, see Add User Authentication Profiles.
- Internal private IP addresses are visible. IP surrogate needs to be able to see the internal private IPs.
- Proxy networks with XFF or network tunnels without NAT.
- In Secure Access, enable HTTPS inspection.
- Do not delete cookies at the end of a browser session, or browse in incognito mode.

Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.

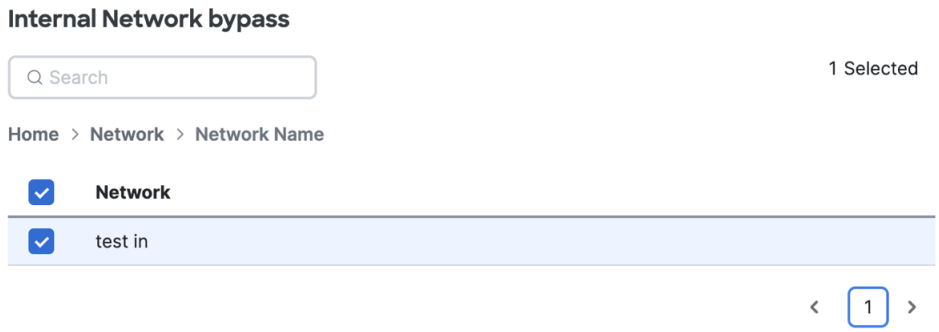


2. On the **Advanced Settings** tab, navigate to **IP Surrogate**.
3. Confirm that you enabled **IP Surrogate**.

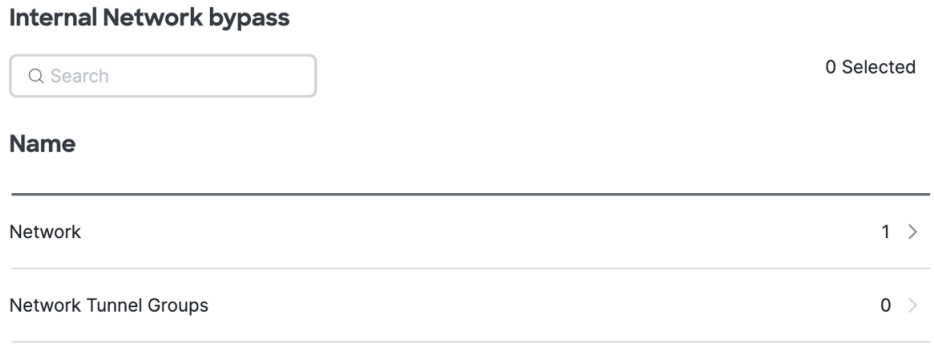


4. Click **Internal Network bypass**.

   Select the internal networks that are associated with Registered Networks and Network Tunnels in Network Tunnel Groups.
5. Expand **Network**.
   a) Expand a specific Network, and then select the internal networks for the Registered Networks.
   b) Click **Apply**.



6. Expand **Network Tunnel Groups**.
   a) Expand a specific Network Tunnel Group, and then select the internal networks for the Network Tunnels in the Network Tunnel Groups.
   b) Click **Apply**.



Delete Internal Networks for Bypass

Provides instructions for completing the Delete Internal Networks for Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

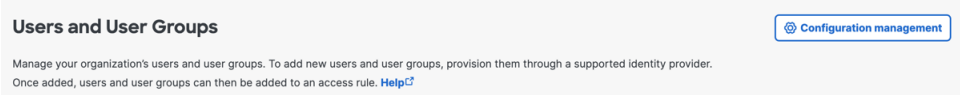
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- At least one configured user authentication IdP integration. For more information, see Add User Authentication Profiles.
- Internal private IP addresses are visible. IP surrogate needs to be able to see the internal private IPs.

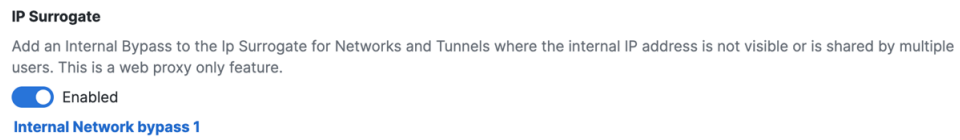
- Proxy networks with XFF or network tunnels without NAT.
- In Secure Access, enable HTTPS inspection.
- Do not delete cookies at the end of a browser session, or browse in incognito mode.

Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.

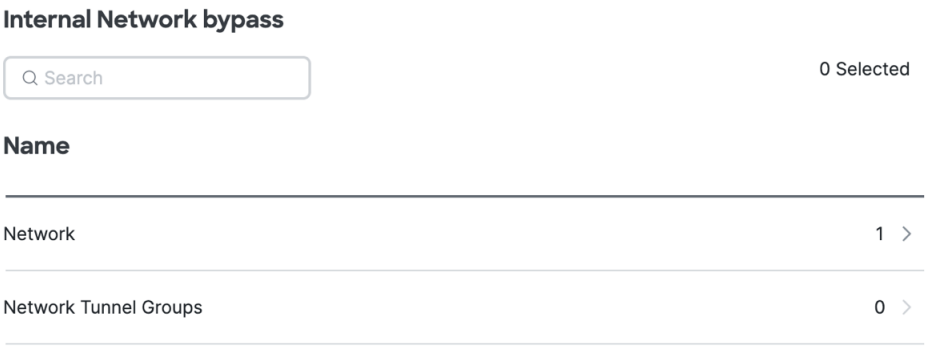


2. On the **Advanced Settings** tab, navigate to **IP Surrogate**.
3. Confirm that you enabled **IP Surrogate**.



4. Click **Internal Network bypass**.

   Select the internal networks that are associated with Registered Networks and Network Tunnels in Network Tunnel Groups.
5. Expand **Network**.
   a) Expand a specific Network, and then remove the internal networks for the Registered Networks.
   b) Click **Apply**.
6. Expand **Network Tunnel Groups**.
   a) Expand a specific Network Tunnel Group, and then remove the internal networks for the Network Tunnels in the Network Tunnel Groups.
   b) Click **Apply**.



Manage Behaviour Analytics Configuration

Describes Manage Behaviour Analytics Configuration in Cisco Secure Access. You can configure User and Entity Behavior Analytics (UEBA) detections for anomalous user activity in Cisco Secure Access.

You can configure User and Entity Behavior Analytics (UEBA) detections for anomalous user activity in Cisco Secure Access. Use behavior analytics to identify activity that differs from a user's established patterns or from thresholds that you configure.

To view the configuration, go to: **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour Analytics**

Note

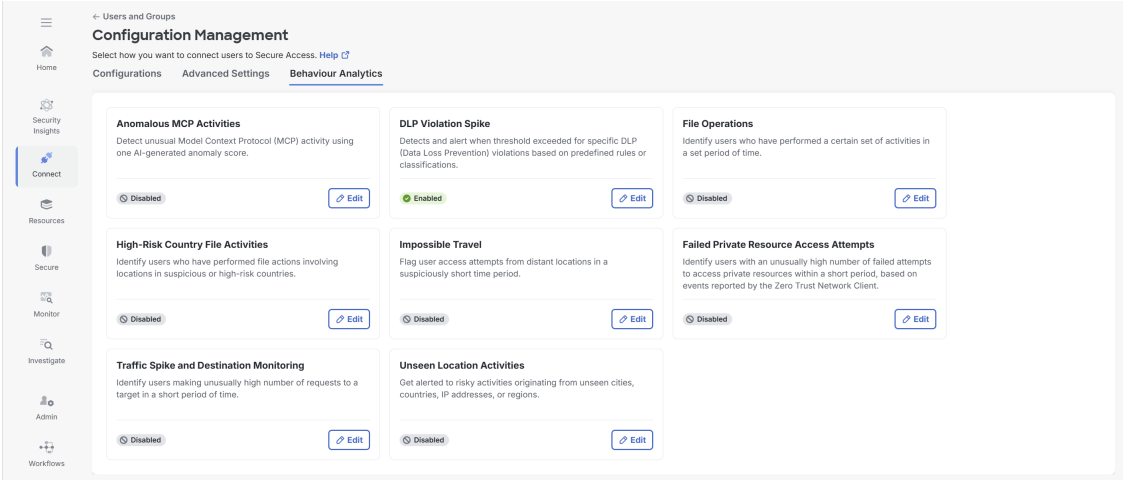
Changes to UEBA configurations appear in the Admin Audit Log. Entries identify UEBA as the feature and the anomaly type as the component. Update entries show the changed property and its previous and new values. For more information, see Admin Audit Log Report.

You can enable or disable anomaly detection for all users, configure limits for operations by hours and minutes, and receive continuous rule updates. Detected anomalies are available to you for 30 days, even if you later disable detection. This setup allows you to proactively detect and respond to potential security threats by monitoring deviations from the configured user behaviour patterns.

Available analytics

Analytics	What it detects	Detection basis
DLP Violation Spike	An unusual increase in Data Loss Prevention (DLP) policy violations for selected DLP rules or classifications.	A fixed threshold or an AI-based user baseline calculated from the previous seven days.
File Operations	Unusual bulk file uploads, downloads, and deletions.	Manually configured thresholds or an AI-based baseline for each user and operation. AI analyzes recent user activity and can require up to seven days to learn normal patterns. You can configure the thresholds manually or using AI.
High-Risk Country File Activities	File uploads to, or downloads from, countries that you designate as high-risk.	Selected file activities and countries.
Impossible Travel	Events from geographically distant locations within an unrealistic timeframe.	Configured travel conditions.
Anomalous MCP Activity	Unusual Model Context Protocol (MCP) activity, including potential injection activity or a sudden increase in requests.	MCP activity patterns evaluated by Secure Access.

Analytics	What it detects	Detection basis
Unseen Location Activity	User activity from a city or source IP address that is not in that user's rolling 60-day location history.	A rolling 60-day user location history. **Note** The system starts to generate alerts only after seven days of configuration.
Failed Private Resource Access Attempts	An unusually high number of failed attempts to access private resources.	An AI-based user baseline and a configured minimum number of failed attempts per hour. **Note** The system starts to generate alerts only after seven days of configuration.
Traffic Spike and Destination Monitoring	An unusual increase in requests to a specific destination or to any TOR relay.	An AI-based user baseline calculated from the previous seven days and the minimum alerting threshold that you configure. **Note** The system starts to generate alerts only after seven days of configuration.



AI-based thresholds

For analytics that use artificial intelligence (AI), Secure Access compares current activity with a baseline learned for the individual user. The threshold that you enter is a minimum alerting level, not the user's learned baseline.

> **Note**
>
> Secure Access generates an AI-based alert only when the activity is anomalous for the user and the activity meets the configured minimum threshold. A low minimum threshold does not force an alert when the activity is normal for the user. A high minimum threshold can suppress an otherwise anomalous event.

UEBA Scope

Describes UEBA Scope in Cisco Secure Access. UEBA supports only Secure Internet Access traffic paths and does not support Secure Private Access.

- UEBA analyzes only events that are associated with Active Directory (AD) users as it profiles user behavior.
- The following table lists the traffic types that each UEBA component analyzes.

Traffic type	UEBA components
Secure Web Gateway (SWG) web traffic	File Operations; High-Risk Country File Activities; Impossible Travel; Anomalous MCP Activity; Unseen Location Activity; Traffic Spike and Destination Monitoring
DLP events	DLP Violation Spike
Client-based ZTNA traffic	Failed Private Resource Access Attempts

- The following table lists the supported Secure Internet Access configurations and user sources.

Access type	Supported user source
Proxy auto-configuration (PAC) file (registered network)	AD user
Roaming Module (Umbrella)	AD user
Remote access VPN (RAVPN) to the internet	AD user; all analytics except Impossible Travel
Branch to the internet (remote tunnel or IPsec tunnel)	AD user; web traffic only
Zero Trust Access (ZTA) TIA	AD user; web traffic, ZTNA (client-based)

- For bulk file operations, UEBA supports uploads, downloads, and deletions only for a limited set of file-sharing applications.
- UEBA analyzes all configured DLP rules and classifications to detect spikes in DLP violations.

Configure Analytics for DLP Violation Spike

Describes Configure Analytics for DLP Violation Spike in Cisco Secure Access. Use DLP Violation Spike to detect unusual increases in Data Loss Prevention policy violations.

Use DLP Violation Spike to detect unusual increases in Data Loss Prevention policy violations. This feature detects any violation that matches selected DLP rules and selected DLP classifications.

Detection methods

Fixed-threshold detection

Secure Access generates an anomaly when the number of violations exceeds the count that you configure within the selected time period.

Artificial intelligence-based detection

Secure Access compares the current violation count with a baseline learned for the individual user from the previous seven days. The count that you configure is a minimum alerting threshold. It does not replace the learned baseline.

> **Note**
>
> With AI-based detection, both conditions must be met: the activity must be anomalous for the user, and the activity must meet the configured minimum threshold.

Threshold examples

Example	Evaluation	Outcome
Fixed threshold: 10 violations in 1 hour	The user reaches 11 violations within 1 hour.	Secure Access generates an anomaly.
AI baseline: 2 violations per hour; minimum threshold: 40	The user reaches 10 violations in 1 hour. The activity is unusual, but it is below the minimum threshold.	Secure Access does not generate an anomaly.
AI baseline: 50 violations per hour; minimum threshold: 10	The user reaches 11 violations in 1 hour. The count is above the minimum, but it is not unusual for the user.	Secure Access does not generate an anomaly solely because the count exceeded 10.

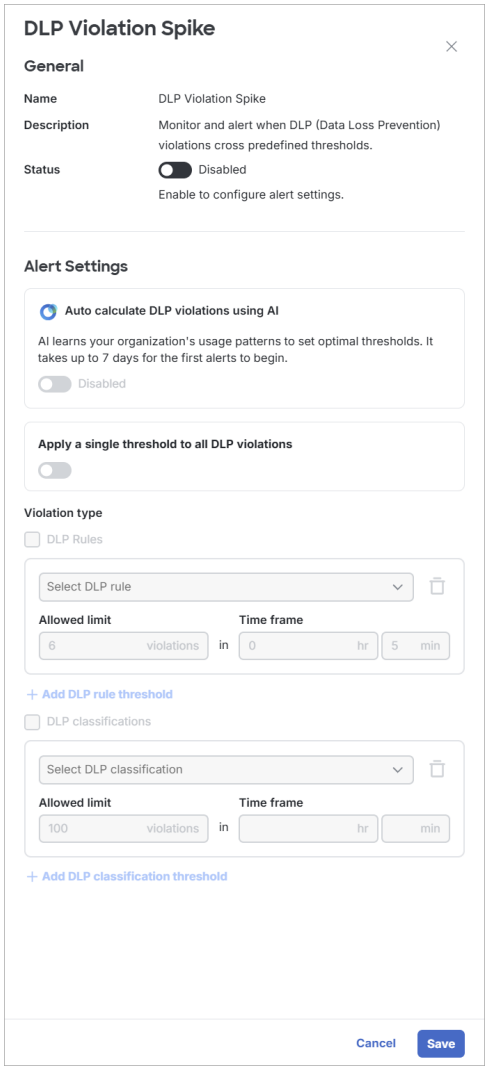
Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. To configure behaviour analytics for DLP Violation Spikes, perform the following steps.

To configure behaviour analytics for DLP Violation Spikes, perform the following steps.

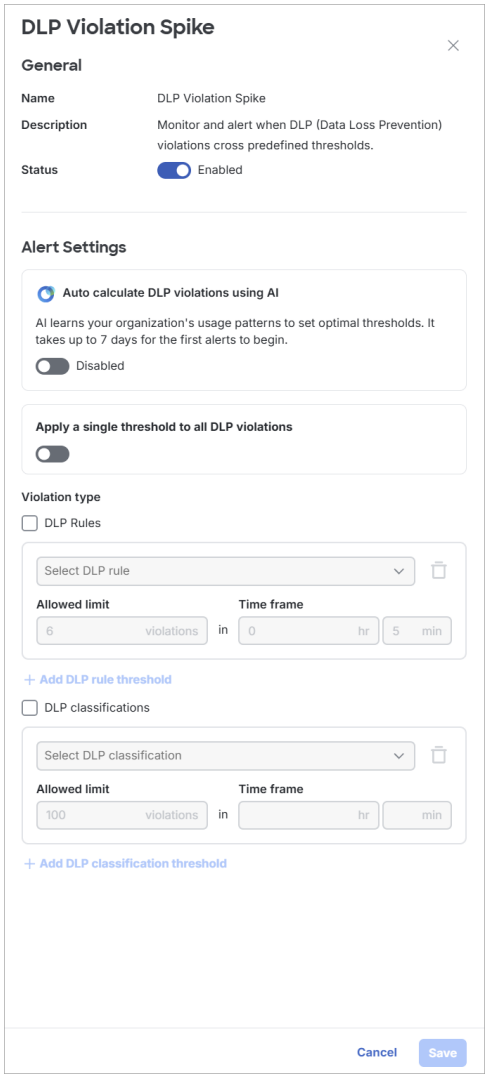
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. Click **Edit** on the **DLP Violation Spike** tile.

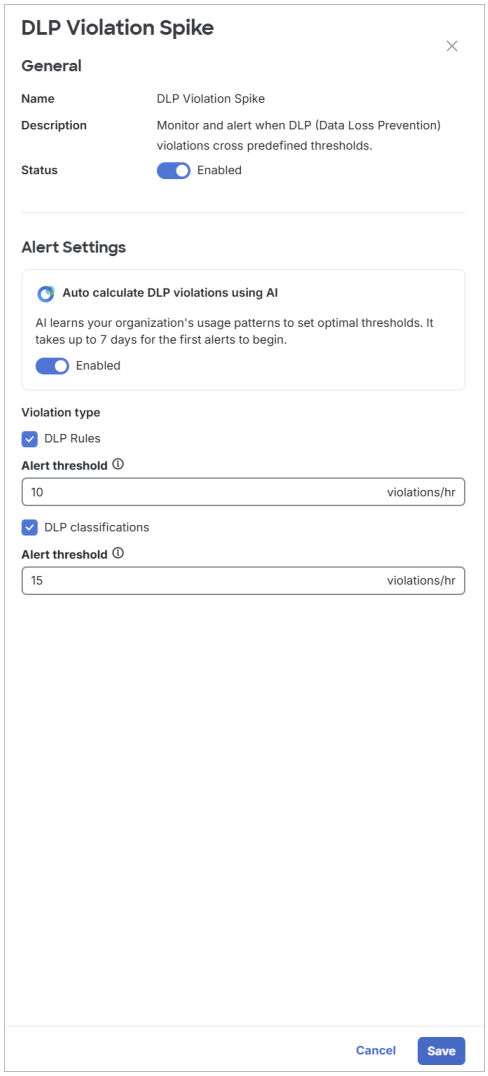


The edit side panel appears.

3. Turn on the **Status** toggle.



4. For AI-based detection, enable the **Auto calculate DLP violations using AI** option and enter the minimum violation count and time period for the required violation types.



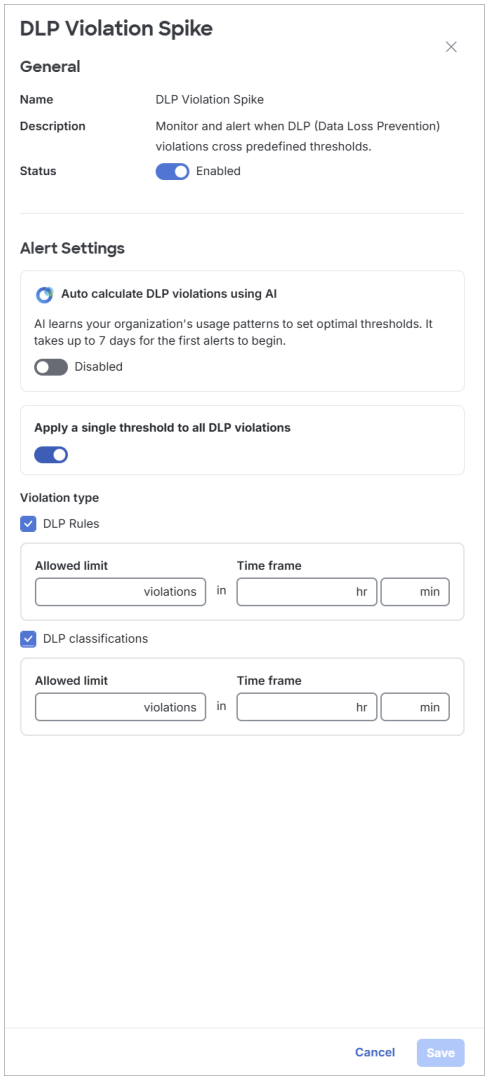
Note

Secure Access uses the previous seven days of user activity to establish a user-specific baseline.

Note

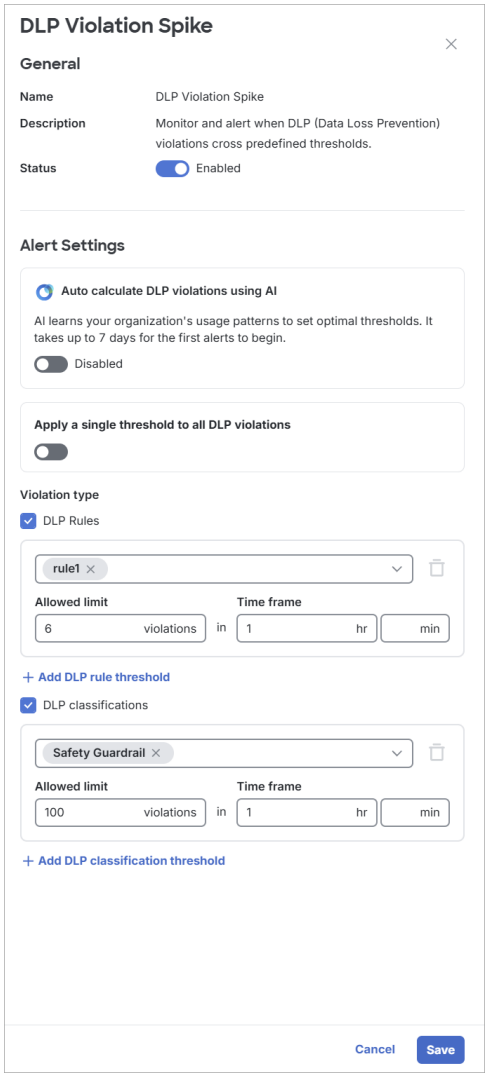
The alert threshold value is optional and can be any number between 0 and 10000.

5. Select **Apply a single threshold to all DLP violations** to select a single threshold for all DLP violations.



   a. Select one or both the Violation types and set the **Allowed limit** along with the **Time frame**.

6. To set threshold limit for each DLP violation separately, select the required DLP violation type and then select the required violations from the drop-down list.
7. Enter the allowed violation count for the selected DLP violations and the respective time frames.



> **Note**
>
> The threshold time frame must be between five minutes and 24 hours.

8. Click **+ Add DLP rule threshold** to add threshold limit for another DLP rule.
9. Click **+ Add DLP classification threshold** to add threshold limit for another DLP classification.
10. Click **Save**.

> **Note**
>
> When AI mode is enabled, repeated alerts for the same user are suppressed for 60 minutes. When configured manually, repeated alerts for the same user are suppressed for the configured time frame.

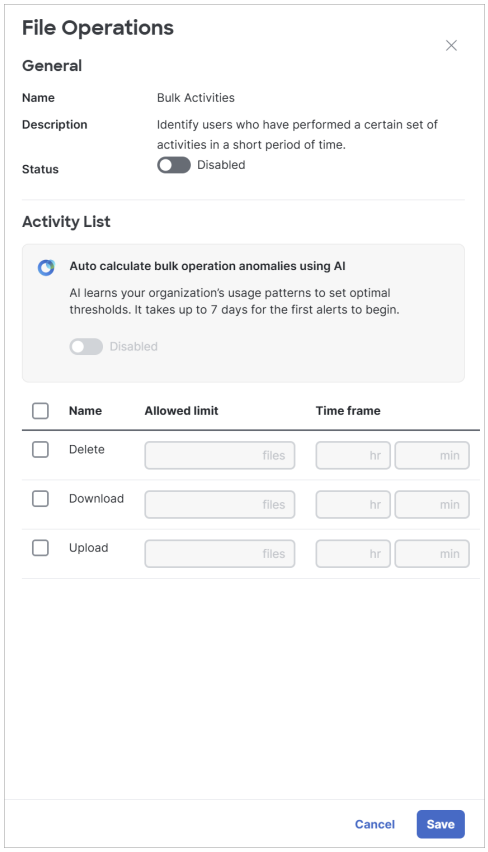
Configure Analytics for File Operations with AI

Provides instructions for completing the Configure Analytics for File Operations with AI workflow in Cisco Secure Access. To configure behaviour analytics for file operations with AI, perform the following steps.

To configure behaviour analytics for file operations with AI, perform the following steps.

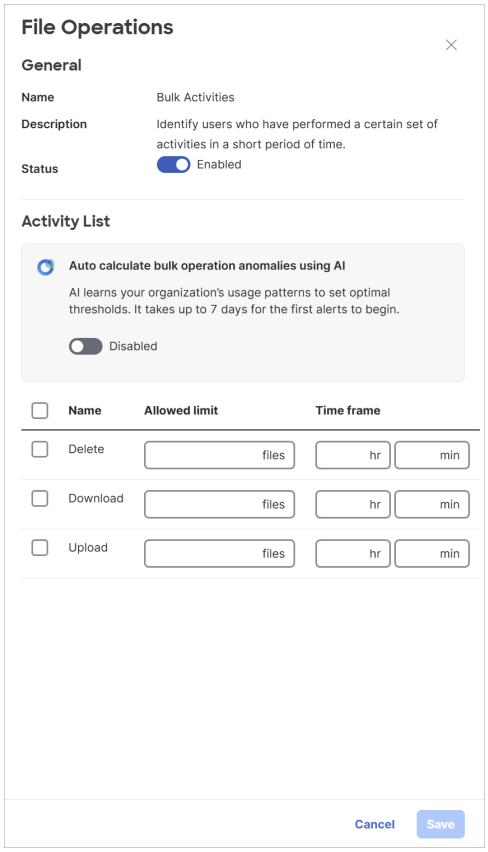
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. Click **Edit** on the **File Operations** tile.

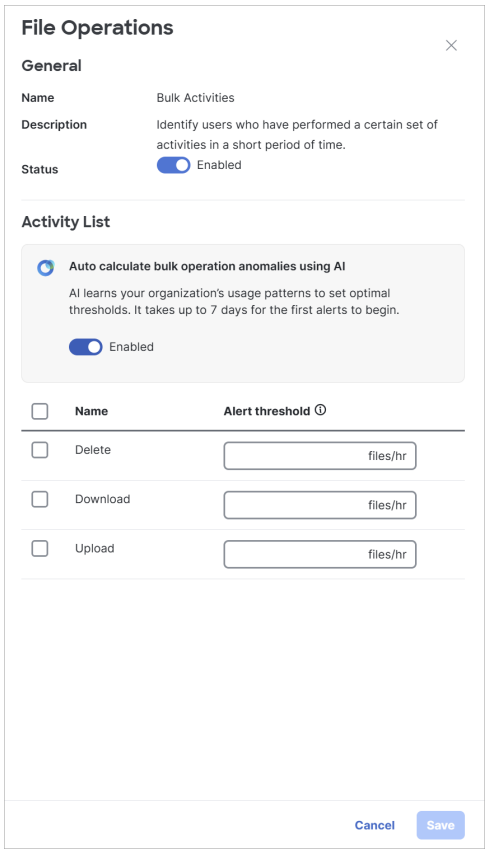


The edit side panel appears.

3. Click the **Status** toggle to enable it.



4. Enable the **Auto calculate bulk operation anomalies using AI** option to use AI to analyze and set the optimal threshold for each operation for each user.

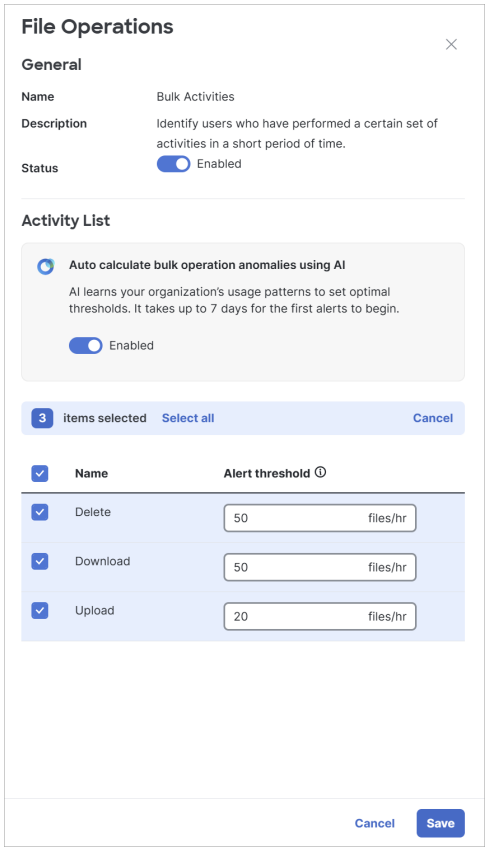


Once enabled, Cisco Secure Access learns normal file activity patterns and generates alerts for anomalous bulk file operations.

> **Note**
>
> The AI learning period can take up to 7 days before the first alert is generated.

> **Note**
>
> When AI mode is enabled, repeated alerts for the same user are suppressed for 60 minutes.

5. Select the required file operation names.
6. You can enter the file count that you want to allow for each operation and the time frames respectively.



> **Note**
>
> The alert threshold acts as a minimum activity level for generating an alert. If activity is anomalous but stays below the threshold, no alert is generated.

> **Note**
>
> The alert threshold value is optional and can be any number between 0 and 10000.

7. Click **Save**.

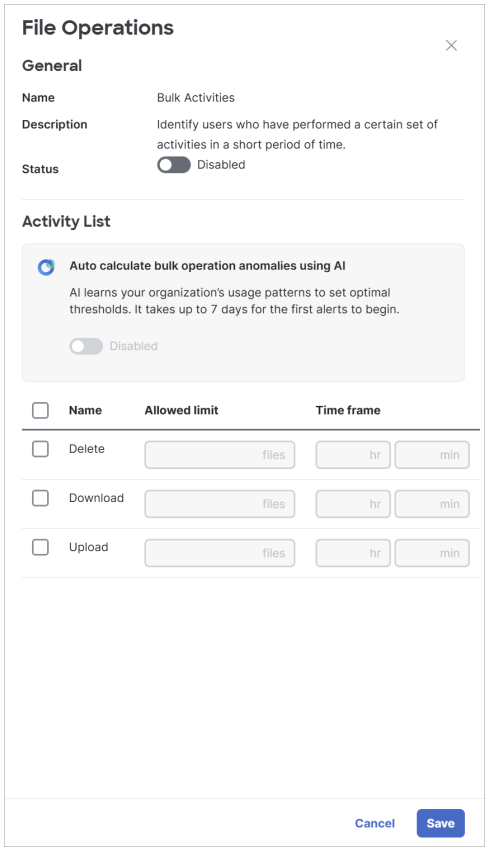
Configure Analytics for File Operations Manually

Provides instructions for completing the Configure Analytics for File Operations Manually workflow in Cisco Secure Access. To configure behaviour analytics for file operations manually, perform the following steps.

To configure behaviour analytics for file operations manually, perform the following steps.

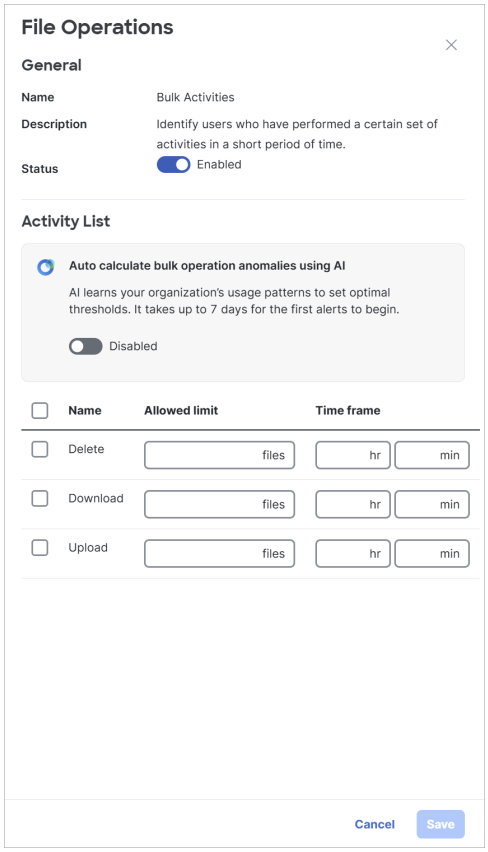
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. Click **Edit** on the **File Operations** tile.

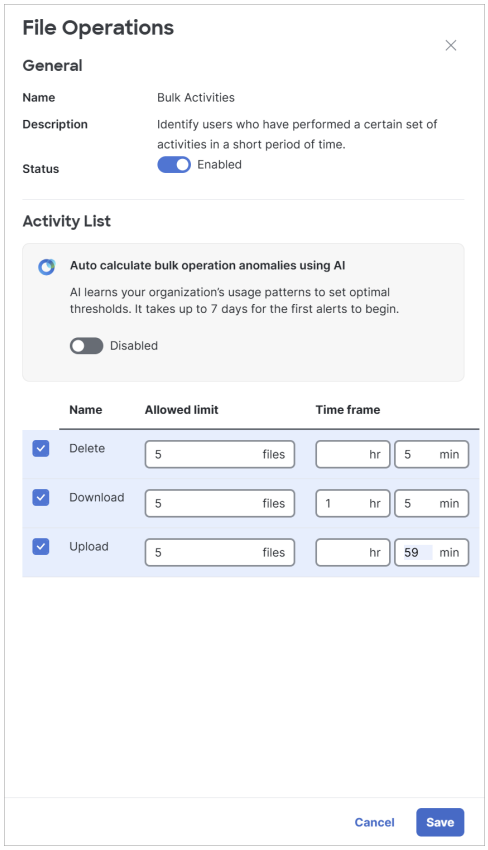


The edit side panel appears.

3. Click the **Status** toggle to enable it.



4. Set the file operation thresholds:
   a. Click the **Delete** checkbox, and then enter the maximum number of deleted files and the duration in the respective fields.
   b. Click the **Download** checkbox, and then enter the maximum number of downloaded files and the duration in the respective fields.
   c. Click the **Upload** checkbox, and then enter the maximum number of uploaded files and the duration in the respective fields.



> **Note**
>
> The threshold file count must be five or more.

> **Note**
>
> The threshold time frame must be between five minutes and 24 hours.

5. Click **Save**.

> **Note**
>
> When manual thresholds are used, repeated alerts for the same user are suppressed for the configured time frame.

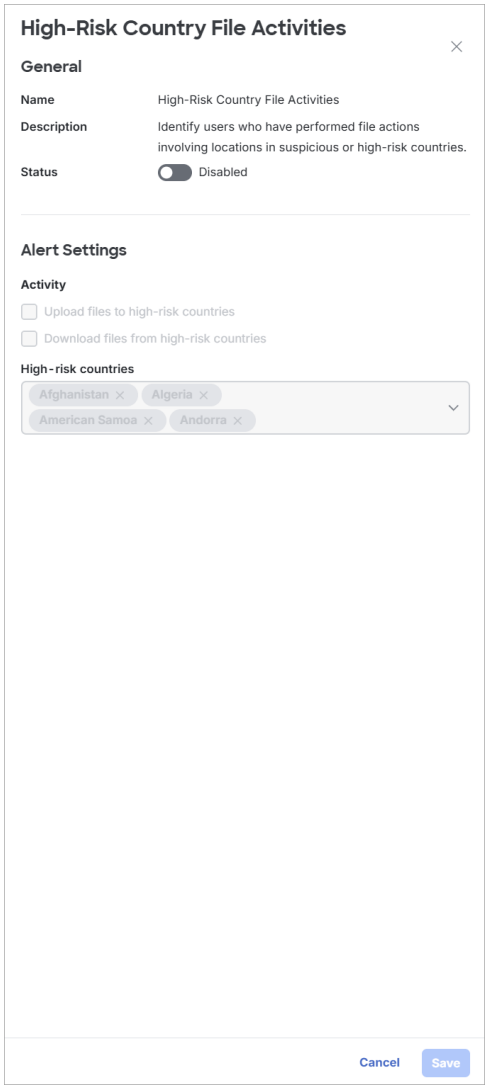
Configure Analytics for High-Risk Country File Activities

Provides instructions for completing the Configure Analytics for High-Risk Country File Activities workflow in Cisco Secure Access. To configure behavior analytics for uploads to and downloads from high-risk countries, perform the following steps.

To configure behavior analytics for uploads to and downloads from high-risk countries, perform the following steps.

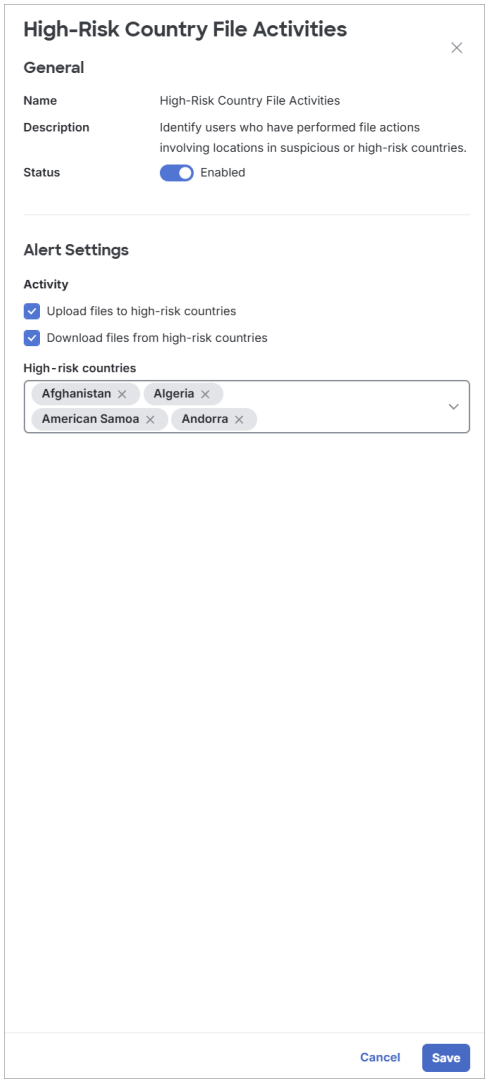
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. Click **Edit** on the **High-Risk Country File Activities** tile.



   The edit side panel appears.

3. Click the **Status** toggle to enable it.
4. Select the required file activities from the following options:
   - **Upload files to high-risk countries** – Enable analytics for upload activity to the selected high-risk country.
   - **Download files from high-risk countries** – Enable analytics for download activity from the selected high-risk country.
5. Select the high-risk countries from the drop-down list.



Note

You can select as many countries as required.

6. Click **Save**.

Note

Repeated alerts for the same user are suppressed for 60 minutes.

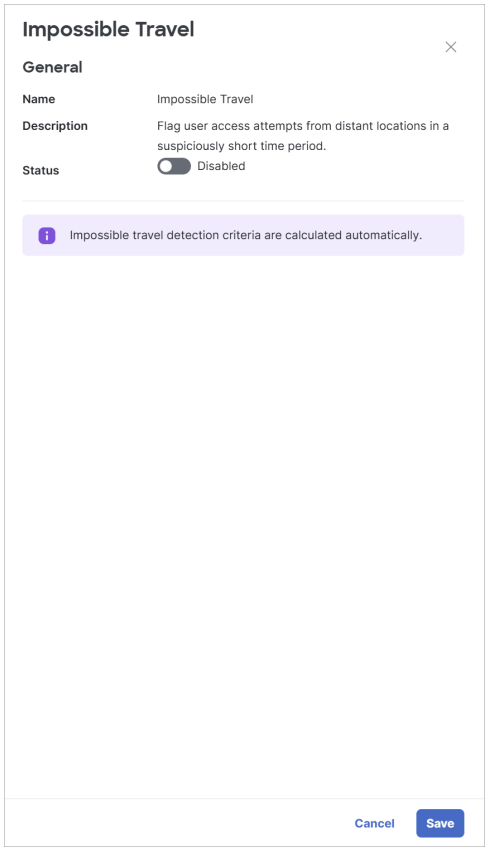
Configure Analytics for Impossible Travel

Provides instructions for completing the Configure Analytics for Impossible Travel workflow in Cisco Secure Access. To configure behaviour analytics parameters, perform these steps.

To configure behaviour analytics parameters, perform these steps.

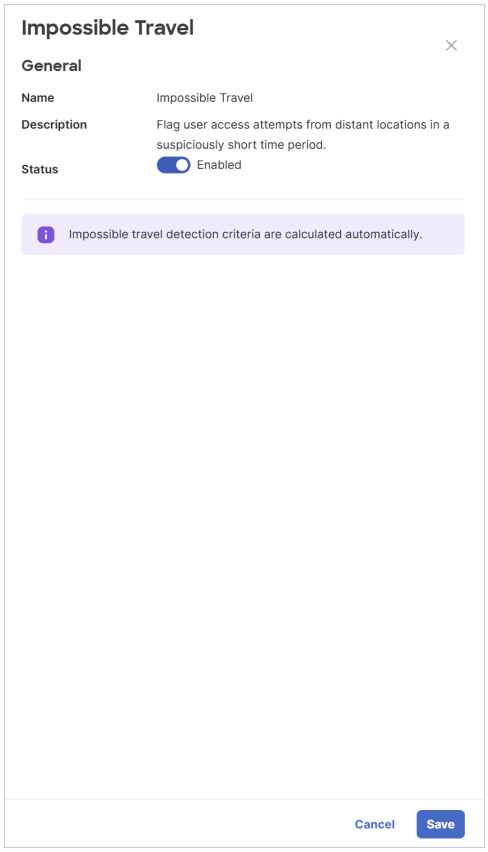
Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. Click **Edit** on the **Impossible Travel** tile.



   The edit side panel appears.

3. Click the **Status** toggle to enable it.



4. Click **Save**.

> **Note**
>
> Repeated alerts for the same user are suppressed for 60 minutes.

> **Note**
>
> The system generates an alert only if the location is not visited by the user in the preceding seven days.

Configure Analytics for Anomalous MCP Activities

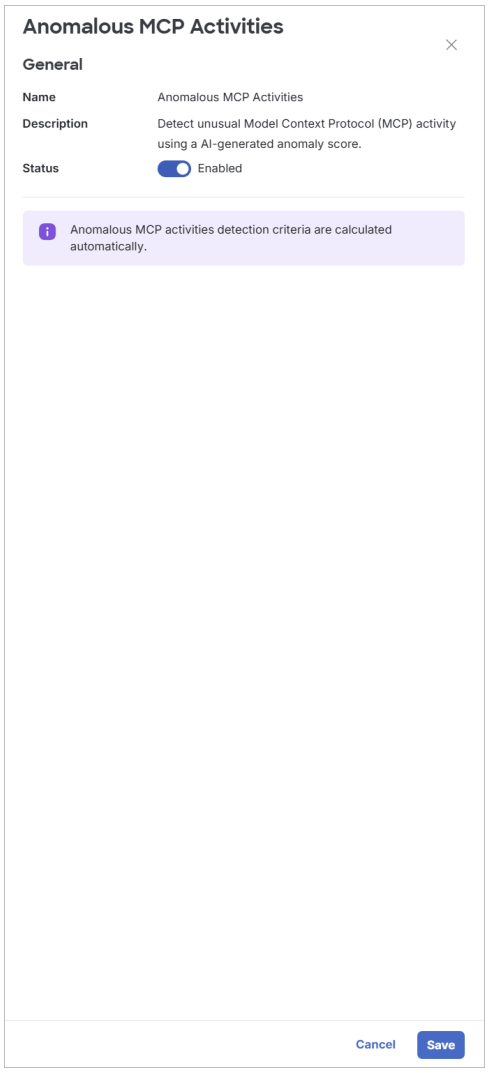
Provides instructions for completing the Configure Analytics for Anomalous MCP Activities workflow in Cisco Secure Access. Anomalous MCP Activities detects Model Context Protocol (MCP) activity that differs from expected patterns.

Anomalous MCP Activities detects Model Context Protocol (MCP) activity that differs from expected patterns. Examples include potential injection activity and a sudden increase in MCP requests.

To configure behaviour analytics for anomalous MCP activity, perform the following steps.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour Analytics**.
2. On the **Anomalous MCP Activities** tile, select **Edit**.
3. Turn on the **Status** toggle.



4. Select **Save**.

> **Note**
>
> Repeated alerts for the same user are suppressed for 60 minutes.

Secure Access begins monitoring MCP activity. To receive notifications, create a behavior analytics alert rule for anomalous MCP activity.

Configure Analytics for Unseen Location Activities

Provides instructions for completing the Configure Analytics for Unseen Location Activities workflow in Cisco Secure Access. Secure Access maintains a rolling 60-day location history for each user when Unseen Location Activities is enabled.

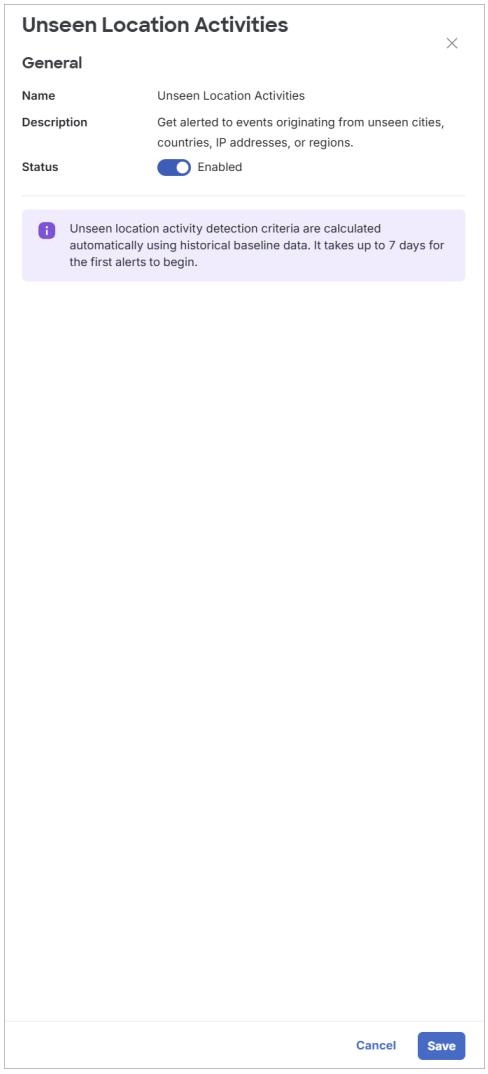
Secure Access maintains a rolling 60-day location history for each user when **Unseen Location Activities** is enabled. Activity can be identified as anomalous when the city or source IP address is not present in that user's history.

> **Note**
>
> The system starts to generate alerts only after seven days of configuration.

To configure behaviour analytics for unseen location activities, perform the following steps.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour Analytics**.
2. On the **Unseen Location Activity** tile, select **Edit**.
3. Turn on the **Status** toggle.



4. Select **Save**.

> **Note**
>
> Repeated alerts for the same user are suppressed for 60 minutes.

Secure Access evaluates user locations against the preceding 60 days of location history. To receive notifications, create a behavior analytics alert rule for unseen location activity.

Configure Analytics for Traffic Spike and Destination Monitoring

Provides instructions for completing the Configure Analytics for Traffic Spike and Destination Monitoring workflow in Cisco Secure Access. The Traffic Spike and Destination Monitoring detects the following activity: An unusually high number of requests to any TOR relay.

The Traffic Spike and Destination Monitoring detects the following activity:

- An unusually high number of requests to any TOR relay.

- An unusually high number of requests to a specific destination.

Secure Access compares current activity with a user-specific baseline calculated from the previous seven days. The threshold that you enter is the minimum activity level at which an AI-based anomaly can generate an alert.

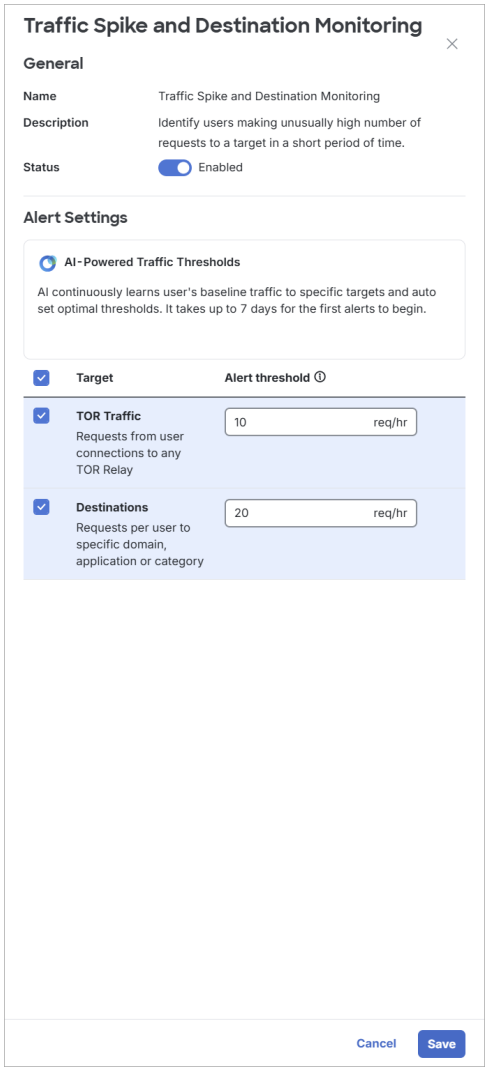
Important

Activity must be anomalous for the user and meet the configured minimum threshold. Exceeding the minimum threshold does not generate an alert when the activity is normal for the user.

To configure behaviour analytics for traffic spikes, perform the following steps.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour Analytics**.
2. Click **Edit** on the **Traffic Spike and Destination Monitoring** tile.
3. Turn on the **Status** toggle.
4. Select the intended target type that you want to configure.
   - Select **TOR traffic** for requests to any TOR Relay.
   - Select **Destination** to monitor requests to a specific domain, application, or category.
5. Enter the minimum request count per hour as the **Alert threshold** for the selected target type.



Note

The alert threshold value is optional and can be any number between 0 and 10000.

6. Select **Save**.

Note

Repeated alerts for the same user are suppressed for 60 minutes.

Secure Access compares request activity with the user's recent baseline. To receive notifications, create a behavior analytics alert rule for each traffic spike type that you enable.

Configure Analytics for Failed Private Resource Access Attempts

Failed Private Resource Access Attempts identifies an unusually high number of failed attempts to access private resources. It analyzes client-based Zero Trust Network Access (ZTNA) traffic only. Your organization must use client-based ZTNA to use this analytics.

Secure Access generates alerts for authentication failures and access-policy rule denials. It does not generate alerts for DNS resolution, profile configuration, device posture, or protocol mismatch failures.

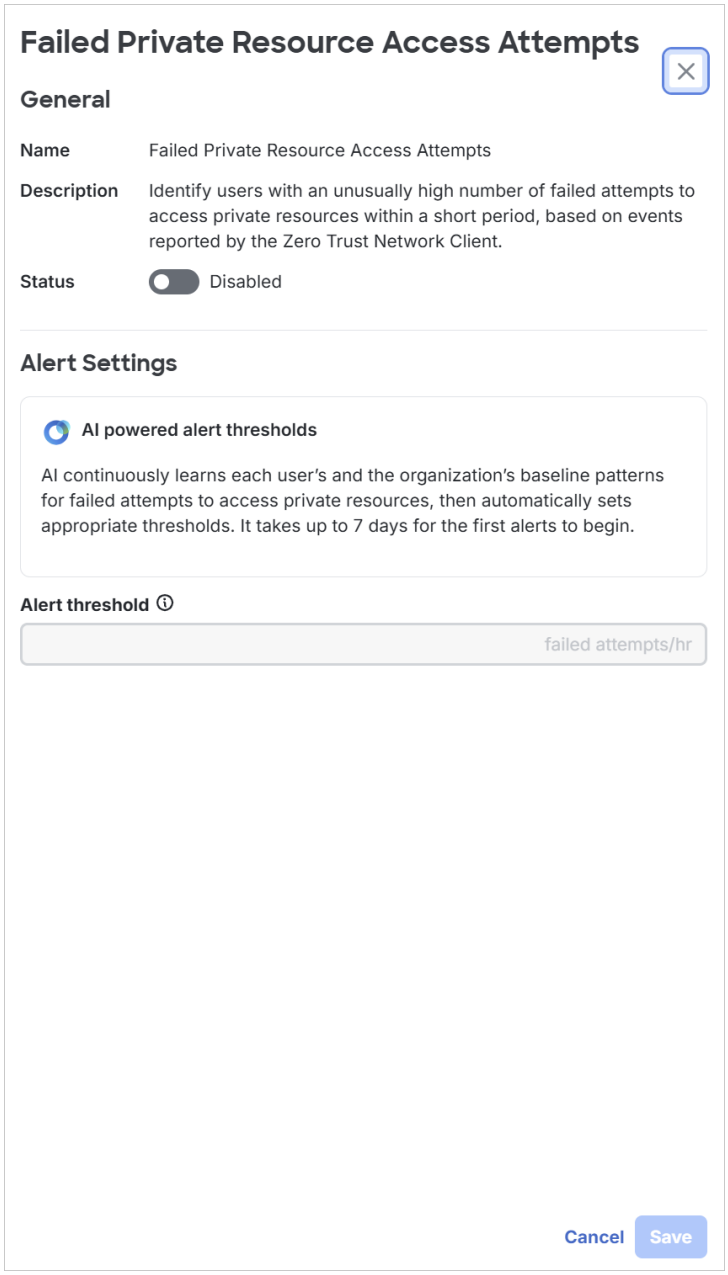
The analytics uses an AI-based user baseline. Secure Access generates an alert when activity is anomalous for the user and meets the configured minimum threshold.

To configure Failed Private Resource Access Attempts, perform these steps:

Before you begin

Procedure

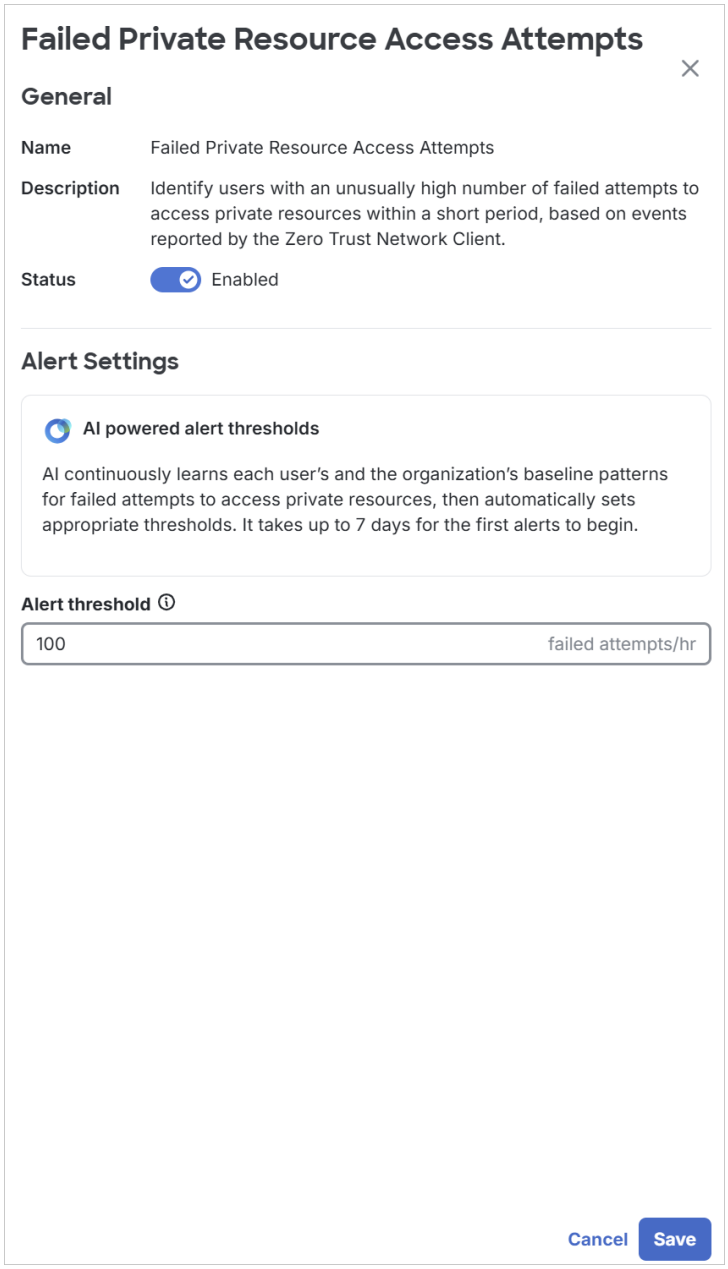
1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **Behaviour analytics**.
2. On the Failed Private Resource Access Attempts tile, click **Edit**.



3. Click the **Status** toggle to enable it.
4. Enter a value in **Alert threshold**.

> **Note**
>
> The alert threshold acts as a minimum activity level for generating an alert. If activity is anomalous but stays below the threshold, no alert is generated.

> **Note**
>
> The alert threshold value is optional and can be any number between 0 and 10,000.



5. Click **Save**.

> **Note**
>
> Secure Access can take up to seven days after you enable this analytics to generate the first alert. It suppresses repeated alerts for the same user for 60 minutes.

What to do next

To receive notifications, create a behavior analytics alert rule for Failed Private Resource Access Attempts. To know more, see Add and Edit Alert Rules for Behavior Analytics

Known Issues

Known issues for the User and Entity Behavior Analysis feature.

The following issues are known and will be addressed in future releases.

- When you view bulk file action anomalies in User and Entity Behavior Analysis event details, the file name might appear as unspecified in some cases.
- The **View more in Events** link at the bottom of UEBA events list pane redirects to the Events page . But it shows all events by the user during past 10 minutes time window of latest anomalous event. It does not show the exact anomalous events in Events page table.

21 Identity Providers

Topics:

- Configure Identity Providers
- Provision Users and Groups from Duo
- Provision Users and Groups from Okta
- Provision Users and Groups from Microsoft Entra ID

Provides an overview of Identity Providers in Cisco Secure Access, including Configure Identity Providers, Provision Users and Groups from Duo, and Provision Users and Groups from Okta. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Configure Identity Providers

Describes Configure Identity Providers in Cisco Secure Access. You can provision an organization's users and groups in Cisco Secure Access by setting up integrations with cloud identity providers (IdPs).

You can provision an organization's users and groups in Cisco Secure Access by setting up integrations with cloud identity providers (IdPs).

After you add an IdP in Secure Access, sign on to the IdP and add your generated Secure Access SCIM token and the Secure Access identity provisioning URL to the IdP. Secure Access uses the System for Cross-domain Identity Management (SCIM) protocol to exchange user and group information with Azure, Okta, and other IdPs.

Provision Users and Groups from Duo

Describes Provision Users and Groups from Duo in Cisco Secure Access. Add Duo as a cloud identity provider (IdP) to provision your organization's users and groups from Duo to Secure Access and use Duo IdP for authentication.

Add Duo as a cloud identity provider (IdP) to provision your organization's users and groups from Duo to Secure Access and use Duo IdP for authentication.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- A valid subscription is required to access the Duo dashboard.
- Add the Cisco Secure Access application, configure it, and proceed to the Provisioning tab.
- Add the provisioning in Secure Access, then generate a valid Bearer token and link from Cisco Secure Access.
- In the Provisioning tab of the Cisco Secure Access Duo application, add the Bearer token generated in Secure Access.
- No concurrent provisioning of the same users or groups from both on-premises AD and Duo. If you are using the on-premises AD Connector to import users and groups, and you also want to import the same users and groups from Duo, ensure that the on-premises AD Connector is either turned off or that the Connector service on the connector machine is stopped.

Limits and Best Practices

Describes Limits and Best Practices in Cisco Secure Access. Secure Access supports provisioning a maximum of 1000 groups from Duo.

- Secure Access supports provisioning a maximum of 1000 groups from Duo. Any groups beyond this number that are in scope are not provisioned. Secure Access does not restrict the number of users that you can provision from Duo. For more information, see Limitations and range limits on page 50.
- To ensure that all users are provisioned, assign the **Everyone** group to the **Cisco Secure Access** app. You can push other additional groups for group-based Secure Access rule enforcement.
- Duo does not support nested groups.
- If you previously imported groups from the on-premises AD and push the same groups from Duo, the groups from Duo do not overwrite the groups imported from the on-premises AD. You must reassign any group-based Secure Access policy rules to the groups imported from Duo.
- Provisioning large numbers of users and groups to Secure Access may take several hours.
- After the initial provisioning of users and groups, it can take up to one hour for subsequent changes to users and groups to reflect in Secure Access.
- Concurrent synchronization of the same users and groups from the on-premises AD and the **Cisco Secure Access** app is not supported and leads to inconsistent policy enforcement.
- For IP-to-user mapping deployments, you must use an on-premises AD Connector. Duo does not store the private IP to AD user mappings.

Supported Features

Describes Supported Features in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports these features in Duo:

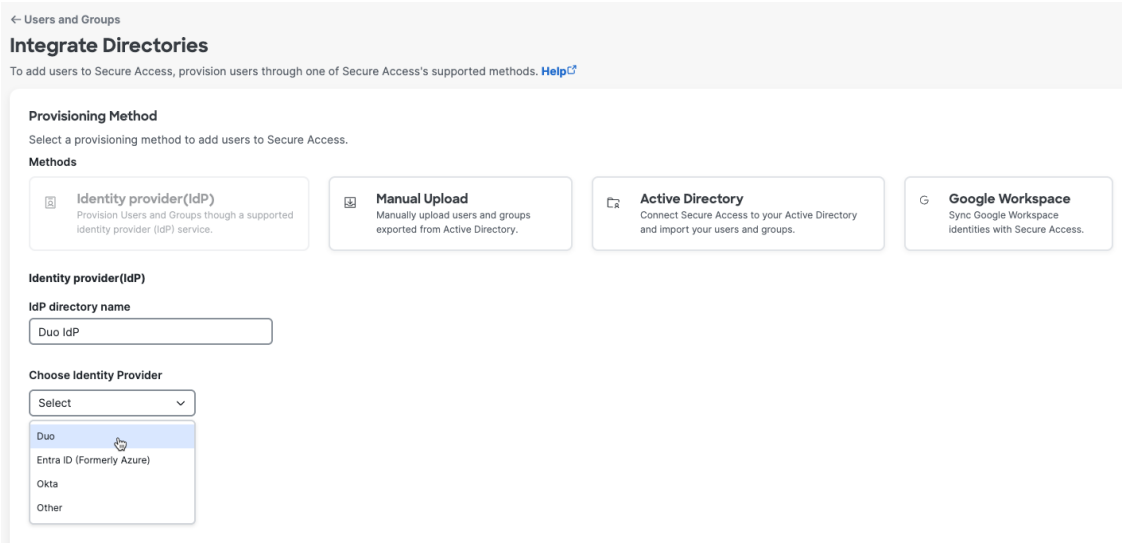
- **Create Users**–New users created in Duo are also created in Secure Access.
- **Update User Attributes**–Updates to a user's profile through Duo are pushed to Secure Access.
- **Deactivate Users**–Deactivating a user through Duo deactivates the user in Secure Access.
- **Group Push**–Groups in Duo are pushed to Secure Access.

Add the Duo IdP directory to Secure Access

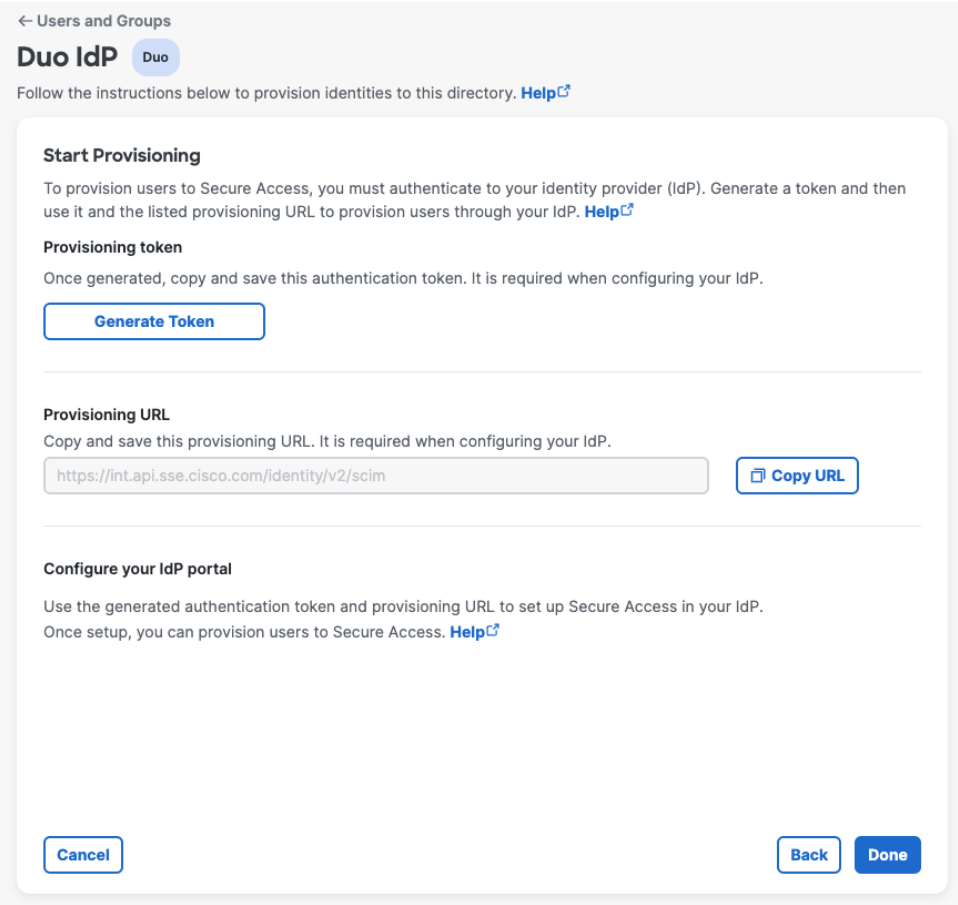
Provides instructions for completing the Add the Duo IdP directory to Secure Access workflow in Cisco Secure Access. Navigate to Connect Users, Groups, and Endpoint Devices Configuration management Directories .

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > > **Directories**.
2. Click **Integrate directories**.
3. Navigate to **Methods** and click **Identity provider (IdP)**.



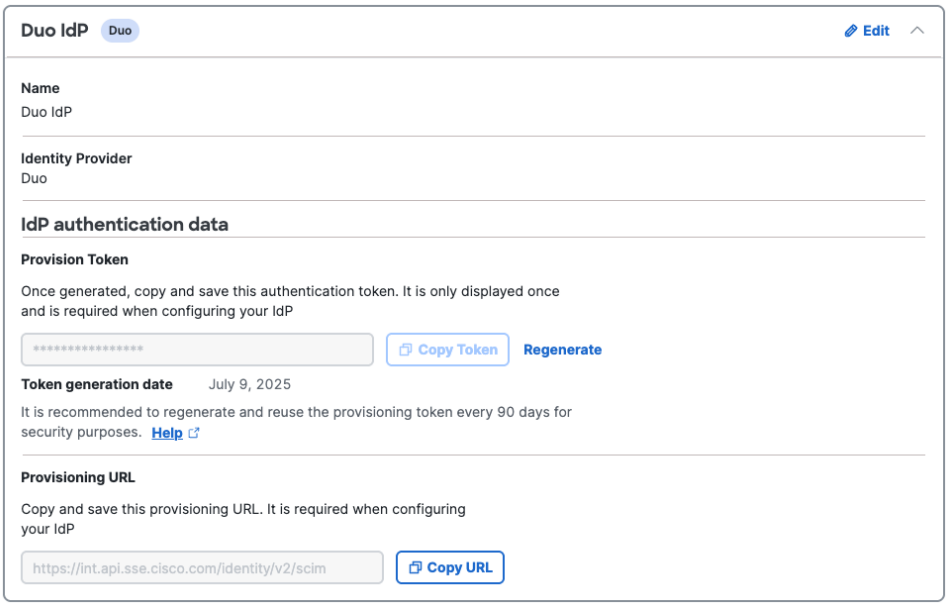
4. Enter an **IdP directory name**.
5. **Choose Identity Provider**: Select **Duo**.
6. Click **Next**.
7. Click **Generate Token**.



8. Copy and save the provisioning token and provisioning URL. It is required to complete the integration with Duo. For security reasons, your token will only be displayed once.
9. Click **Done**.

What to do next

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration** to review your Duo IdP directory settings. You can regenerate your provision token from this menu. It is recommended to regenerate and reuse the provisioning token every 90 days for security purposes.



View Provisioned Users and Groups in Secure Access

Provides instructions for completing the View Provisioned Users and Groups in Secure Access workflow in Cisco Secure Access. Navigate to Connect Users, Groups, and Endpoint Devices to view the users and groups provisioned from Duo.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** to view the users and groups provisioned from Duo.

- For more information, see View User Details.
- For more information, see View Groups and Organizational Unit Details.

Refresh SCIM Token

Describes Refresh SCIM Token in Cisco Secure Access. To avoid disrupting the provisioning of users and groups, we recommend that you refresh the SCIM token in Secure Access at least once every 90 days and immediately copy the new token to the Cisco User Management Connector app in Duo.

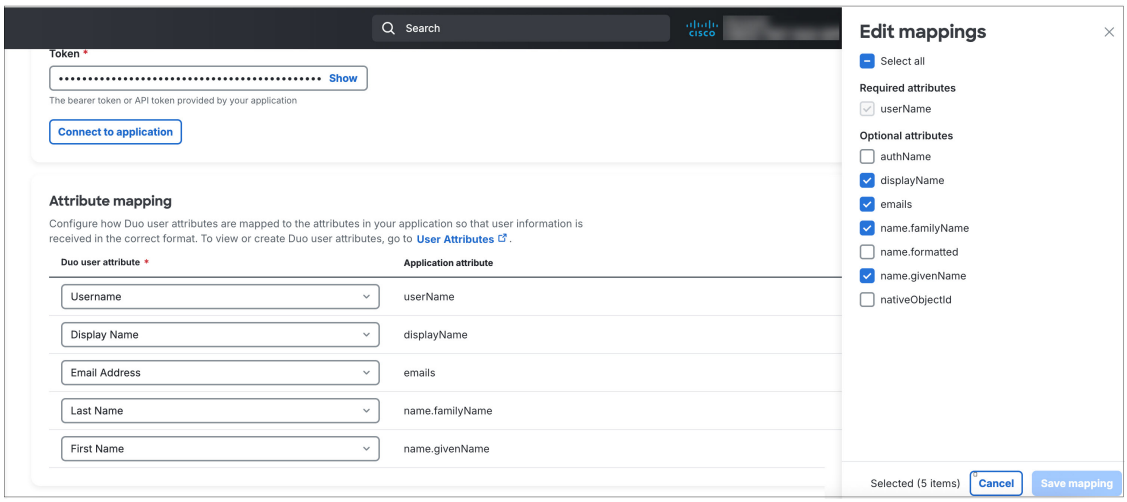
To avoid disrupting the provisioning of users and groups, we recommend that you refresh the SCIM token in Secure Access at least once every 90 days and immediately copy the new token to the **Cisco User Management Connector** app in Duo. For more information about generating the SCIM token, see Add a Cloud Identity Provider.

The administrators in the Secure Access organization are responsible for refreshing the SCIM token. Secure Access does not perform this action.

Attribute Mapping (Mandatory)

Describes Attribute Mapping (Mandatory) in Cisco Secure Access. To ensure the Duo Secure Access integration functions properly, the customer must open the user attributes panel, select the attributes on the right-hand side, and choose the attribute from the drop-down menu in the specified order.

To ensure the Duo Secure Access integration functions properly, the customer must open the user attributes panel, select the attributes on the right-hand side, and choose the attribute from the drop-down menu in the specified order. The mapping will only work correctly if these steps are followed.



Provision Users and Groups from Okta

Describes Provision Users and Groups from Okta in Cisco Secure Access. Cisco Secure Access supports the provisioning of users and groups from the Okta identity provider (IdP).

Cisco Secure Access supports the provisioning of users and groups from the Okta identity provider (IdP).

After you generate your System for Cross-domain Identity Management (SCIM) token in Secure Access, add the SCIM token in the **Cisco User Management Connector** app in the Okta portal.

Then, provision users and groups to Secure Access through the app.

Limits and Best Practices

- Secure Access supports provisioning a maximum of 1000 groups from Okta. Any groups beyond this number that are in scope are not provisioned. Secure Access does not restrict the number of users that you can provision from Okta. For more information, see Limitations and Range Limits.
- To ensure that all users are provisioned, assign the **Everyone** group to the **Cisco User Management Connector** app. You can push other additional groups for group-based Secure Access rule enforcement.
- Okta does not support nested groups.
- If you previously imported groups from the on-premises AD and push the same groups from Okta, the groups from Okta do not overwrite the groups imported from the on-premises AD. You must reassign any group-based Secure Access policy rules to the groups imported from Okta.
- Provisioning large numbers of users and groups to Secure Access may take several hours.
- After the initial provisioning of users and groups, it can take up to one hour for subsequent changes to users and groups to reflect in Secure Access.
- Concurrent synchronization of the same users and groups from the on-premises AD and the **Cisco User Management Connector** app is not supported and leads to inconsistent policy enforcement.
- For IP-to-user mapping deployments, you must use an on-premises AD Connector. Okta does not store the private IP to AD user mappings.

Supported Features

Secure Access supports these features in Okta:

- **Create Users**–New users created in Okta are also created in Secure Access.
- **Update User Attributes**–Updates to a user's profile through Okta are pushed to Secure Access.
- **Deactivate Users**–Deactivating a user through Okta deactivates the user in Secure Access.
- **Group Push**–Groups in Okta are pushed to Secure Access.

Refresh the SCIM Token

We recommend that you refresh the SCIM token at least once every 90 days and immediately copy the SCIM token to the **Cisco User Management Connector** app on Okta.

Refreshing the SCIM token is the responsibility of the administrator. Secure Access does not perform this action.

Configure the Cisco User Management Connector App in Okta

Describes Configure the Cisco User Management Connector App in Okta in Cisco Secure Access and outlines Multi-App Configuration, In-App SAML Configuration, and Supported Functionality. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

There are currently two methods of configuring the Cisco User Management Connector application in Okta, a method that involves multiple yet separate applications to confirm, test, and deploy your configuration or a single in-app experience with SAML within Okta. Review the following methods to discover which one is best for your environment:

Multi-App Configuration

This procedure uses multiple applications; if you have a simplified SAML configuration and do not want to use multiple applications consider using the **In-App SAML Configuration** instead.

Use Cases

- **Existing Deployments** - If you already have the Cisco Management Connector application configured in Okta, we encourage you to continue this method. There is no change in functionality or app availability once your configuration is deployed.
- **Complex Configurations** - If you configurations that require advanced settings or fine-tuned control, using multiple independent apps to provision and authenticate your users is the ideal method as it allows you to shift your custom applications separately as needed instead of relying on one internal app to manage everything.

In-App SAML Configuration

Utilizing SAML in the Cisco User Management Connector app allows for a single application in Okta to both provision and authenticate a limited selection of configurations. This method allows a simplified and unified administrative experience where you can configure both the user lifecycle provisioning and SAML-based authentication from a single Okta application, eliminating the need to manage separate integrations for these capabilities; with reduced operational complexity, this method minimizes the number of Okta applications required for common deployments while keeping advanced SAML options available when needed. Using one setup and management workflow for provisioning and SAML configuration instead of coordinating across multiple Okta applications; this also allows you to customize username and attribute mapping during provisioning to match your organization's naming conventions and identity standards.

Also provided with new deployments is **custom username mapping** where you can map provisioning usernames to organizational standards (for example, email prefix, employee ID, or UPN) using configurable username attribute settings. For more information about how Okta handles SAML app integrations, see Okta SAML app integrations documentation.

Use Cases

- **New Deployment** - Use a single application in Okta hat handles new user provisioning and SAML SSO for a straightforward, consolidated identity workflow.
- **Gradual Migration** - Evaluate the unified application in a test Okta environment before changing production identity flows; this is ideal for new deployments **or** small, simple deployments from existing users.

> **Note**
>
> Only SP-initiated SSO is supported at this time.

Supported Functionality

The following actions are supported in Okta:

- **Create Users** - New users created in Okta will also be created in Umbrella.
- **Update User Attributes** - Updates to a user's profile through Okta will be pushed to Umbrella.
- **Deactivate Users** - Deactivating a user through Okta deactivates the user in Umbrella.
- **Group Push** - Groups in Okta can be pushed to Umbrella.

> **Note**
>
> Be aware that communication for this integration moves one-way from Secure Access to Okta regardless of whether you choose multi-app or in-app provisioning and authentication.

Once you decide the SAML method for your Okta integration, use the following procedures to commit and deploy your environment:

- Add the Cisco User Management Connector App in Okta
- Enable In-App SAML SSO for the Cisco Management Connector in Okta on page 664
- Add the Secure Access SCIM Token and URL in the App
- Configure User Options in the App
- Assign Users or Groups in the App
- Push Users or Groups from the App to Secure Access
- View Logs in the App

Add the Cisco User Management Connector App in Okta

Provides instructions for completing the Add the Cisco User Management Connector App in Okta workflow in Cisco Secure Access. Navigate to Applications, and then select Create App Integration or Browser App Catalog.

Note that this connector app only supports SAML authentication in Okta.

Procedure

1. Navigate to **Applications**, and then select **Create App Integration** or **Browser App Catalog**.
2. Select the **Cisco User Management Connector** app, and then click **Add Integration**.
3. Click **Done**.

Enable In-App SAML SSO for the Cisco Management Connector in Okta

Provides instructions for completing the Enable In-App SAML SSO for the Cisco Management Connector in Okta workflow in Cisco Secure Access. You must already add a Cisco User Management Connector integration on the Okta portal.

Use the following procedure to use SAML SSO (single-sign on) in Okta to streamline provisioning and authentication for new users or small deployments.

Before you begin

You **must** already add a **Cisco User Management Connector** integration on the Okta portal.

Procedure

1. In the Okta app, select the **Sign on** tab.
2. Ensure the **SAML 2.0** toggle is enabled. Once enabled, scroll to the **Advanced Sign-on Settings** section of the window and take note of the ACS URL and your ENTITY ID.

   Note

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. This is applicable to both SAML options in Okta. For more information see Configure the Cisco User Management Connector App in Okta on page 662.

   For Cisco Secure Access Control Server (ACS), the `EntityID` is **https://fg.id.sse.cisco.com/gw/auth/acs/response**.

3. (Optional) Click **Update now** to update the application username upon the "create and update" stage.
4. (Optional) Check the **Allow users to securely see their password** to streamline the SAML SSO process for users who may not know their credentials.
5. Complete the **Settings**
6. (Optional) At the top of the **Sign on methods** window, click **Configure profile mapping** to map provisioning usernames to organizational standards. For more information see App to OKta attribute mapping.

What to do next

Complete the rest of the settings for your application. We **strongly** recommend validating the sign-in and provisioning in a test group before you deploy a broad rollout.

Add the Secure Access SCIM Token and URL in the App

Provides instructions for completing the Add the Secure Access SCIM Token and URL in the App workflow in Cisco Secure Access. In this step of the procedure, add the access token and the provisioning URL for the Secure Access SCIM API.

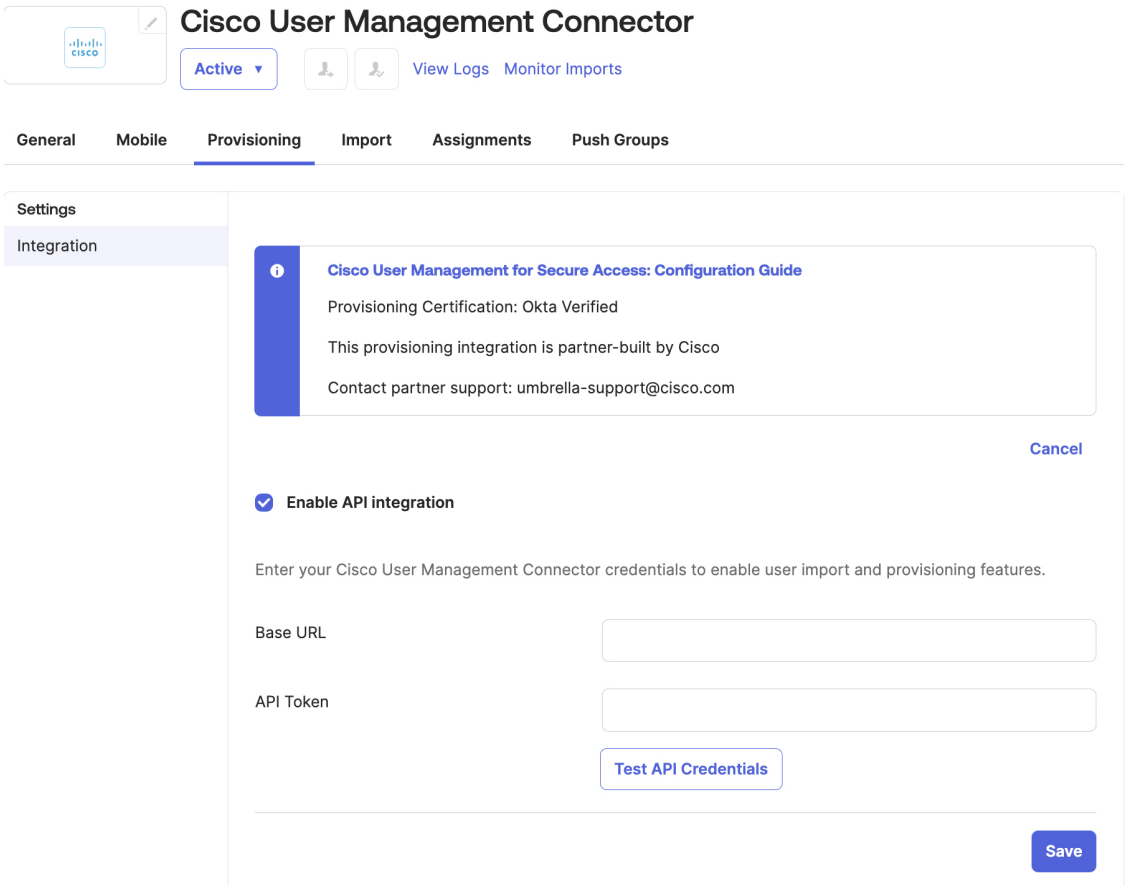
In this step of the procedure, add the access token and the provisioning URL for the Secure Access SCIM API. When you configure the cloud IdP in Secure Access, copy the access token and provisioning URL for the Secure Access SCIM API. For more information, see Add a Cloud Identity Provider.

Procedure

1. Click the **Provisioning** tab in the app.

2. Navigate to **Settings**, and then click **Integration**.
3. Click **Enable API Integration**.
4. For **Base URL**, enter the Secure Access provisioning URL for the SCIM API.

```
https://api.sse.cisco.com/identity/v2/scim
```



5. For **API Token**, enter the access token for the Secure Access SCIM API.
6. Click **Test API credentials**, to confirm that you can use your Secure Access SCIM token to connect the Secure Access API with Okta.
7. Click **Save**.

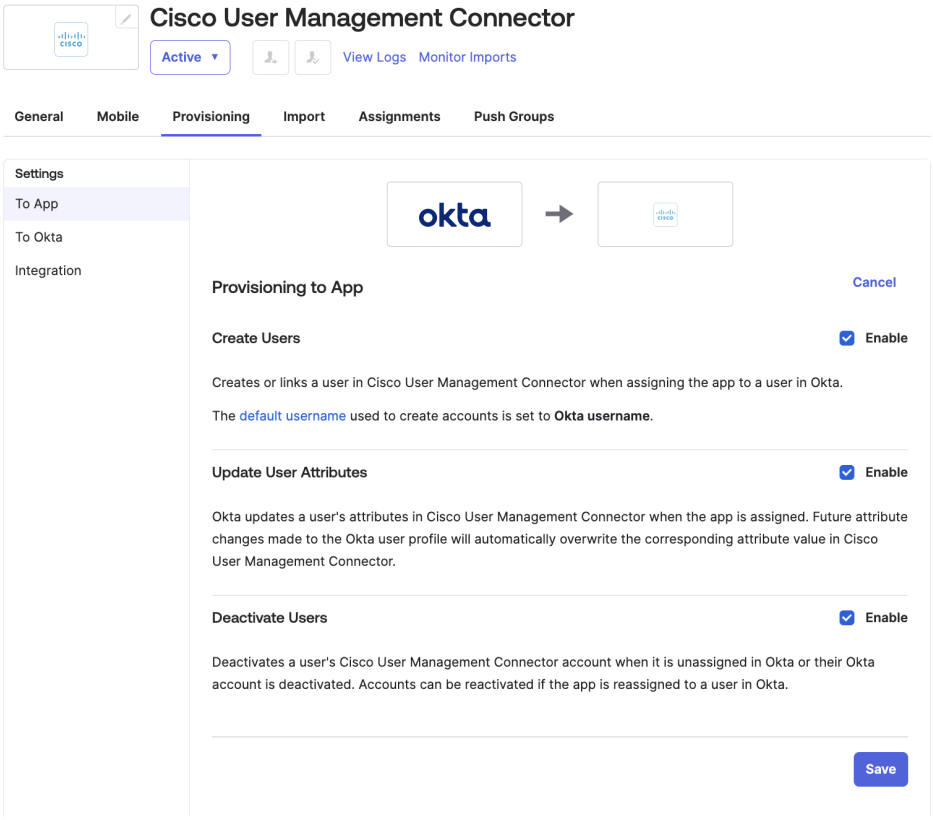
Configure User Options in the App

Provides instructions for completing the Configure User Options in the App workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

---

1. Click the **Provisioning** tab in the app.
2. Navigate to **Settings**, and then click **To App**.
3. Navigate to **Provisioning to App**.
4. Click edit, and then select these options: **Create Users**, **Update User Attributes**, and **Deactivate Users**.



5. Verify that you select these attributes for synchronization to Secure Access. Secure Access only lists the **Display name** and **Username** attributes for users, not the **Given name** and **Family name** attributes.
    - **Username**
    - **Given name**
    - **Family name**
    - **Display name**
    - **Email**
6. Click **Save**.

(Optional) Add an objectGUID Attribute and Create the User Profile Mapping

Describes (Optional) Add an objectGUID Attribute and Create the User Profile Mapping in Cisco Secure Access. If you need to import the objectGUID attribute for users, add a new attribute and map the attributes in the profile mapping.

If you need to import the `objectGUID` attribute for users, add a new attribute and map the attributes in the profile mapping.

The on-premises Secure Access AD Connector and the Cisco Secure Client rely on the `objectGUID` attribute for user and group identification. Ensure that the `objectGUID` attribute of users is synchronized from Okta to Secure Access only if either of the following conditions are true:

- You have previously imported AD users to Secure Access using the on-premises Secure Access AD connector, are now importing the same user identities from Okta, and want the previously imported identities to be persisted for policy or reporting purposes.
- You have endpoints that authenticate against on-premises AD and run the Cisco Secure Client.

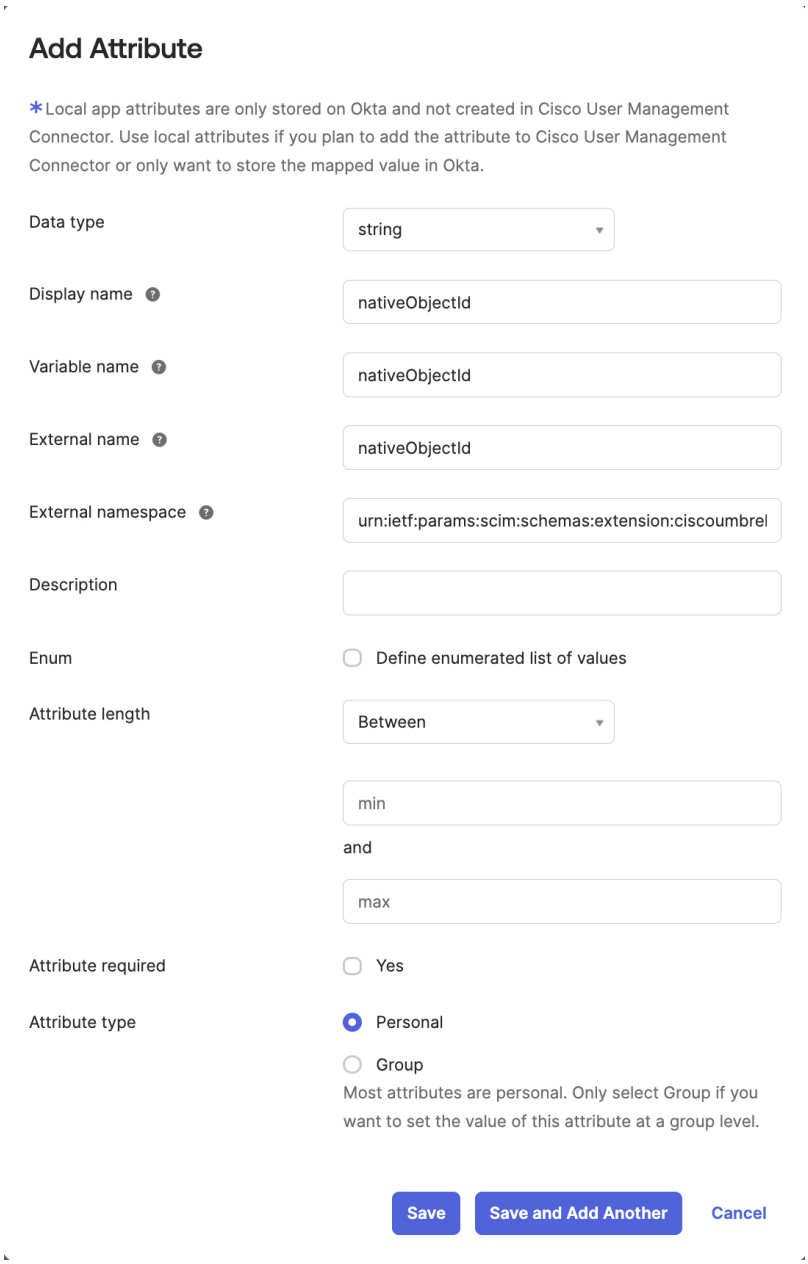
> **Note**
>
> The Okta Active Directory agent does not synchronize the `objectGUID` attribute of users from on-premises AD to Okta by default.

Add the objectGUID Attribute

Provides instructions for completing the Add the objectGUID Attribute workflow in Cisco Secure Access. In Okta, navigate to the Provisioning tab on the Cisco User Management Connector app.

Procedure

1. In Okta, navigate to the **Provisioning** tab on the **Cisco User Management Connector** app.
2. From **Settings** > **To App**, navigate to **Profile Editor**.



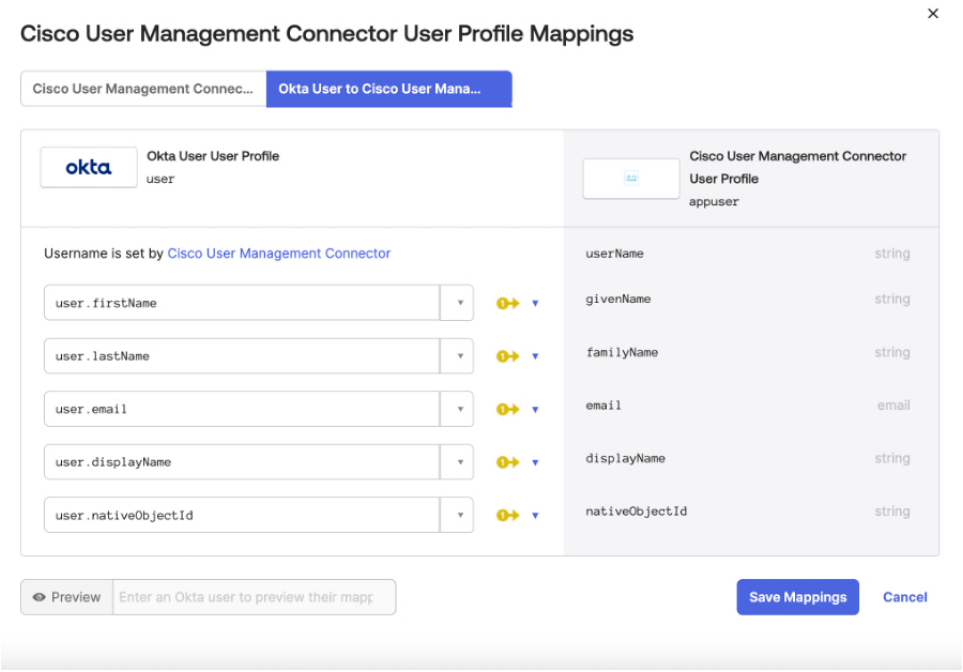
3. For **Okta Attribute Mappings**, click **Add Attribute** to create a custom attribute of string type called `objectGUID`.
   - Set **Display name**, **Variable name**, and **External name** to `native.ObjectId`.
   - For **Scope**, click **User personal**.
   - Set **External namespace** to `urn:ietf:params:scim:schemas:extension:ciscoumbrella:2.0:user`
4. Click **Save**.

Create the User Profile Mappings

Provides instructions for completing the Create the User Profile Mappings workflow in Cisco Secure Access. In Okta, navigate to the Provisioning tab on the Cisco User Management Connector app.

Procedure

1. In Okta, navigate to the **Provisioning** tab on the **Cisco User Management Connector** app.
2. From **Settings > To App**, navigate to **Profile Editor**.
3. For **Cisco User Management Connector User Profile Mappings**, create a new Okta User Profile that maps the Okta user to the **Cisco User Management Connector** user. The profile must map the `user.objectGUID` to `nativeObjectId`.
4. Click **Save Mappings**.
5. Select the option to **Apply the Mappings to All Users with this Profile**.



Customize the authName Attribute

Provides instructions for completing the Customize the authName Attribute workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

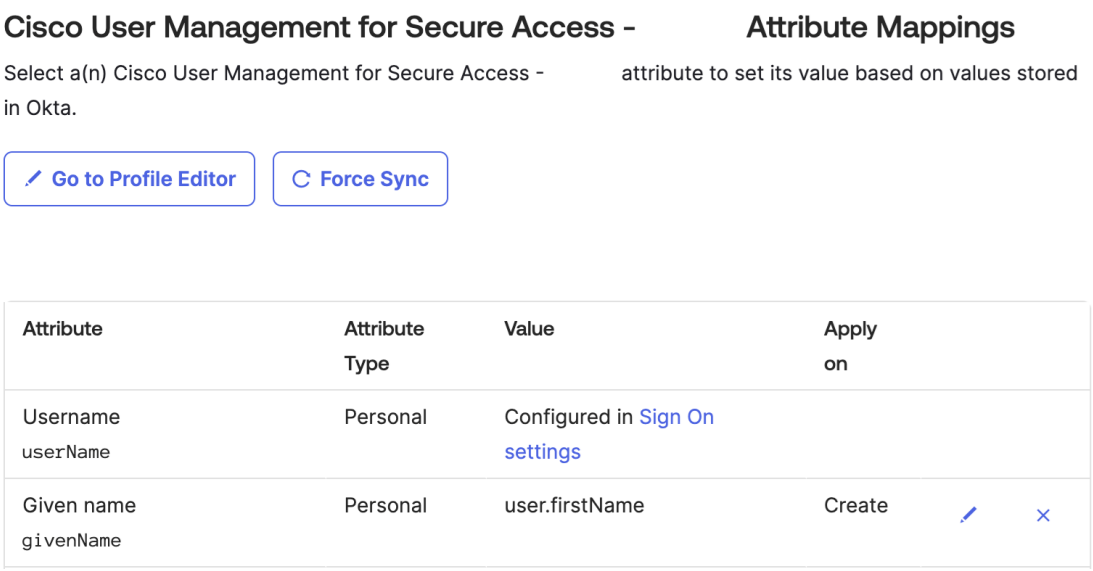
To use an attribute to authenticate users in addition to the user principal name (UPN) attribute, customize the authName attribute and map it to a user profile (such as employee email or ID).

Before you begin

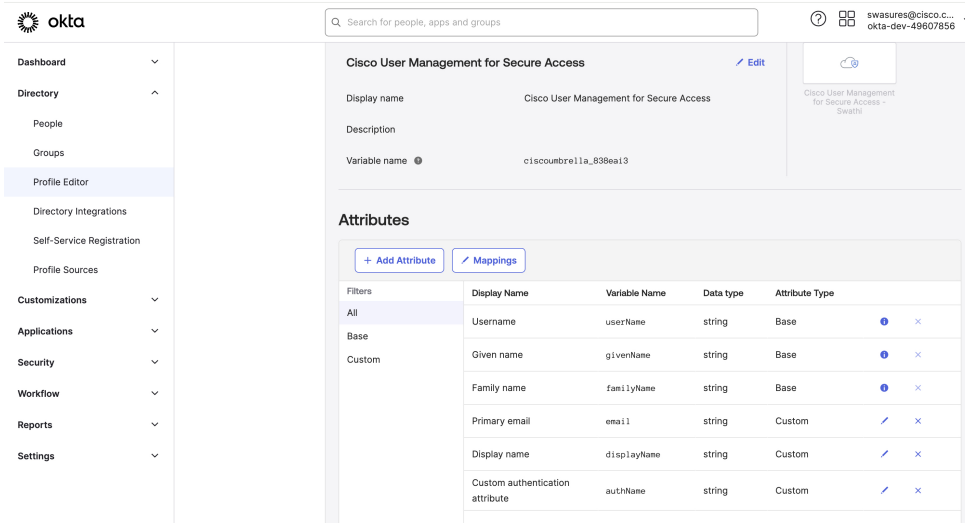
Authorize the use of the authName attribute. For more information, see Set Up Authentication Preferences for Identity Providers.

Procedure

1. In Okta, open the **Cisco User Management for Secure Access** app.
2. Navigate to the **Provisioning** tab.
3. Navigate to **Cisco User Management Connector for Secure Access - Attribute Mappings**.
4. Click **Go to Profile Editor**.

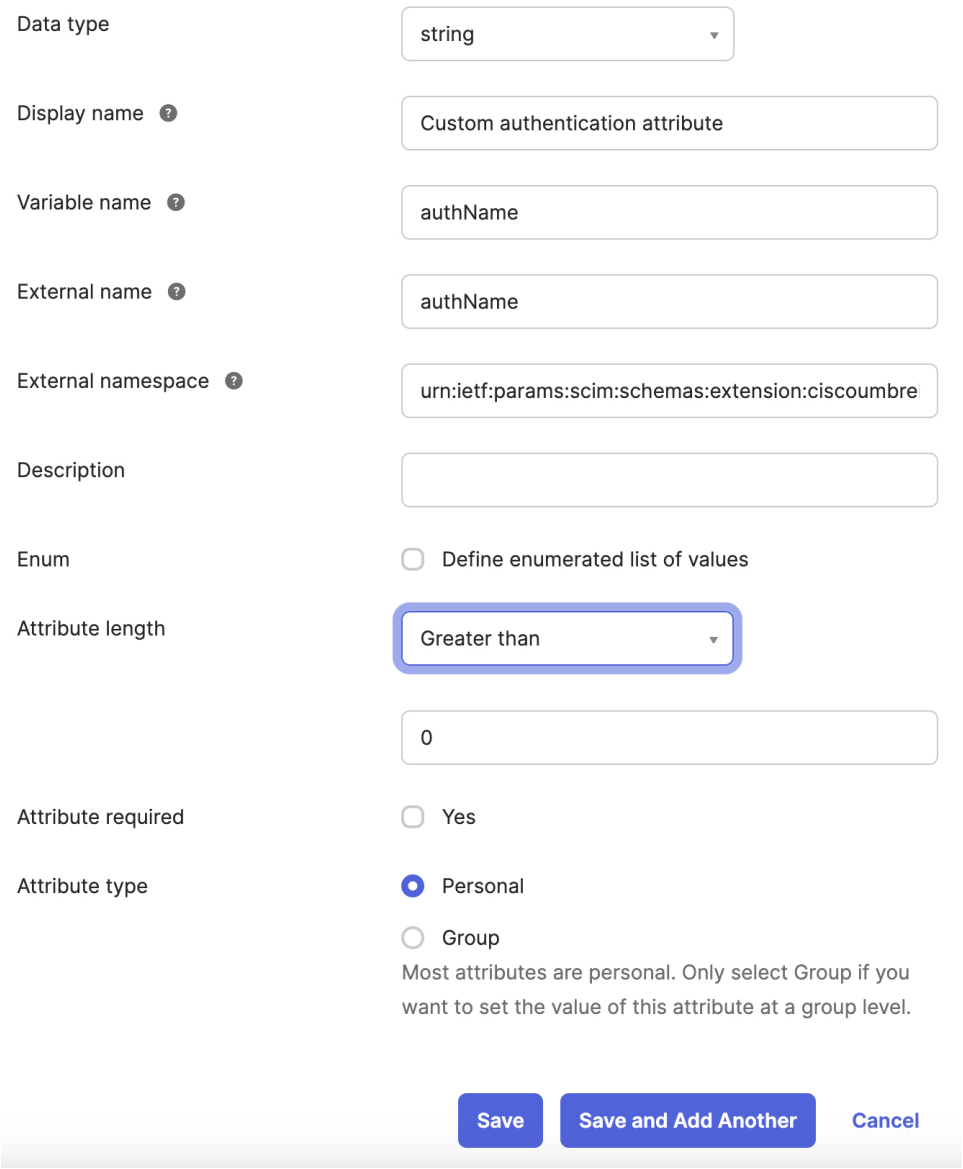


5. On the **Profile Editor** page, scroll down to the **Cisco User Management for Secure Access** section.
6. In the **Attributes** section, click **Add Attribute**.



7. In the **Custom attribute** window, complete the following fields:
   - **Data type**–Choose **string**.
   - **Display name**–Type **Custom authentication attribute**.
   - **Variable name**–Type **authName**.
   - **External name**–Type **authName**.
   - **External namespace**–Select**urn:ietf:params:scim:schemas:extension:ciscoumbrella:2.0:User**.
   - **Description**–(Optional) Enter a description for your unique authentication attribute.
   - **Enum**–Leave **Define enumerated list of values** unchecked.
   - **Attribute length**–Choose **Greater than**.
   - **Min value**–Enter a number of characters for the unique authentication attribute.
   - **Attribute required**–Click **Yes** if you want all users to be authenticated with the unique authName attribute.

- **Attribute type**–Click the **Personal** radio button.



8. Click **Save**.

Map the Custom authName Attribute to a User Profile

Provides instructions for completing the Map the Custom authName Attribute to a User Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

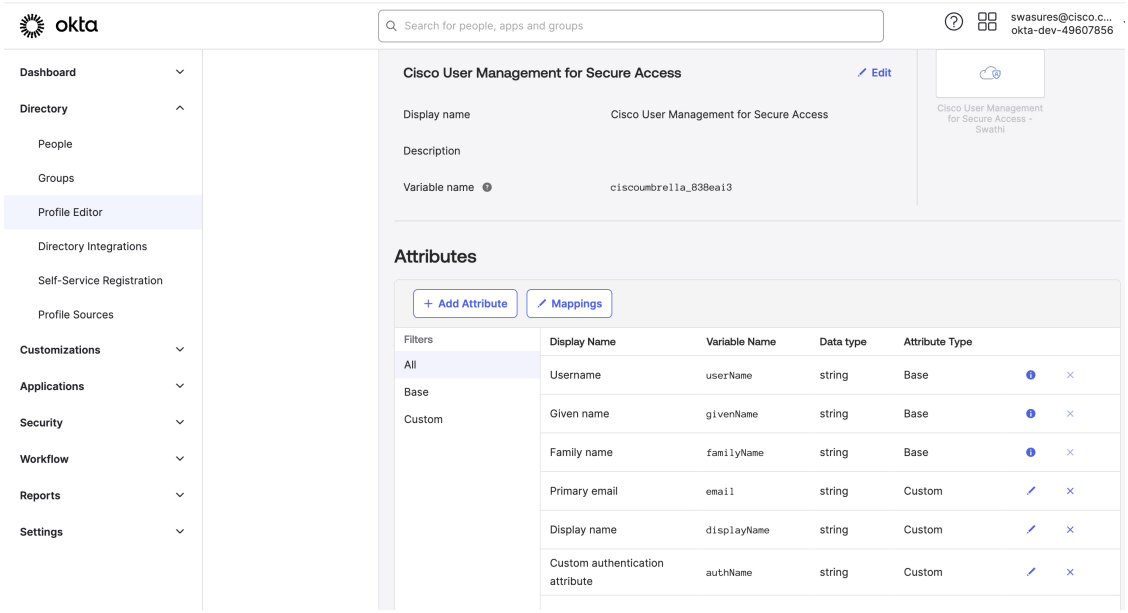
To use an attribute to authenticate users in addition to the user principal name (UPN) attribute, customize the authName attribute and map it to a user profile (such as employee email or ID).

Before you begin

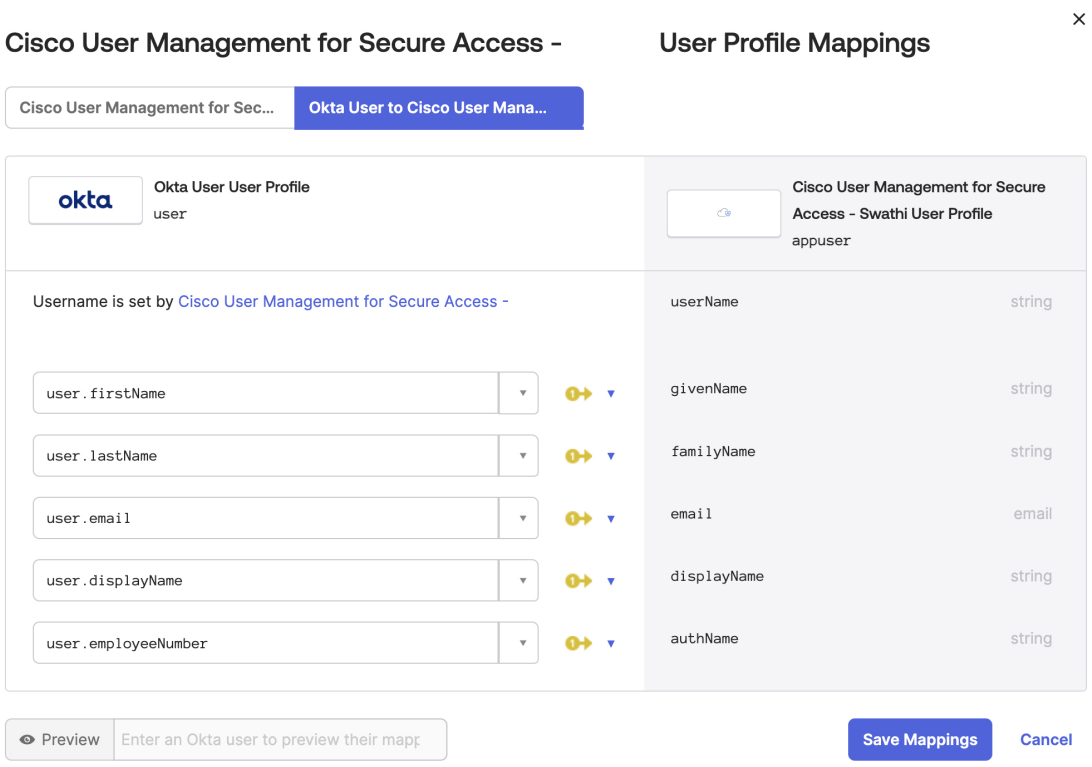
Authorize the use of the authName attribute. For more information, see Set Up Authentication Preferences for Identity Providers.

Procedure

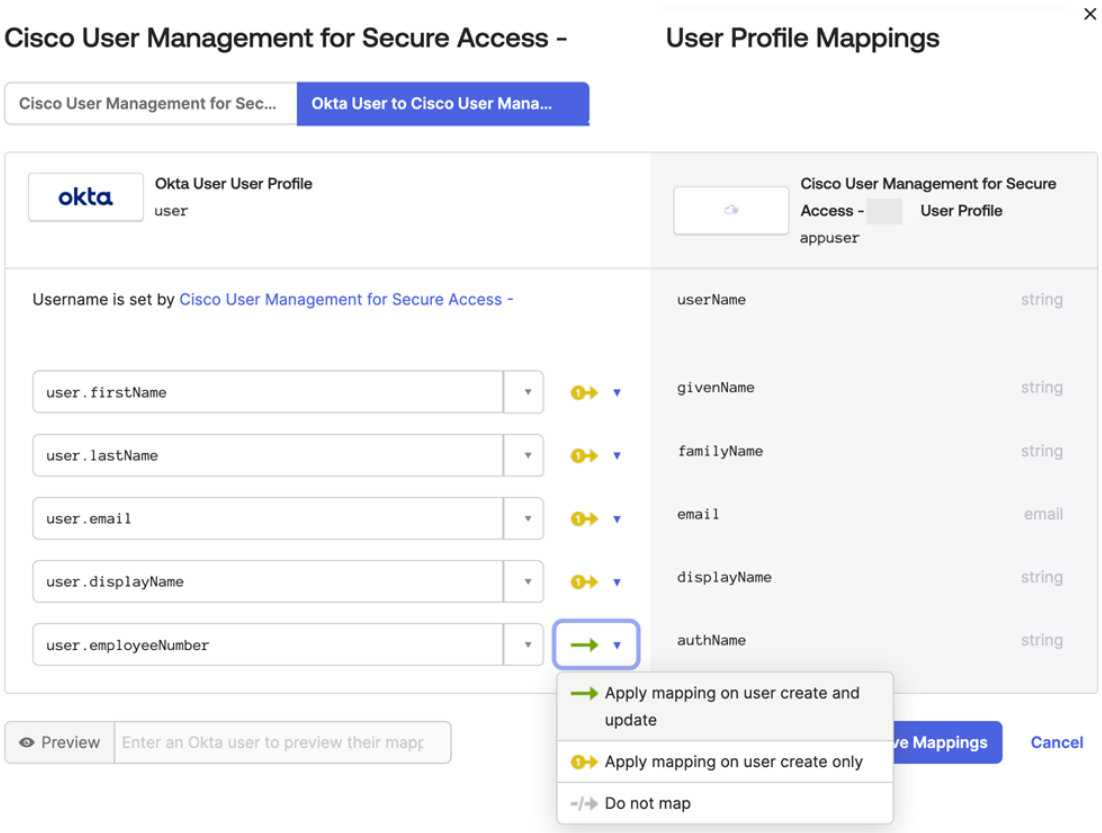
1. In the left pane, select **Profile Editor**.
2. In the **Attributes** section, click **Mappings**.



3. On the **Cisco User Management for Secure Access - User Profile Mappings** page, click **Okta User to Cisco Umbrella User Management Connector**.



4. In the left pane for the user profile, click the yellow arrow and select **Apply mapping on user create and update**.



5. Click **Save Mappings**.

Assign Users or Groups in the App

Provides instructions for completing the Assign Users or Groups in the App workflow in Cisco Secure Access. After you add users and groups in Okta, you can assign these users and groups in the Cisco User Management Connector app.

After you add users and groups in Okta, you can assign these users and groups in the **Cisco User Management Connector** app.

> **Note**
>
> Once users and groups are assigned, the app begins to provision the selected users to Secure Access. Wait for all users to show up in Secure Access before starting to push groups. The amount of time that syncing groups and provisioning users with Secure Access depends upon the number of users provisioned. We recommend that you confirm that all users selected provision from Okta to Secure Access.

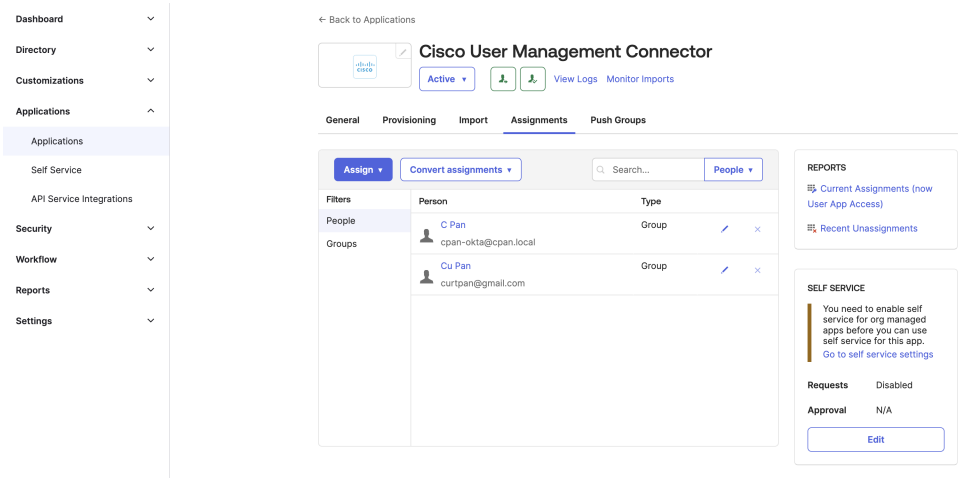
Procedure

1. Click the **Assignments** tab in the app.
2. Assign users and groups in the app.

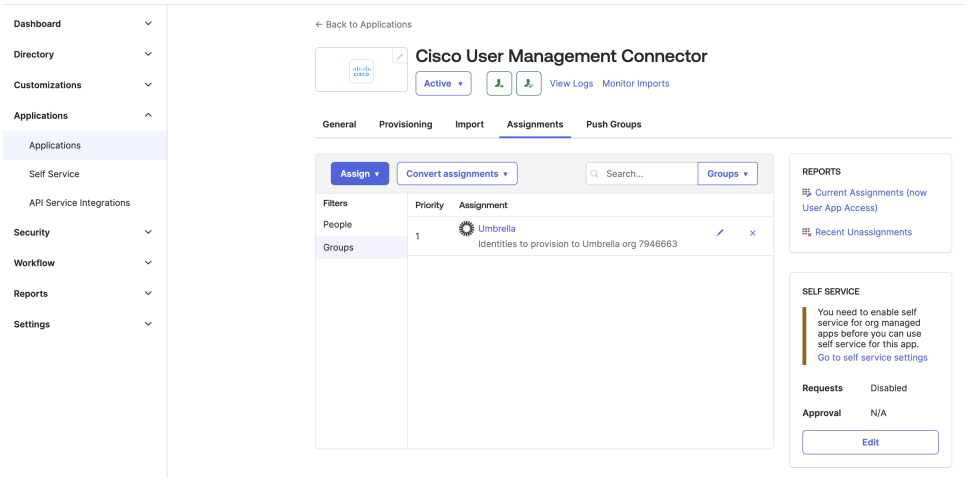
> **Note**
>
> Assigning groups to the app does not provision these groups to Secure Access. Okta only provisions users that are members of the assigned groups. Do not manually change the value of the `nativeObjectId` field when assigning any groups and users.

a) Navigate to **People**, and then click **Assign**.

(Optional) To assign all users, assign the **Everyone** group to the app.



b) Navigate to **Groups**, and then click **Assign**.

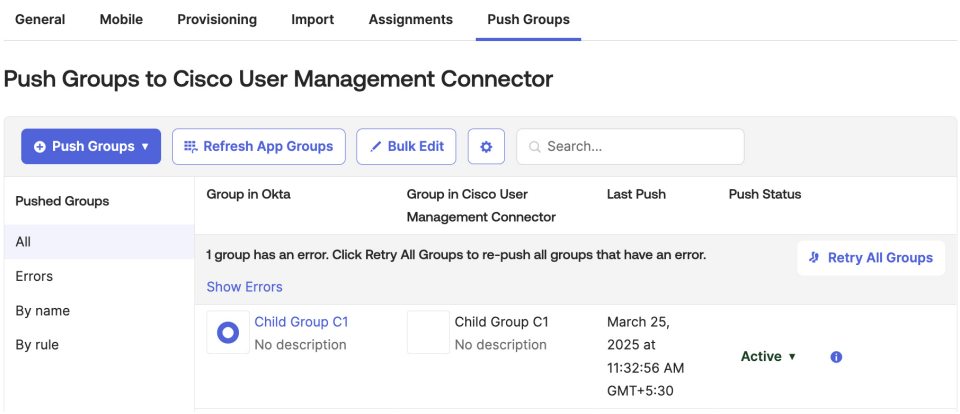


Push Users or Groups from the App to Secure Access

Provides instructions for completing the Push Users or Groups from the App to Secure Access workflow in Cisco Secure Access. Click the Push Groups tab in the app.

Procedure

1. Click the **Push Groups** tab in the app.

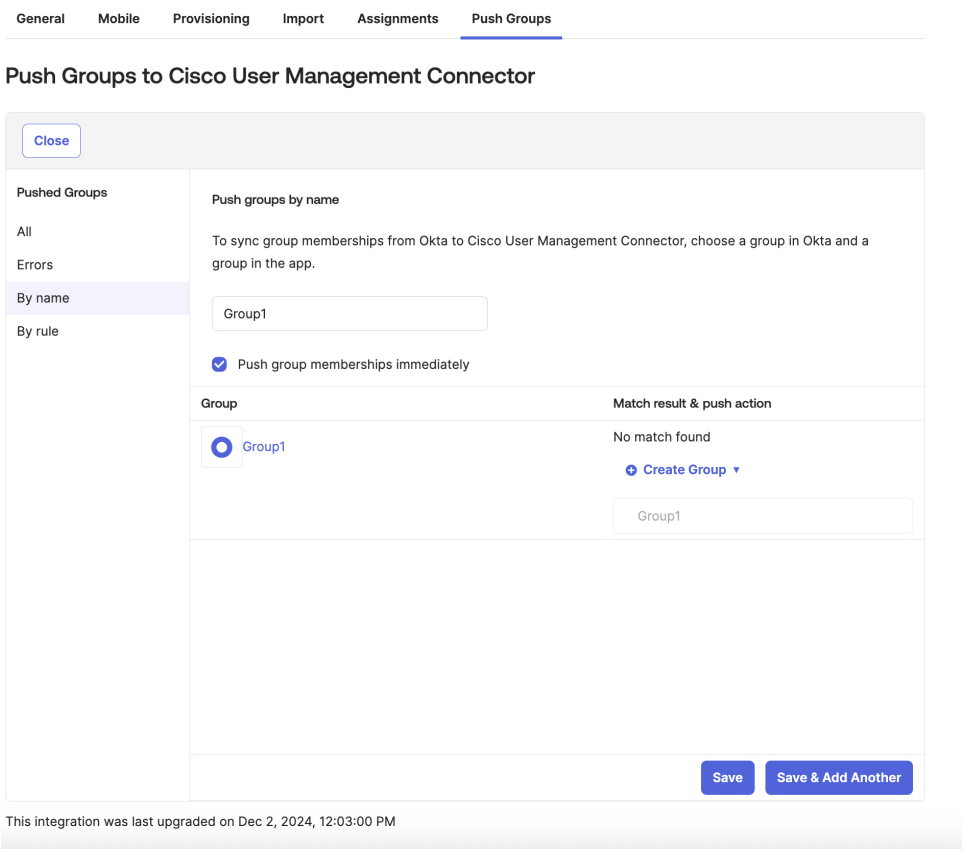


2. Sync specific groups to Secure Access.

> **Note**
>
> Pushing a group from Okta provisions the group in Secure Access only, and does not sync any users.

If you push a group from Okta to Secure Access and the group includes users, then the app adds to the group in Secure Access any users assigned to the Okta app directly or in a group.

> **Note**
>
> Okta does not recommend pushing groups that are assigned to the app. If you have assigned the **Everyone** group to the app, you should not push the same group.



3. Click **Save** or **Save & Add Another**.

View Logs in the App

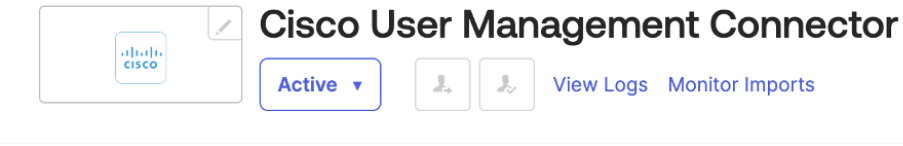
Provides instructions for completing the View Logs in the App workflow in Cisco Secure Access. From the Cisco User Management Connector app in your instance of Okta, view the provisioning logs.

From the **Cisco User Management Connector** app in your instance of Okta, view the provisioning logs.

Procedure

Navigate to **View Logs** on the **Cisco User Management Connector** app in Okta.

The app displays the progress of the provisioning.



Provision Users and Groups from Microsoft Entra ID

Describes Provision Users and Groups from Microsoft Entra ID in Cisco Secure Access. Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory).

Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory).

With your Secure Access System for Cross-domain Identity Management (SCIM) token, configure the **Cisco User Management for Secure Access** app on the Microsoft Enter ID portal. When you configure and provision users and groups through the app, Microsoft Entra ID exchanges user and group information with Secure Access.

Note

You do not need to deploy an on-premises Cisco Active Directory (AD) Connector.

Limitations

- You can provision a maximum of 1000 groups from Microsoft Entra ID to Secure Access. Secure Access supports the provisioning of an unlimited number of users from Microsoft Entra ID. For more information, see Limitations and Range Limits.
- Concurrent synchronization of the same users and groups from the Cisco AD Connector and the Cisco User Management for Secure Access app is not supported and leads to inconsistent access rule enforcement.
- To ensure that all users are provisioned, create a dynamic **All Users** group and assign this group to the Cisco User Management for Secure Access app. For more information, see Dynamic Membership Rules for Groups in Azure Active Directory. You can assign additional groups as required for group-based access rule enforcement.
- Guest users invited to your Microsoft Entra ID tenant are provisioned to the same Secure Access user group as all other users provisioned by Microsoft Entra ID. Since members of the same user group inherit the same access rules in Secure Access, this may result in your Entra ID guest users gaining access to resources intended only for your Entra ID member users.
- Provisioning large numbers of users and groups to Secure Access may take several hours.
- Microsoft Entra ID does not support nested group memberships for group-based assignment to any SaaS application.
- After the initial provisioning of users and groups, Microsoft Entra ID synchronizes changes to Secure Access once every 40 minutes. Synchronization of updates to identities from Microsoft Entra ID to Secure Access may take up to one hour.

Refresh SCIM Token

We recommend that you refresh the SCIM token at least once every 90 days. Secure Access requires a valid SCIM token to provision the users and groups from Microsoft Entra ID to Secure Access.

After you generate a new SCIM token, immediately copy the token to the **Cisco User Management for Secure Access** app in Microsoft Entra ID.

For information about refreshing the SCIM token, see Add a Cloud Identity Provider.

> **Note**
>
> The administrators in the Secure Access organization are responsible for refreshing the SCIM token. Secure Access does not perform this action.

Supported Attributes for Users

Cisco Attributes for Users	Microsoft Entra ID Attributes
userName	userPrincipalName
active	Not([IsSoftDeleted])
displayName	displayName
name.givenName	givenName
name.familyName	surname
name.formatted	Join(" ", [givenName], [surname])
externalId	objectId

Supported Attributes for Groups

Cisco Attributes for Groups	Microsoft Entra ID Attributes
displayName	displayName
externalId	objectId
members	members

Configure Provisioning in Microsoft Entra ID

Provides instructions for completing the Configure Provisioning in Microsoft Entra ID workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

With your Secure Access SCIM token and API Identity URL, set up the Cisco User Management for Secure Access app on Microsoft Entra ID and provision users and groups.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A valid Microsoft Entra ID subscription with a premium Microsoft Entra ID license.
- Add the IdP in Secure Access and generate a valid SCIM token. For more information, see Add a Cloud Identity Provider.
- No concurrent provisioning of the same users or groups from on-premises AD or Microsoft Entra ID. If you are using the on-premises Cisco AD Connector to import users and groups and choose to import the same users and groups from Microsoft Entra ID, ensure that the on-premises Cisco AD Connector is switched off or that the Cisco AD Connector service on the connector machine is stopped.
- For IP-to-user mapping deployments, you must use the on-premises Cisco AD Connector. Microsoft Entra ID does not store the private IP to Active AD user mappings.

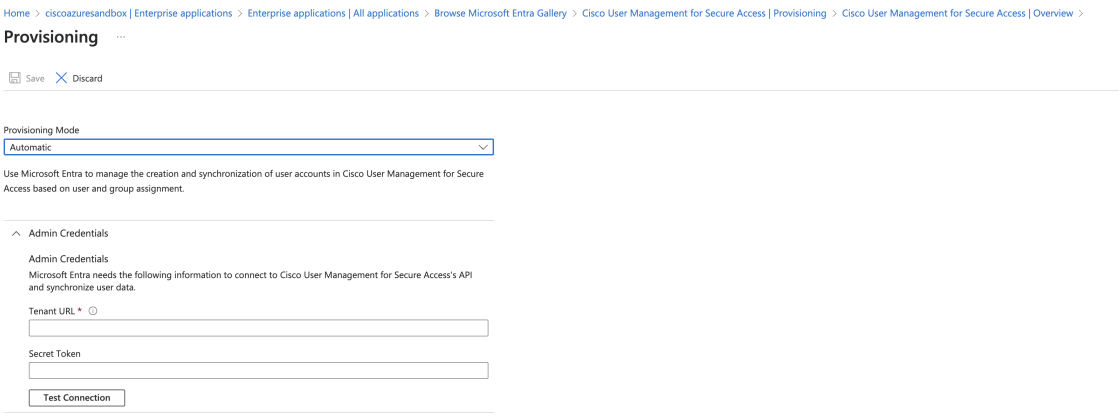
- Import the `ObjectGUID` attribute from Microsoft Entra ID to Secure Access. The on-premises Cisco AD Connector and Cisco Secure Client rely on the `ObjectGUID` attribute for user identification. If all of your endpoints have the Cisco Secure Client deployed, you do not have to import the `ObjectGUID` attribute from Microsoft Entra ID.
  - Before you set up the import of the `ObjectGUID` attribute, ensure that the on-premises Cisco AD Connector that is synchronizing these identities is switched off or that the Cisco Connector service on the connector machine is stopped.
  - To ensure that the `ObjectGUID` attribute for users is synchronized from Microsoft Entra ID to Secure Access, your endpoints must authenticate against on-premises AD and run the Cisco Secure Client. For more information about importing the `ObjectGUID` attribute for users, see Tutorial: Configure Cisco Secure Access User Management for automatic user provisioning.
- If you previously configured access rules that included groups imported from on-premises AD, and then choose to import the same groups from Microsoft Entra ID, you must reconfigure the access rules to map the Microsoft Entra ID groups instead of the on-premises AD groups. In an access rule, on-premises AD group names are displayed with the domain name preceding the group name, for example: **Domain1\ADGroup1**. For Microsoft Entra ID, only group names are displayed, for example: **ADGroup1**.

Procedure

1. In Microsoft Entra ID, navigate to the **Cisco User Management for Secure Access**app.



2. Add your Secure Access SCIM API token to the **Secret Token** field.
3. Add the Secure Access API Identity URL to the **Tenant URL** field.
4. Click **Test Connection** to confirm that you can use your Secure Access SCIM token to connect the Secure Access API with Microsoft Entra ID.



5. Complete the steps to provision users from Microsoft Entra ID to Secure Access. For more information, see Tutorial: Configure Cisco Secure Access User Management for automatic user provisioning.

   Review the user attributes that are synchronized from Microsoft Entra ID to the Cisco User Management for Secure Access app in **Attribute Mappings**. The attributes selected as **Matching** properties are used to match the user accounts in Cisco User Management for Secure Access app for update operations. If you choose to change the matching target attribute, ensure that the Cisco User Management for Secure Access app supports filtering users based on that attribute.

6. Click **Save**.

Configure Guest Users

Provides instructions for completing the Configure Guest Users workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To provision a guest user from Microsoft Entra ID to Secure Access, sign into the Cisco User Management for Secure app in Microsoft Entra ID and associate the Cisco **userName** attribute with the Microsoft Entra ID **originalUserPrincipalName** attribute.

Before you begin

You must have the following configured before you add a guest user to your Entra ID SAML application:

- Full Admin user role. For more information, see Manage Accounts.
- Add your Secure Access organization to your Entra ID account. For more information see Add an enterprise application to your external tenant.
- Register the SAML application with Secure Access. For more information, see Register a SAML app in your external tenant.
- A valid Microsoft Entra ID subscription with a premium Microsoft Entra ID license.
- Add the IdP in Secure Access and generate a valid SCIM token. For more information, see Add a Cloud Identity Provider.
- Import the `ObjectGUID` attribute from Microsoft Entra ID to Secure Access. The on-premises Cisco AD Connector and Cisco Secure Client rely on the `ObjectGUID` attribute for user identification. If all of your endpoints have the Cisco Secure Client deployed, you do not have to import the `ObjectGUID` attribute from Microsoft Entra ID.
  - Before you set up the import of the `ObjectGUID` attribute, ensure that the on-premises Cisco AD Connector that is synchronizing these identities is switched off or that the Cisco Connector service on the connector machine is stopped.
  - To ensure that the `ObjectGUID` attribute for users is synchronized from Microsoft Entra ID to Secure Access, your endpoints must authenticate against on-premises AD and run the Cisco Secure Client. For more information about importing the `ObjectGUID` attribute for users, see Tutorial: Configure Cisco Secure Access User Management for automatic user provisioning.

Limitations and Guidelines

Review the following recommended use cases and limitations to keep in mind as you add a guest user to your Entra ID:

- For IP-to-user mapping deployments, you must use the on-premises Cisco AD Connector. Microsoft Entra ID does not store the private IP to Active AD user mappings.
- No concurrent provisioning of the same users or groups from on-premises AD or Microsoft Entra ID. If you are using the on-premises Cisco AD Connector to import users and groups and choose to import the same users and groups from Microsoft Entra ID, ensure that the on-premises Cisco AD Connector is switched off or that the Cisco AD Connector service on the connector machine is stopped.
- If you previously configured access rules that included groups imported from on-premises AD, and then choose to import the same groups from Microsoft Entra ID, you must reconfigure the access rules to map the Microsoft Entra ID groups instead of the on-premises AD groups. In an access rule, on-premises AD group names are displayed with the domain name preceding the group name, for example: **Domain1\ADGroup1**. For Microsoft Entra ID, only group names are displayed, for example: **ADGroup1**.

Procedure

1. Complete the prereuqisites listed above.
2. In your SAML application, navigate to the **Cisco User Management for Secure Access** app.
3. Navigate to the **Attribute Mappings** of your SAML app.
4. Click **Add New Mapping**.
5. Add a mapping for the source attribute with the following conditions. For more information, see Emit claims based on conditions:
   - For the User Type **Any**, map the **userName** (or **source**) value to **user.userprincipalname**.
   - For the User Type **External** user, map the **userName** (or **source**) value to **user.mail**
6. Click **Save**.

22 Provision Users, Groups, and Endpoint Devices from Active Directory

Topics:

- Provision Users, Groups, and Endpoint Devices from Active Directory
- Manage AD Connectors
- Edit AD Authentication Properties
- Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications
- AD Integration with Virtual Appliances

Provides an overview of Provision Users, Groups, and Endpoint Devices from Active Directory in Cisco Secure Access, including Provision Users, Groups, and Endpoint Devices from Active Directory, Manage AD Connectors, and Edit AD Authentication Properties. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Provision Users, Groups, and Endpoint Devices from Active Directory

Describes Provision Users, Groups, and Endpoint Devices from Active Directory in Cisco Secure Access. Provisioning users, groups, and endpoint devices from Active Directory (AD) to Cisco Secure Access requires the deployment of a Cisco AD Connector in your environment.

Provisioning users, groups, and endpoint devices from Active Directory (AD) to Cisco Secure Access requires the deployment of a Cisco AD Connector in your environment. The AD Connector securely retrieves non-sensitive user, group, and device information from your instance of Microsoft AD and integrates the identities with Secure Access. Once your users, groups, and devices are provisioned in Secure Access, you can create and enforce AD group or device-based Access rules and view AD user-based reports.

Next Steps

1. Review the requirements for setting up the AD components and Cisco AD Connector in your environment. For more information, see Prerequisites for AD Connectors.
2. Review how to connect multiple AD domains. For more information, see Connect Multiple Active Directory Domains.
3. Manage the AD components with Secure Access. For more information, see Manage AD Components.
4. Manage the AD Connectors. For more information, see Manage AD Connectors.
5. View the installed AD components. For more information, see View AD Components in Secure Access.
6. Enable or disable DLP email notifications for reporting managers. For more information, see Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications.
7. Troubleshoot the AD deployments. For more information, see AD Connector Communication Flow and Troubleshooting.

Prerequisites for AD Connectors

Describes Prerequisites for AD Connectors in Cisco Secure Access. To integrate your organization's identities from Microsoft Active Directory (AD) with Cisco Secure Access, deploy the Cisco AD Connector in your environment.

To integrate your organization's identities from Microsoft Active Directory (AD) with Cisco Secure Access, deploy the Cisco AD Connector in your environment.

This guide describes the Windows Server, user account in the AD domain, and network requirements to deploy the AD Connector. You must meet these requirements before you deploy the AD Connector.

Connector Server

You must configure a server that is a member of the AD domain with the following environment:

- Windows Server 2016, 2019, 2022, or 2025.
- 100MB free hard disk drive space.
- .NET Framework 4.5 or above.
- If a local anti-virus application is running, allow the **CiscoAuditClient.exe** and **CiscoAuditService.exe** processes to run on the system.

You can deploy the AD Connector directly on the domain controller. In this case, the domain controller must meet all prerequisites for the Connector server. Only one AD Connector is required to provision identities from an AD domain. If you require high-availability of the AD Connector, deploy a second AD Connector.

Outbound Network Access to Secure Access

The server where you install the AD Connector requires outbound access on certain domains and URLs. If you are using a transparent HTTP web proxy, ensure that these domains and URLs on port 80/443 are excluded from the proxy, and not subject to authentication.

- For syncing, allow traffic on 443 (TCP) to **api.sse.cisco.com**.
- For Windows to perform Certificate Revocation List and Code-Signing checks, allow access to additional URLs on port 80/443 (TCP). For a complete list of ports, see AD Connector Communication Flow and Troubleshooting.
- For downloading upgrades, allow traffic on 443 (TCP) to **disthost.umbrella.com**.

Connector Account

To deploy the AD Connector, create a new user account in the AD domain. This account should have:

- The logon name (**sAMAccountName**) set to **Cisco_Connector**. You can use a custom username, but you must configure it with the required permissions.
- Select **Password never expires**.

> **Note**
>
> Passwords can not include backslashes, quotations (single or double), greater-than or less-than chevron brackets (**< >**), or colons.

- Assign **Read** and **Replicating Directory Changes** permissions. Alternatively, you can make the AD Connector account a member of the built-in **Enterprise Read-only Domain Controllers** group, which will automatically assign these permissions.
  - The AD Connector does an initial synchronization of the AD structure to Secure Access. After this, it detects changes to the AD structure and communicates these changes only. The detection of changes requires the **Replicating Directory Changes** permission. The AD Connector cannot function without this permission.
  - The **Replicating Directory Changes** permission is different from the **Replicating Directory Changes All** permission, which enables the retrieval of password hashes. The AD Connector does not read password hashes. Thus, the AD Connector does not require the **Replicating Directory Changes All** permission.

Connect Multiple Active Directory Domains

Describes Connect Multiple Active Directory Domains in Cisco Secure Access. To import users, groups, and endpoint devices from multiple Active Directory (AD) domains or multiple AD forests, register a domain controller or domain in Cisco Secure Access for each AD domain that needs to integrate with Secure Access.

To import users, groups, and endpoint devices from multiple Active Directory (AD) domains or multiple AD forests, register a domain controller or domain in Cisco Secure Access for each AD domain that needs to integrate with Secure Access. We recommend that you deploy a separate Cisco AD Connector for each AD domain. For more information, see Welcome to Cisco Secure Access.

If you wish to use the same Cisco AD Connector to provision users and groups from multiple AD domains, ensure that the connector account is created with the same **sAMAccountName** name and password across all of your domains.

This feature is not enabled by default. Contact Support to have the feature enabled. For more information, see Welcome to Cisco Secure Access.

> **Note**
>
> If you have groups in an AD domain that have member users in another AD domain, Secure Access requires that you deploy a single Cisco AD Connector for multiple AD domains

Active Directory Components

Active Directory (AD) components—AD domains, domain controllers, and AD Connectors—integrate Cisco Secure Access with Microsoft Active Directory so you can authenticate users and apply identity-based policies.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with Microsoft Active Directory. After you add AD domains, domain controllers, and AD Connectors in Secure Access, you can view component details, assign load-balancing groups, edit site associations, and delete AD components.

Use the following topics to manage AD components in Secure Access:

- Add AD components
- View AD components
- Assign a load-balancing group to AD components
- Edit sites for AD components
- Delete AD components

Add AD Components

Add AD domains or domain controllers in Secure Access to integrate Microsoft Active Directory with the Cisco AD Connector.

To integrate Microsoft Active Directory with Cisco Secure Access, add AD domains or domain controllers in Secure Access and configure communication with the Cisco AD Connector.

To add a domain controller, first complete Verify Auditing of Logon Events on Domain Controllers, Download the Windows Configuration Script for Domain Controllers, and Run the Windows Configuration Script for the Domain Controllers. Then see Add a Domain Controller.

To add a domain, see Add a Domain.

Support for Multiple AD Domains and Forests

To integrate multiple AD domains or AD forests with Secure Access through domain controller integrations, deploy one AD Connector for each AD domain. For redundancy, deploy an additional AD Connector for each AD domain.

Verify Auditing of Logon Events on Domain Controllers

Describes Verify Auditing of Logon Events on Domain Controllers in Cisco Secure Access. The AD integration with domain controllers requires each domain controller to audit logon events.

The AD integration with domain controllers requires each domain controller to audit logon events.

On each domain controller (excluding read-only domain controllers), enable the **Audit account logon events** to include `Success` and `Failure` if it is set to `No Auditing`.

By default, this group policy is set to log `Success` logon events and you should not modify it. Secure Access requires the **Audit account logon events** setting so that it knows whether a user has logged in successfully and can then compare that login to subsequent events generated by that user.

If the Audit Policy is not set, the **Windows Configuration Script for Domain Controller** script displays this error message:

```
"ERROR: "



--------------------------------------------------------------------------------


Your Group Policy for this Domain Controller is set to NOT audit successful
logon events!

You MUST edit the following Group Policy for all DCs:



Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events



Define that policy to audit Success attempts, gpupdate, and re-run this script!
```

Download the Windows Configuration Script for Domain Controllers

Provides instructions for completing the Download the Windows Configuration Script for Domain Controllers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Windows Configuration Script automates the permissions for the **Cisco_Connector** user.

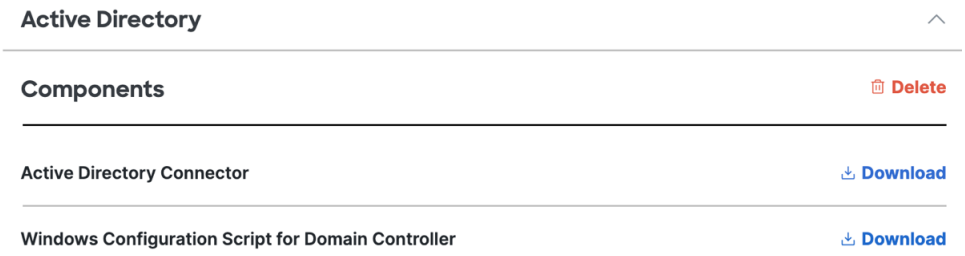
In Secure Access, download the **Windows Configuration Script for Domain Controller** script to the domain controllers in your environments.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. After an initial AD deployment, navigate to **Connect > Users and Groups > Users**, click **Configuration Management**, and expand **Active Directory**.
3. For **Windows Configuration Script for Domain Controller**, click **Download**.



4. Download and save the configuration script to a location on the machine where you plan to run it.

> **Note**
>
> The configuration script is written in Visual Basic Script and is in plain text.

Run the Windows Configuration Script for the Domain Controllers

Provides instructions for completing the Run the Windows Configuration Script for the Domain Controllers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Run the **Windows Configuration Script for Domain Controller** on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) for each domain that will integrate with Secure Access. The configuration script prepares the domain controllers to communicate with the AD Connector.

Before running the script, you must create the **Cisco_Connector** user. Also, there are several Group Policies that affect system operation that may need manual configuration. The script displays the status of these settings and, if needed, provides instructions on how to change them.

Repeat the steps to add your domain controllers in Secure Access. It is essential that each domain controller in each AD domain environment has the configuration script run on it in order for the service to work as expected, both for high availability and overall reliability.

> **Note**
>
> The configuration script is not an application or service. If you change the IP address or hostname of the domain controller, remove the previous instance of the domain controller and re-register the domain controller.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. As an administrator, open an elevated command prompt.
2. Locate the **Windows Configuration Script for Domain Controller** file and run the script in the command prompt.
3. Substitute the Windows configuration script filename (including the **.wsf** file extension) in the **cscript** command.

```
cscript forcenonva=true <Windows Configuration Script filename with extension>
 or cscript forcenonva=true <Windows Configuration Script filename with
extension> --username <sAMAccountName for custom user>
```

> **Note**
>
> The script displays your current configuration, then offers to auto-configure the domain controller. If the auto-configure steps are successful, the script offers to registers the domain controller with Secure Access. Registration only occurs if you accept this offer.

Add a Domain Controller

Provides instructions for completing the Add a Domain Controller workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Choose the domain controller component type and set up the domain controller to sync with Secure Access.

For LDAP or LDAPS AD queries, AD integration requires that you register an AD domain controller or AD domain in Secure Access. The Cisco AD Connector performs an LDAP sync against this domain controller or domain to retrieve the Users and Groups. The Cisco AD Connector server communicates with the domain controller on port 389 over TCP for LDAP sync or port 636 over SSL for LDAP.

The Cisco AD Connector can only retrieve users and groups from a single domain controller. If you register multiple domain controllers in Secure Access, the Cisco AD Connector only attempts to perform an LDAP sync against the first domain controller in the list. Ensure that the domain controller you are registering is not subject to any AD replication delays. Read-only Domain Controller (RODC) registrations are supported for retrieval of users and groups.

If you need to periodically bring down your domain controller for maintenance or updates or your domain controllers are behind a load balancer that does not support LDAP queries, we recommend that you register the domain instead.

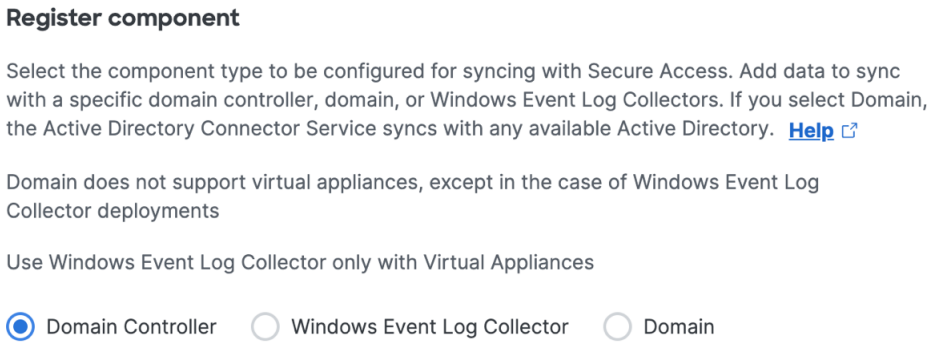
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain Controller**.

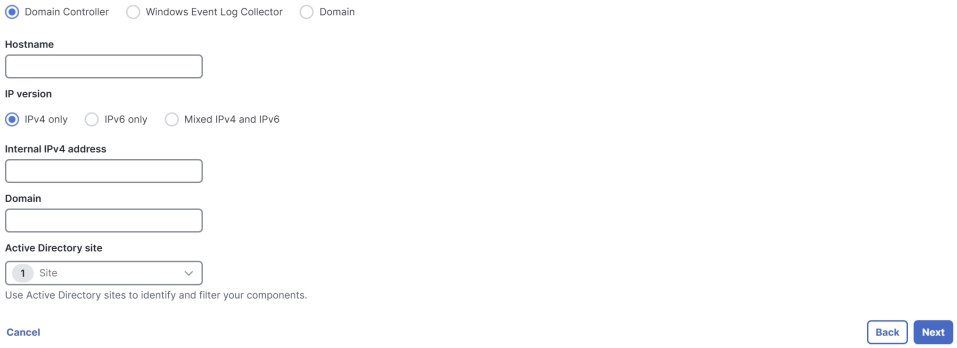
   Register the domain controller with Secure Access.

3. Enter the details for the domain controller.
   - **Hostname**–The hostname of the server where the domain controller is deployed.

- **IP version**–The IP address version to use. You can use **IPv4 only**, **IPv6 only**, or **Mixed IPv4 and IPv6**.
- **Internal IPv4 address** / **Internal IPv6 address** / both –The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
- **Domain**–The domain where the domain controller receives the events.

4. For **Active Directory site**, choose a Site to associate with the domain controller.



5. Click **Next**, and then follow the instructions to install the AD Connector.

Add a Domain

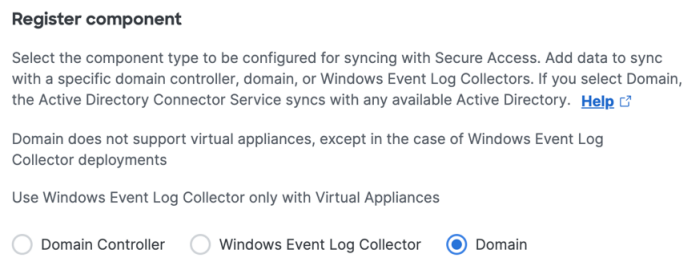
Provides instructions for completing the Add a Domain workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

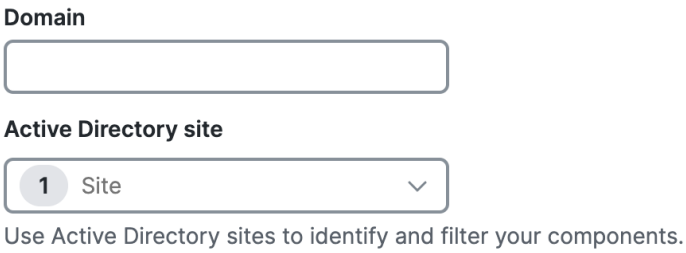
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain**.Register the AD domain with Secure Access.



3. For **Domain**, enter the domain name.
4. For **Active Directory site**, choose a Site to associate with the AD domain.



5. Click **Next**, and then follow the instructions to install the Cisco AD Connector.

View AD Components

In Secure Access, view the AD components and AD Connectors that you deployed.

The integration of Active Directory (AD) with Cisco Secure Access requires that you add the organization's AD components on Secure Access and integrate a Cisco AD Connector. Once these AD components are added, you can view them in Secure Access. You can also view the AD Connector deployments in Secure Access.

This guide describes how to view the AD components that you registered with Secure Access and the AD Connectors, which you deployed in your environments.

It can take up to four hours for large numbers of AD user and group objects to synchronize for the first time.

Seeing your groups listed means the domain controllers have automatically synchronized user and computer group memberships with Secure Access through the AD Connector successfully. Any subsequent changes should also sync successfully.

> **Note**
>
> If the AD Connector does not appear in Secure Access and you have met the network requirements, check that the AD Connector server is not missing the DigiCert CA. If a certificate error is presented, download and install the latest DigiCert Global Root CA from DigiCert and restart the Cisco Active Directory Service. If it does not appear, contact Cisco Secure Access Support.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connectors.

Procedure

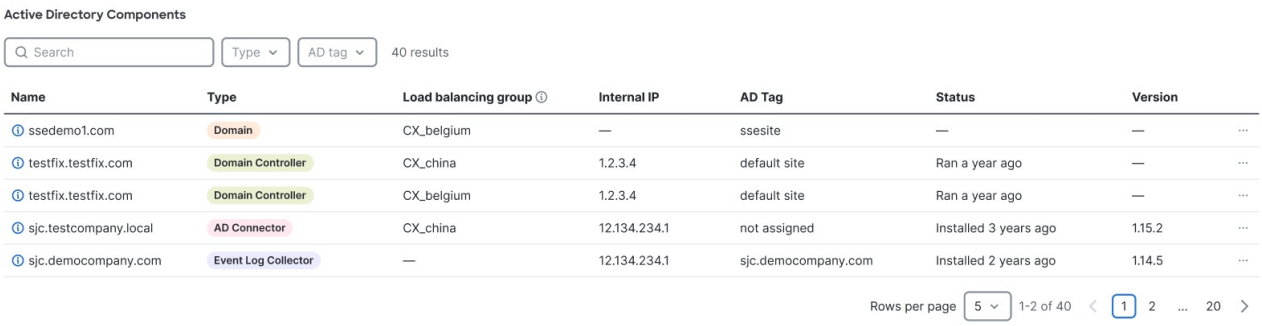
---

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** , click **Configuration management**, then expand **Active Directory**.



2. For **Active Directory components**, view the properties of the installed AD components.

- **Name**–The hostname of the Windows computer where you installed the AD Component.
- **Type**–The type of AD component, either **Domain Controller**, **Domain**, or **AD Connector**.
- **Load Balancing Group**–The group assigned to the Domain, Domain Controller, or AD Connector. Components with the same value process authentication events only within the same group.
- **Internal IPv4**–The internal IPv4 address of the AD component.
- **Internal IPv6**–The internal IPv6 address of the AD component.
- **AD Tag**–The unique label that identifies the Site associated with the AD component.
- **Status**–The state of the AD component.
- **Version**–The version of the AD component.



Assign a Load Balancing Group to AD Components

In Secure Access, assign a Load Balancing Group to a Domain, Domain Controller, or AD Connector so that authentication events are processed only within the same group.

Use the **Load Balancing Group** column in the **Active Directory Components** table to group related AD components for load balancing. To place components in the same group, enter the same **Load Balancing Group** value for each component.

To create a new Load Balancing Group, enter a new group name and save your changes.

Before you begin

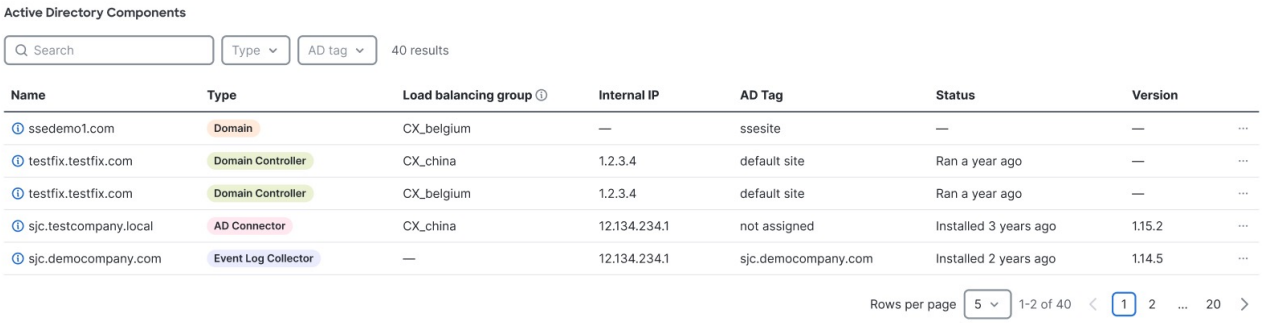
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users and User Groups**, click **Configuration management**, and then expand **Active Directory**.
2. At the top of the **Active Directory** section, click **Edit**.

> **Note**
>
> Do not use the Actions menu (**...**) for an individual component. That edit option is for changing the AD site association.

3. In the row for the Domain, Domain Controller, or AD Connector that you want to update, enter a value in **Load Balancing Group**.



> **Note**
>
> The **Load Balancing Group** value is case-sensitive. Differences in spelling or letter case create a different group.

4. Repeat Step 3 for each component that you want to include in the same group.

   Use the same **Load Balancing Group** value for all components that must process authentication events together.

5. Click **Save** at the end of the **Active Directory** section.

Secure Access updates the **Load Balancing Group** assignment for the selected AD components.

Edit Sites for AD Components

Provides instructions for completing the Edit Sites for AD Components workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Cisco Active Directory (AD) Connector and the organization's AD domains and domain controllers integrate Cisco Secure Access with your instance of Microsoft AD. After you add an AD component in Secure Access, you can select a Secure Access Site for the AD Component.

Follow these steps to edit a Site for an AD component that is deployed in your on-premises environment.

Before you begin

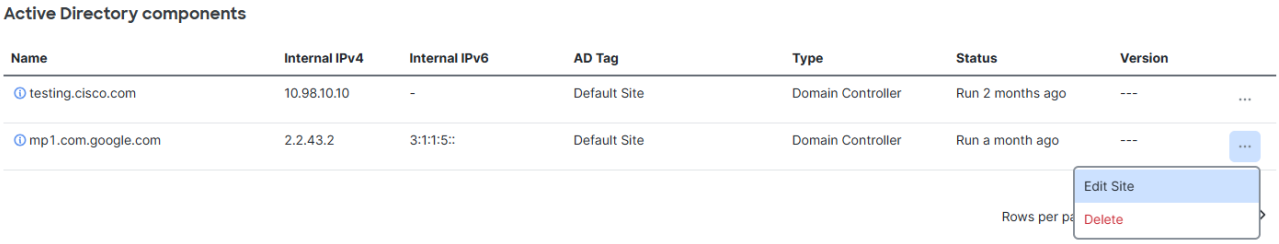
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors.

Procedure

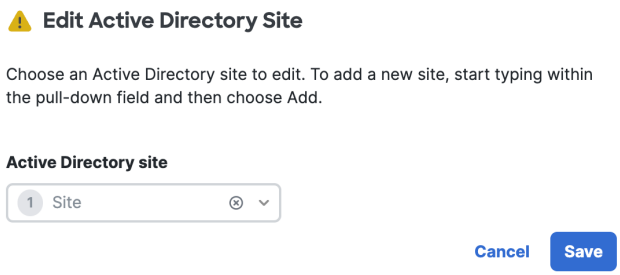
---

1. Navigate to **Connect** > **Users and User Groups**.
2. Click **Configuration management**

3. Expand **Active Directory**.
4. Click the ellipsis (**...**) to the right of an installed AD component in the **Active Directory components**.
5. Click **Edit Site**.



6. Choose an **Active Directory site** for the AD component.



7. Click **Save**.

Delete AD Components

In Secure Access, delete one AD component or delete all AD components for your organization.

Use this procedure to delete a single AD component or all AD components from Secure Access.

If you delete all AD components, Secure Access also removes the users and groups that were provisioned from AD.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

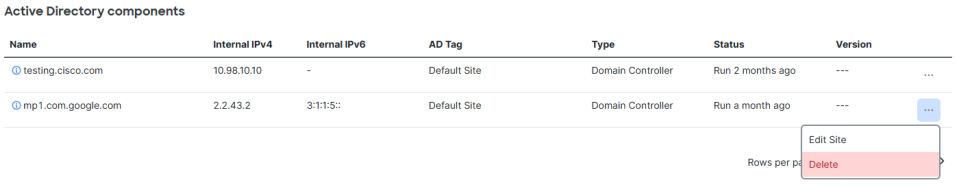
Procedure

---

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, click **Configuration management**, and then expand **Active Directory**.

Delete one AD component

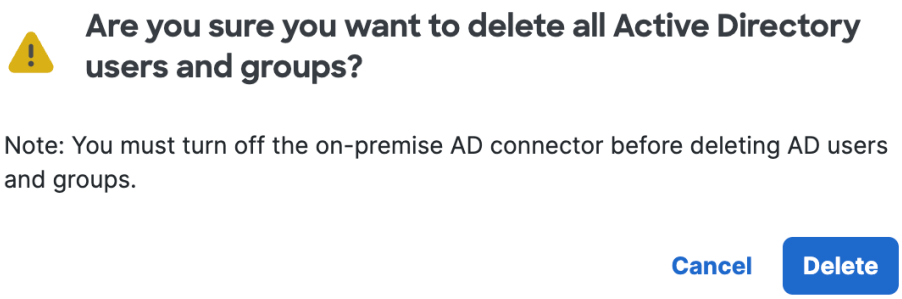
2. In **Active Directory Components**, locate the AD component that you want to delete, and then click the ellipsis (**...**).
3. Click **Delete**.



4. Click **Delete** to confirm.

Delete all AD components

5. In **Active Directory Components**, click **Delete**.



> **Warning**
>
> Deleting all AD components also removes the users and groups that were provisioned from AD.

6. Click **Delete** to confirm.

Secure Access deletes the selected AD component or all registered AD components, depending on the action that you chose.

Manage AD Connectors

Describes Manage AD Connectors in Cisco Secure Access. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD).

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD). Before you can provision users, groups, and endpoint devices from AD to Secure Access, complete the setup of the AD components, register the AD Components in Secure Access, and install the Cisco AD Connector in the organization's environment.

How to Connect Active Directory to Secure Access

The deployment of the AD Connector has various components and configuration settings. You can configure the Cisco AD Connector to provision users and groups from Microsoft AD using LDAP or LDAPS (domain controller or domain), or LDAP Interchange Format (LDIF) source files.

1. Add domain controllers or domains in Secure Access for LDAP or LDAPS deployments. For more information, see Add AD Components to Secure Access.
2. (Optional) Configure authentication for the AD Connectors in your environment. For more information, see Configure Authentication for AD Connectors and VAs.
3. (Optional) Configure updates for the AD Connectors in your environment. For more information, see Configure Updates for on AD Connectors.
4. Download the AD Connector software package and install it on your AD server. For more information, see Connect Active Directory to Secure Access.
5. (Optional) Configure the provisioning of users, groups, and endpoint devices with LDIF source files. For more information, see Deploy LDIF Files for AD Connector.
6. (Optional) Change the AD Connector account password. For more information, see Change the Connector Account Password.

7. View the installed AD components in Secure Access and verify that users and groups begin to sync with Secure Access. For more information, see View AD Components in Secure Access.

Configure Authentication for AD Connectors and VAs

Describes Configure Authentication for AD Connectors and VAs in Cisco Secure Access. Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments.

Cisco Secure Access communicates with the deployed Cisco Active Directory (AD) Connectors in your environments. Secure Access makes software syncs and health checks to the AD Connectors and requires that API requests from the AD Connectors use authentication. For information about deploying the Cisco AD Connector, see Connect Active Directory to Secure Access.

To manage the authentication of the communications from the AD Connectors to Secure Access, we recommend that you configure API key credentials for your AD Connector deployments. Your API key credentials apply to all AD Connectors and Secure Access Virtual Appliances that are deployed in your environment.

For more information about authentication and deploying Virtual Appliances, see Configure Authentication for Virtual Appliances.

> **Note**
>
> The API key authentication is available for Secure Access Virtual Appliances version 3.7.0 and newer and the Cisco AD Connector version 1.14.4 or newer. The API keys apply to the Virtual Appliances and the Cisco AD Connectors in the organization.

How to Set Up Your API Credentials

Describes How to Set Up Your API Credentials in Cisco Secure Access. Create a Secure Access Key Admin API key and secret.

Create a Secure Access Key Admin API key and secret. Then, use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

The Secure Access client API key and secret are stored in the AD Connectors that you deploy in your environments. The generated API credentials (key and secret) apply to all AD Connectors in the organization.

AD Connectors use the organization's Secure Access client API key credentials to generate an OAuth 2.0 access token, which authorizes API requests from the AD Connectors to Secure Access. The access token is included in every API request from the AD Connector to Secure Access.

> **Note**
>
> Secure Access client API key credentials are valid for 90 days.

- Step 1 – Create the Key Admin API Key Credentials
- Step 2 – Add the Key Admin API Key Credentials

Step 1 – Create the Key Admin API Key Credentials

Provides instructions for completing the Step 1 – Create the Key Admin API Key Credentials workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Create a Secure Access Key Admin API key. For more information, see Add Key Admin API Keys

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

Select each type of permission for the key.

> **Note**
>
> Save your Key Admin API key and secret and use these credentials to configure the authentication for the AD Connectors in the organization.

Permissions
Select the areas of Secure Access API Key functionality that this key is allowed to manage.

☑ List API Keys	Read-Only
☑ Create API Keys	Write
☑ Update API Keys	Write
☑ Refresh API Keys	Write
☑ Delete API Keys	Write

Step 2 – Add the Key Admin API Key Credentials

Provides instructions for completing the Step 2 – Add the Key Admin API Key Credentials workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

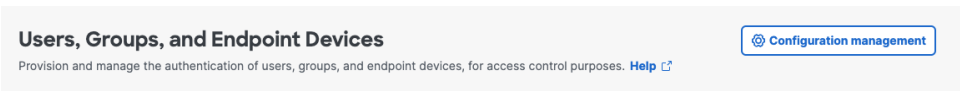
Add the Secure Access Key Admin API key and secret to the AD Connector in **Users and Groups > Configuration Management > API Authentication**. Then, generate a Secure Access client API key and secret.

Before you begin

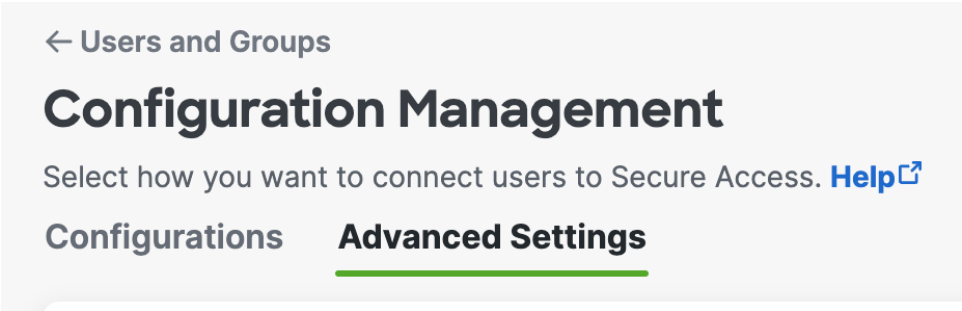
- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

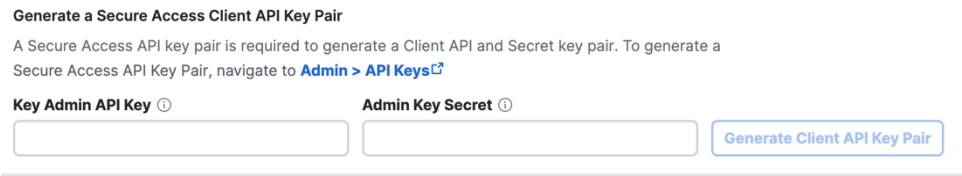


2. Click **Advanced Settings**.



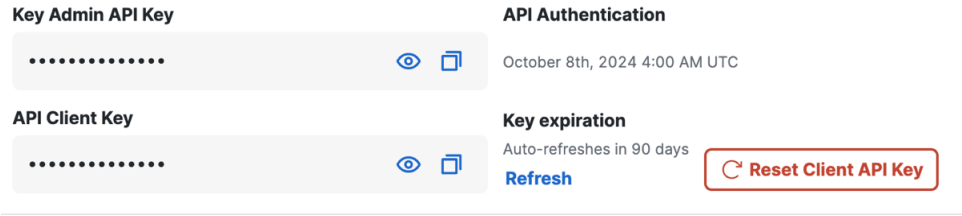
3. For **Key Admin API Key**, add the Key Admin API key, and for **Key Admin Key Secret**, add the Key Admin API key secret.

   For information about creating the Key Admin API key, see Step 1 - Create the Key Admin API Key Credentials.



4. After you add the Key Admin API key and secret, click **Generate Client API Key Pair**.
5. Save the Secure Access client API key and secret.

   Secure Access updates the client API key and secret automatically every 90 days.



Refresh Client API Key and Secret

Provides instructions for completing the Refresh Client API Key and Secret workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Refresh your Secure Access client API key and secret.

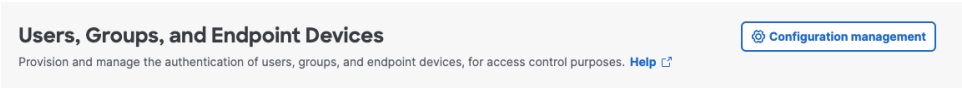
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

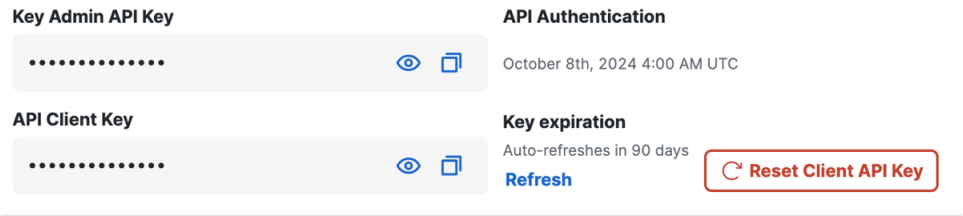
---

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

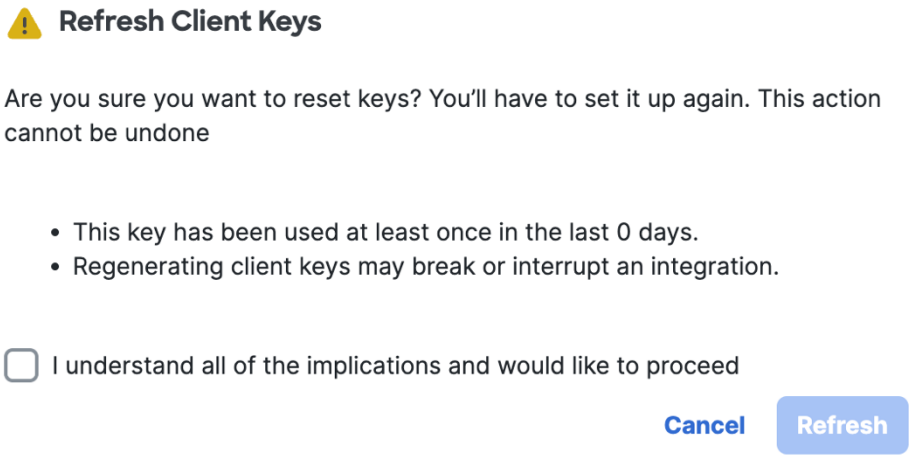


2. Click **Advanced Settings**.
3. Click **Refresh**.

   Secure Access refreshes the client API key and secret.



4. For **Refresh Client Keys**, check the box to confirm the deletion of the client API key and secret.



5. Click **Refresh**.

Reset Client API Key

Provides instructions for completing the Reset Client API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Delete your Secure Access Key Admin API key and Secure Access client API key.

> **Note**
>
> After you delete the Key Admin API key and client API key, existing AD Connector deployments may continue to use the stored Secure Access client API key and secret for up to 90 days.

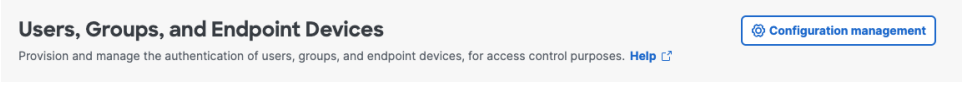
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

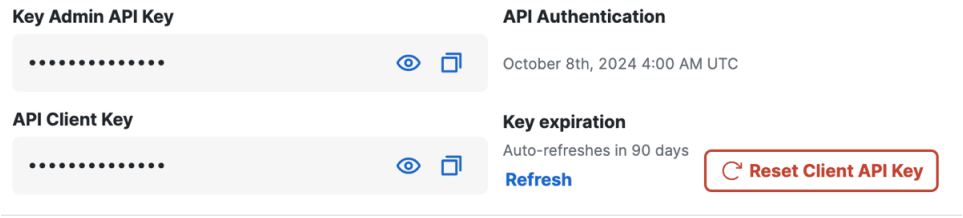
---

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

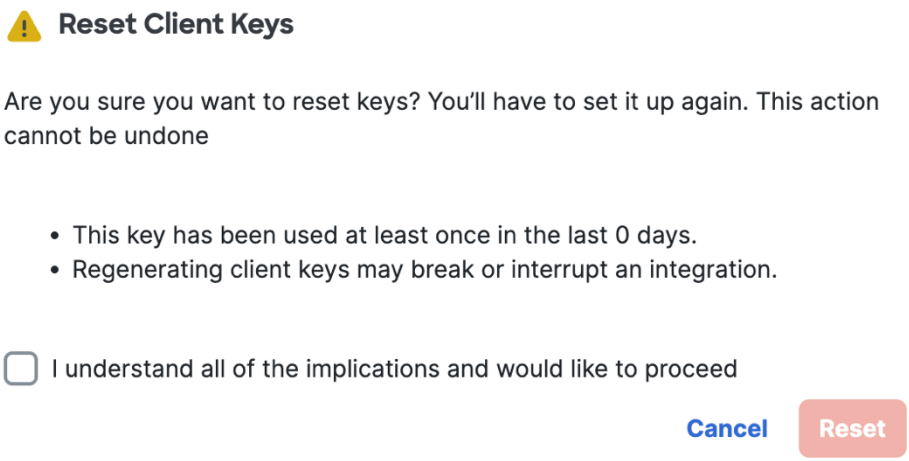


2. Click **Advanced Settings**.

3. Click **Reset Client API Key**.



4. For **Reset Client Keys**, check the box to confirm the deletion of both the Key Admin API key and client API key for the AD Connectors in the organization.



5. Click **Reset**.

Configure Updates on AD Connectors

Provides instructions for completing the Configure Updates on AD Connectors workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can schedule the date and time that Cisco Secure Access updates the Active Directory (AD) Connector software on your deployed Cisco AD Connectors. When scheduled, Secure Access checks if an AD Connector has the latest version of the software.

If a new version is available, Secure Access removes the installed AD Connector software from your systems and deploys the latest version of the AD Connector.

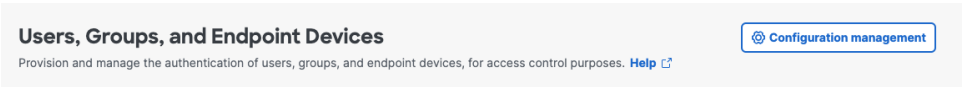
Select the day and time to update your deployed AD Connectors automatically.

Before you begin

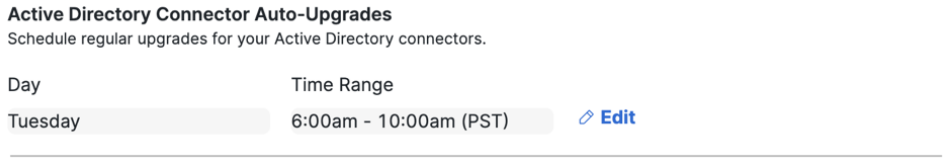
- Full Admin user role. For more information, see Manage Accounts.
- Deploy an AD Connector in your environment. For more information, see Connect Active Directory to Secure Access.

Procedure

1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.

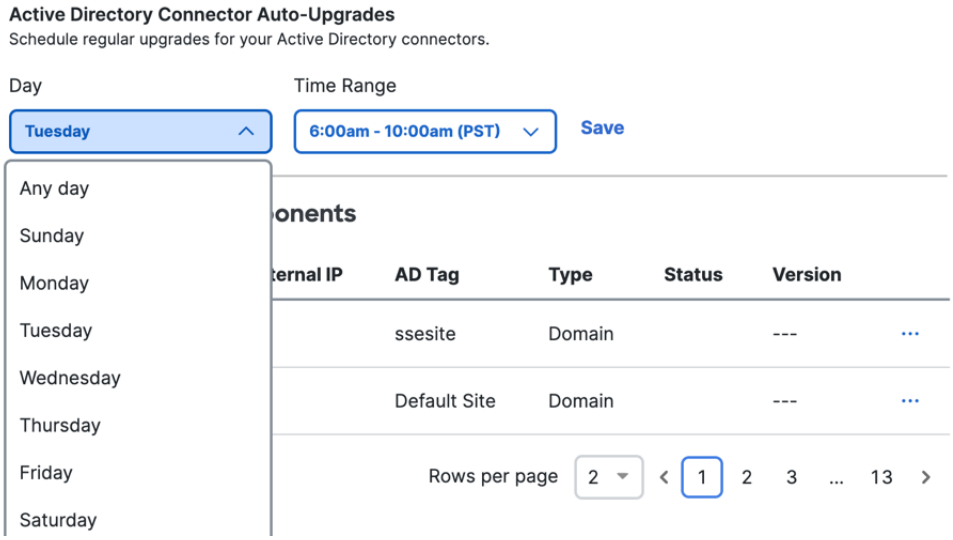


2. For **Provisioning**, expand **Active Directory**.
3. Navigate to **Active Directory Connector Auto-Upgrades**, and then click **Edit**.



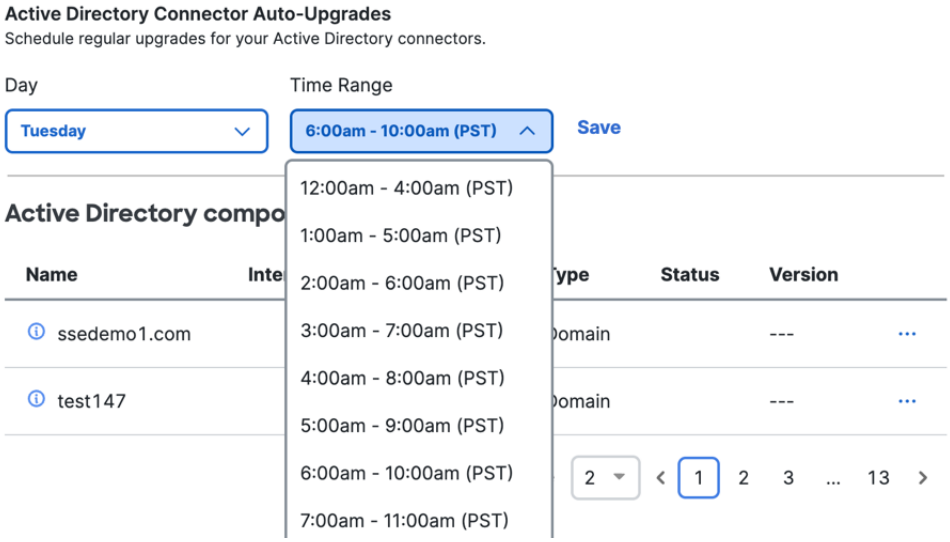
4. For **Day**, choose the day of the week to update the AD Connector software.

> **Note**
>
> The default **Day** is **Any day**–On every day of the week, if a software update is available, Secure Access attempts to redeploy the AD Connectors with the latest version of the software.



5. For **Time Range**, choose the four-hour time period to update the AD Connectors on the scheduled day.

> **Note**
>
> The default **Time Range** is **2:00 am - 6:00 am PST**.



6. Click **Save**.

Connect Active Directory to Secure Access

Describes Connect Active Directory to Secure Access. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD).

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft Active Directory (AD). Before you can provision users, groups, and endpoint devices from AD to Secure Access, register the AD Components in the environment (domain controller or domain) to Secure Access. Then, download the Cisco AD Connector software package and install the AD Connector in the organization's environment.

This guide describes the steps to install the Cisco AD Connector for LDAP or LDAPS, and provision users and groups from your instance of Microsoft AD to Secure Access.

Step 1 – Download the Active Directory Connector

Provides instructions for completing the Step 1 - Download the Active Directory Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Download the Cisco AD Connector from Secure Access to your server.

> **Note**
>
> When you download the Cisco AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

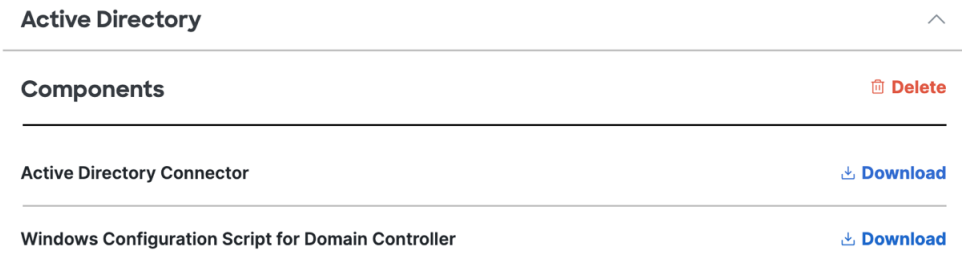
> **Note**
>
> You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the Cisco AD Connector from a network drive or run the **setup.msi** directly from the compressed file.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

1. Configure a server to run the Cisco AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
3. Under **Directories**, expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the Cisco AD connector software package to the server. The deployment package is named: **CiscoAuditClient_vX.X.X.zip**.



Step 2 - Install the Active Directory Connector

Provides instructions for completing the Step 2 - Install the Active Directory Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

As an administrator, extract the contents of the Cisco AD Connector ZIP file to a folder on the server, and then navigate to that folder.

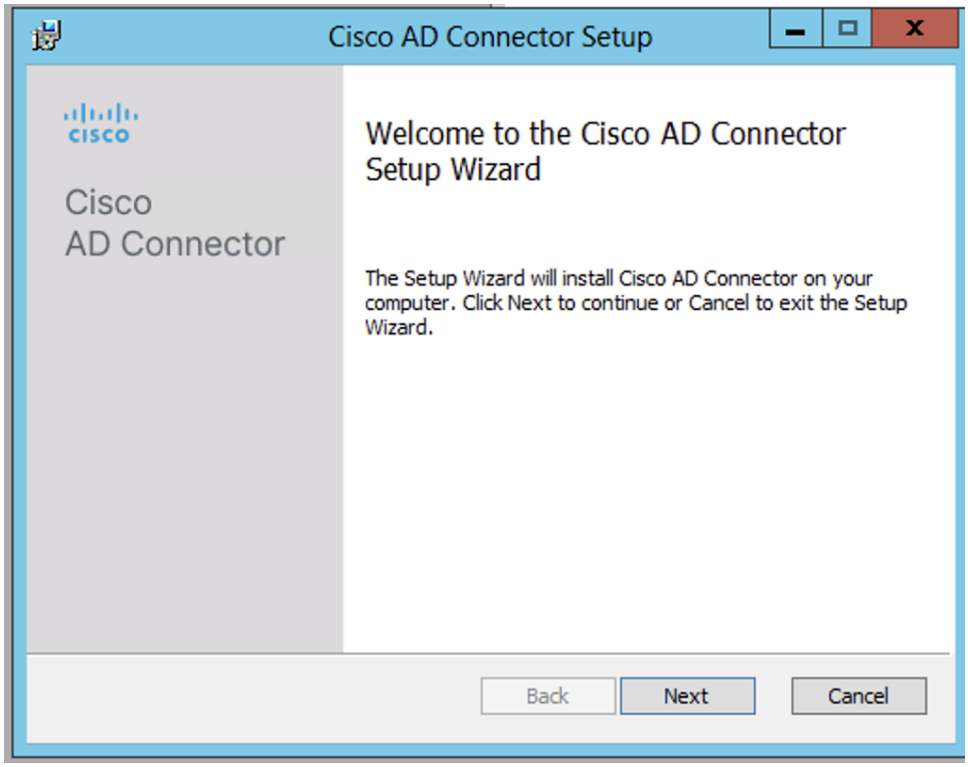
> **Note**
>
> If you run the AD Connector installer from the root directory of your server, you may encounter installation errors.

Before you begin

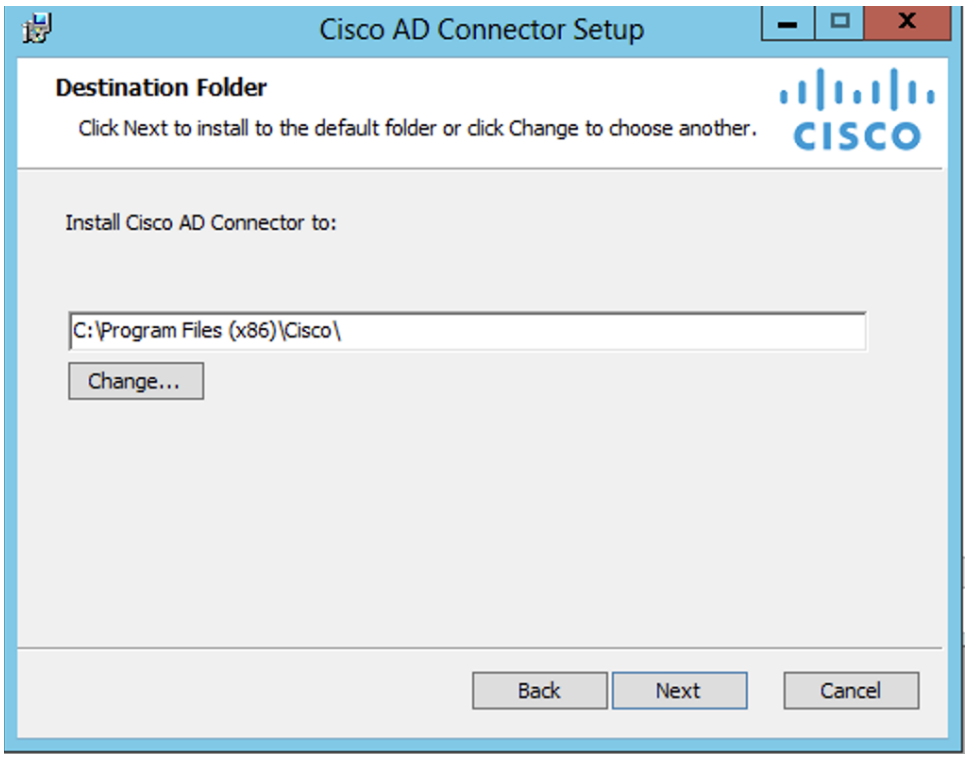
- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

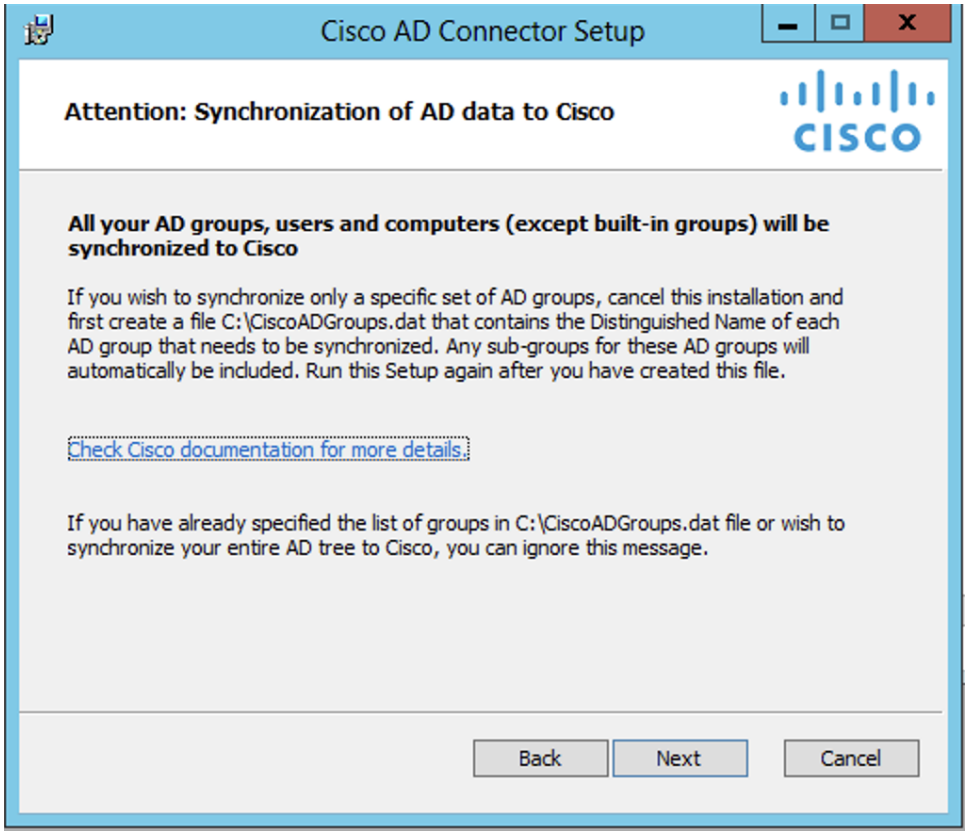
1. Run **setup.msi**, and then in the **Cisco AD Connector Setup** wizard, click **Next**.



2. Choose the directory on the server to install the Cisco AD Connector.



3. Confirm that you permit your AD Users and Groups to sync to Secure Access from the Cisco AD Connector.



4. Add your Active Directory credentials. Enter the **Username** of the Connector user (**Cisco_Connector** or custom username) and the **Password**.

5. Follow the remaining prompts in the setup, and when finished click **Finish**.

(Optional) Specify AD Groups in Selective Sync File

Describes (Optional) Specify AD Groups in Selective Sync File in Cisco Secure Access. You can specify the AD Groups for the purpose of creating Access rules in Secure Access.

You can specify the AD Groups for the purpose of creating Access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

Supported Organizational Units

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

```
CN=Engineering,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Sales,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Marketing,CN=Builtin,DC=ciscoumbrella,DC=com
```

Total Number of Groups Selected for Synchronization

Groups specified in the selective sync file and all of their subgroups should not exceed 15,000. Also, these Groups should not be nested within more than five OU levels. Selective synchronization fails in both cases.

> **Note**
>
> If you can not meet either of these requirements, we recommend that you do not use the selective sync file. Instead, you can do a full AD tree synchronization.

Rename Selective Sync File After Upgrading to AD Connector v1.14.4

Describes Rename Selective Sync File After Upgrading to AD Connector v1.14.4 in Cisco Secure Access. If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file C:\CiscoUmbrellaADGroups.dat to C:\CiscoADGroups.dat.

If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file **C:\CiscoUmbrellaADGroups.dat** to **C:\CiscoADGroups.dat**.

Note: The selective sync file–previously named **CiscoUmbrellaADGroups.dat**–is not recognized by the Cisco AD Connector v1.1.4.4 or later.

After you rename the selective sync file, Secure Access automatically reads the selective sync file (**C:\CiscoADGroups.dat**) and syncs the Users in the specific Groups from AD to Secure Access. You are not required to restart the AD Connector service.

Create AD Groups in a Selective Sync File

Provides instructions for completing the Create AD Groups in a Selective Sync File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Set up the AD Connector server, user account, and environment for deploying the AD Connector. For more information, see Prerequisites for AD Connectors.
- Add the AD components in Secure Access. For more information, see Add AD Components in Secure Access.
- (Optional) Configure Authentication for AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.
- (Optional) Configure software updates on the AD Connector. For more information, see Configure Updates on AD Connectors.

Procedure

1. Identify the AD Groups of interest. Users and computers belonging to these Groups synchronize to Secure Access. For each sub-tree, only the parent group needs to be specified. All AD groups, users, and computers that are part of this parent group are automatically included.

   Note

   If you enabled **Selective Sync**, AD Users and Computers that are not members of Groups specified in **CiscoADGroups.dat** or their subgroups are not synchronized to Secure Access and are completely exempt from Secure Access access rules and reports.

   Note

   When configuring **Selective Sync** for **Cisco AD Connector**, do not use top-level built-in groups such as **Domain Users** or **Domain Computers** in the group filter. These built-in primary groups typically include most or all identities in the domain. In multi-domain environments, their use may result in users and computers from all domains being synchronized unintentionally. To maintain precise and predictable control over which identities are synchronized, create and use dedicated custom groups for selective sync instead.

2. Create a **CiscoADGroups.dat** file in the **C:** drive of each machine where the connector is installed. The connector only reads the **C:\CiscoADGroups.dat** file. If the file is incorrectly named or is not present in the **C:** drive, all groups are imported to Secure Access.
3. List the AD groups that need to be synchronized in `distinguished name` (DN) format in this file.
4. Ensure that there are no blank lines anywhere in the file.

   Note

   If you are running multiple AD Connectors, the file **C:\CiscoADGroups.dat** should be present on each system running the AD Connector and should be identical on each system.

Deploy LDIF Files for AD Connector

Describes Deploy LDIF Files for AD Connector in Cisco Secure Access. The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD.

The Cisco Active Directory (AD) Connector integrates with Cisco Secure Access to provision the organization's users and groups from AD. You can install and configure the AD Connector to provision users and groups using LDAP Interchange Format (LDIF) source files. Once you deploy the LDIF files on your server, the AD Connector syncs the users and groups in your organization with Secure Access.

For information about deploying the AD Connector with LDAP or LDAPS, see Connect Active Directory to Secure Access.

Best Practices for LDIF Source Deployments

- Do not combine manually provisioned (CSV file) users and groups with LDIF-based sourcing deployments. If you use both deployment methods, you may add duplicate users and groups in your organization.
- To migrate from the manually provisioned users and groups to LDIF-based sourcing, delete the CSV file with the users and groups that you uploaded to Secure Access.
- If you have multiple Active Directory deployments and choose to manually provision users and groups, we recommend that you deploy the AD Connector with LDIF source files.
- Once you provision users and groups with LDIF-based sourcing, we do not recommend that you delete the deployment and provision the users and groups using another deployment method.
- LDIF-based sourcing does not require Secure Access Domain Controllers.

Requirements

Requirements for deploying LDIF source files on your server:

- LDIF can support multiple domains.
- Create the LDIF files in the **Text** document format.

Known Limitations

- No support for selective groups-only sync.
- No support for incremental sync.

Download, install, and configure the Cisco AD Connector. Then, deploy the LDIF source files.

- Step 1 – Download the Active Directory Connector
- Step 2 – Install the Cisco AD Connector
- Step 3 – Deploy the LDIF Source Files

Step 1 – Download the Active Directory Connector

Provides instructions for completing the Step 1 – Download the Active Directory Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Download the Cisco AD Connector from Secure Access to your server.

When you download the Cisco AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

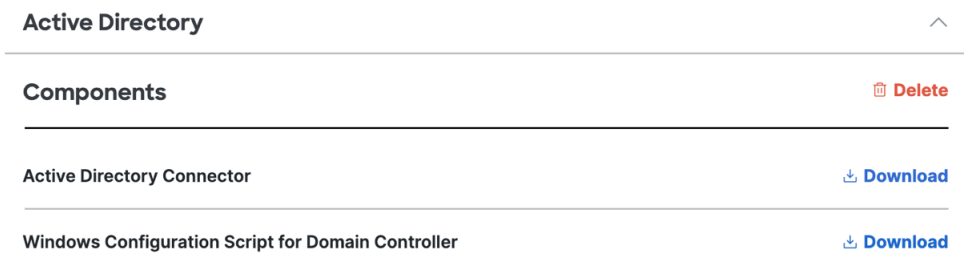
> **Note**
>
> You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the Cisco AD Connector from a network drive or run the **setup.msi** directly from the compressed file.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Configure a server to run the Cisco AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and then click **Configuration management**.
3. Navigate to **Directories**, expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the Cisco AD connector software package to the server. The software package is named: **CiscoAuditClient_vX.X.X.zip**.



Step 2 – Install the Cisco AD Connector

Provides instructions for completing the Step 2 – Install the Cisco AD Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

As an administrator, extract the contents of the ZIP file that you downloaded to a folder and then navigate to that folder.

If you run the Cisco AD Connector installer files from the root directory of your device, you may encounter installation errors.

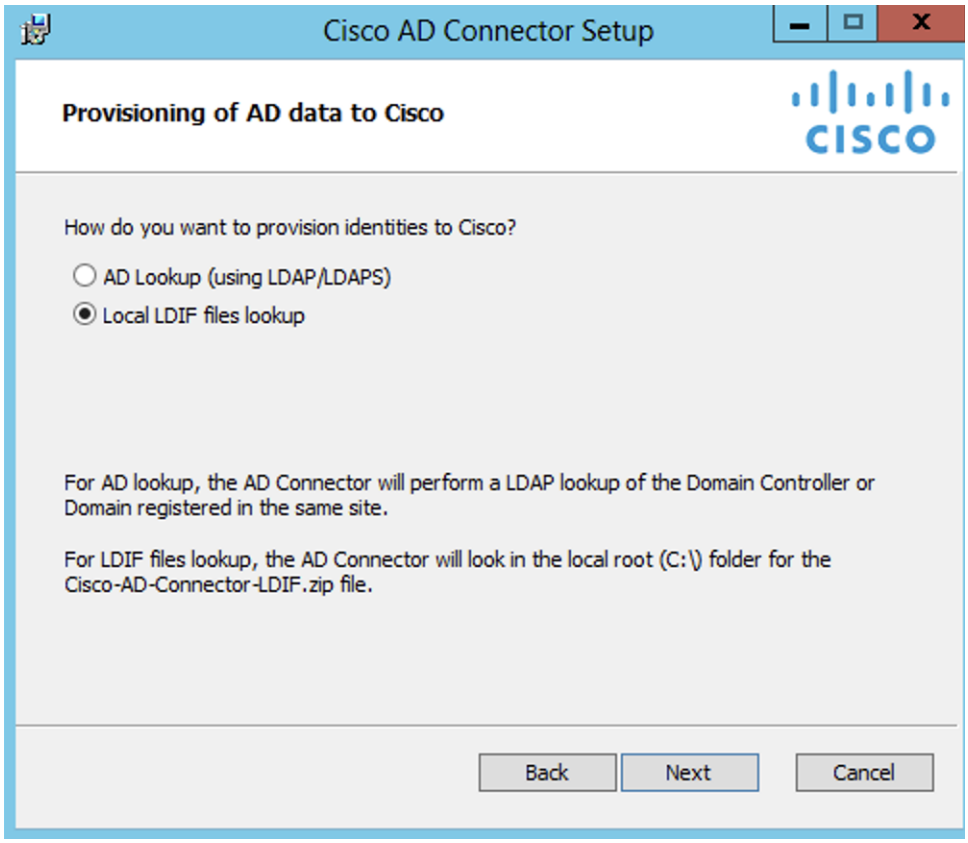
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Run **setup.msi**.

2. Enter the username of the Connector user (**Cisco_Connector** or custom username) and the password.
   For more information, see Prerequisites for AD Connectors.
3. Select **Local LDIF files lookup**, and then click **Next**.
4. Follow the prompts in the setup, and then click **Finish**.



Step 3 – Deploy the LDIF Source Files

Provides instructions for completing the Step 3 – Deploy the LDIF Source Files workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Deploy the LDIF source files on your server.

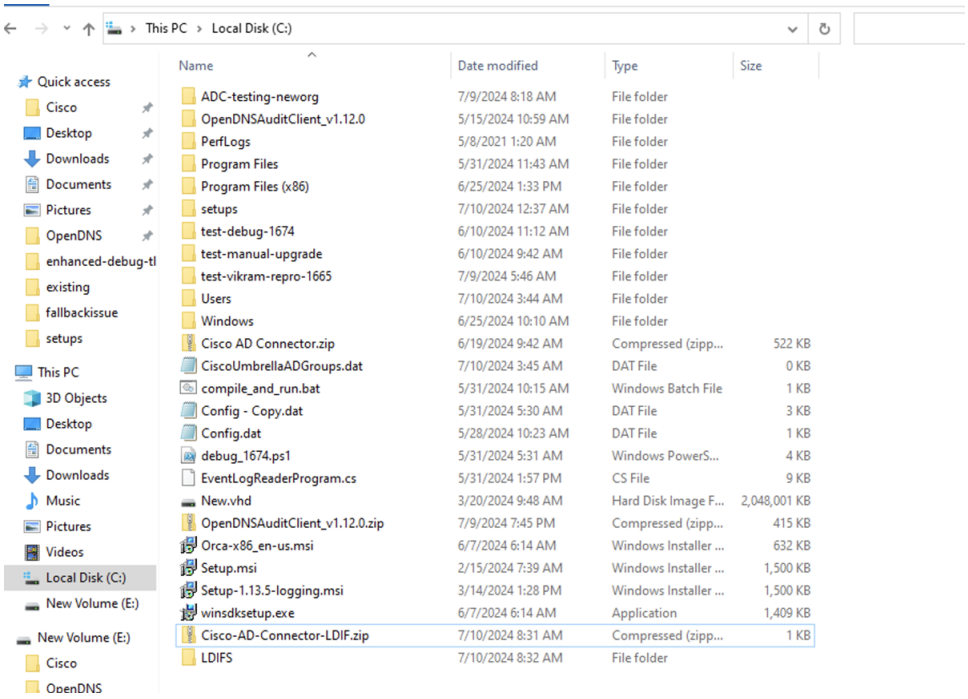
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about network requirements, and connector user account and server prerequisites, see Prerequisites for AD Connectors.
- Cisco AD Connector version 1.14.4 or newer.

Procedure

1. Navigate to the **C:** drive on your server.
2. Generate the LDIF files for the users and groups in your organization, and zip the files into a file. Name the file **Cisco-AD-Connector-LDIF.zip**.
   - Base-64 encode the value of the **objectGUID** fields.
   - Use two colons (**::**) to separate the **objectGUID** fields.

- For users, create an **UserStruct.ldif** file. The supported fields are:
  - **dn**, **objectGUID**, **sAMAccountName**, **userPrincipalName**, **memberOf**, and **primaryGroupID**.
- For groups, create a **GroupStruct.ldif** file. The supported fields are:
  - **dn**, **objectGUID**, **sAMAccountName**, **userPrincipalName**, **memberOf**, and **primaryGroupToken**.



Troubleshooting

Describes Troubleshooting in Cisco Secure Access. Various configuration conditions of the AD Connector with LDIF source files can result in provisioning errors.

Various configuration conditions of the AD Connector with LDIF source files can result in provisioning errors.

Scenario 1

- You uploaded an **Cisco-AD-Connector-LDIF.zip** file with users and groups in a particular set of domains. Later, you uploaded another **Cisco-AD-Connector-LDIF.zip** file (with a different set of domains) and expected only the identities from these domains to be present. However, the identities from the domain of the previous upload were retained and not removed.

Possible Cause: This configuration is not supported.

Solution: Raise a request with Cisco Support.

Scenario 2

The **Cisco-SSE-AD-Connector-LDIF.zip** file is not found. The Cisco AD Connector can not sync the users and groups with Secure Access.

Solution: Ensure that the **Cisco-AD-Connector-LDIF.zip** file is located under the **C:** drive on the server.

Scenario 3

If one or both of the LDIF source files (**UserStruct.ldif** and **GroupStruct.ldif**) are not present or empty, then the Cisco AD Connector can not sync the users and groups with Secure Access.

Solution: Verify the contents in the **Cisco-AD-Connector-LDIF.zip** file and upload the file to the **C:** drive on the server.

Scenario 4

Ensure that all fields in the LDIF source files are valid with no inappropriate values. The **dn** field is required and should contain appropriate values.

Analyze Logs

You can find the Cisco AD Connector logs on the server in the **C:\Program Files (x86)\Cisco\CiscoAD Connector\v1.14.4** folder. The log files are:

- For errors–**CiscoAuditClient.error.log**.
- For all events–**CiscoAuditClient.log**.

Change the Connector Account Password

Provides instructions for completing the Change the Connector Account Password workflow in Cisco Secure Access. Administrative privileges on the server where you will install the AD Connector.

For regulatory compliance, you may need to change the password of the Cisco Active Directory (AD) Connector account. You can modify this password without impacting the functionality of the Cisco AD Connector.

Changing the password on the Cisco AD Connector ensures that the AD connector can communicate with Microsoft AD using the new credentials. If the AD Connector account password is not correct, the Cisco AD Connector is unable to subscribe to login events and AD changes.

> **Note**
>
> If the password is not changed, Secure Access can not identify DNS requests with the AD users or groups accurately, and can not sync user and group changes from AD.

Before you begin

- Administrative privileges on the server where you will install the AD Connector.
- Install and set up the AD Connector on a server in your organization. For more information, see Connect Active Directory to Secure Access.

Procedure

1. Sign in to the account from any system that is a member of the domain and then set the new password.
2. Stop the **Cisco AD Connector** service.
3. Navigate to **C:\Program Files (x86)\Cisco\CiscoADConnector** and run the file **CiscoPasswordManager.exe**.

   You may need to run this utility as an administrator.
4. When prompted, add your new password.

5. Start the **Cisco Active Directory Service** service.

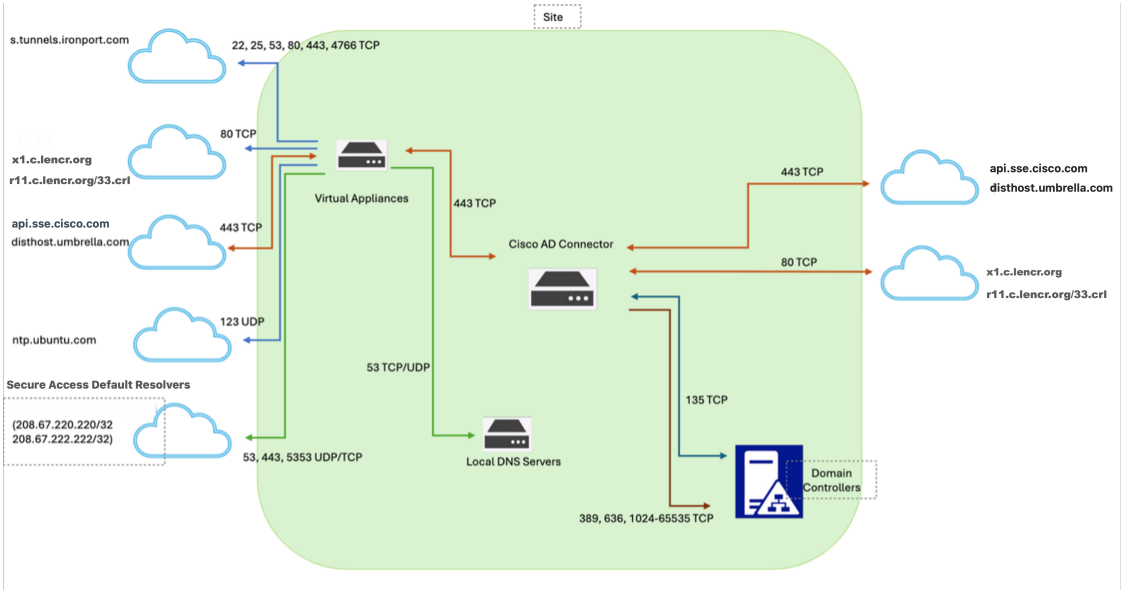
What to do next
Repeat steps 2 and 3 for each deployed AD Connector.

AD Connector Communication Flow and Troubleshooting

Describes AD Connector Communication Flow and Troubleshooting in Cisco Secure Access. The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access and AD domain controllers.

The Cisco Active Directory (AD) Connector is a Windows application and service that communicates with Cisco Secure Access and AD domain controllers. The Cisco AD Connector only syncs the required AD User and Group attributes with Secure Access.

The following information describes the communication flow between a Cisco AD Connector and AD domain controllers, the attributes that sync between AD, the AD Connector, and Secure Access, and the steps that you can take to troubleshoot your Cisco AD Connector deployment. The diagram includes the deployment of the Secure Access Virtual Appliance.



Communication Flow

Describes Communication Flow in Cisco Secure Access. The Cisco AD Connector first attempts to communicate to the AD domain controller over secure lightweight directory access protocol (LDAPS) on port 646.

1. The Cisco AD Connector first attempts to communicate to the AD domain controller over secure lightweight directory access protocol (LDAPS) on port 646. If unsuccessful, the Cisco AD Connector falls back to communicating over LDAP on port 389 using first Kerberos authentication and if that does not succeed, NTLM authentication (Windows NT LAN Manager) over LDAP.
2. The Cisco AD Connector retrieves the AD Users, Groups, and Endpoint Devices details only. Secure Access stores these required attributes from each object:
   - `cn`–The common name.
   - `dn`–The distinguished name.
   - `dNSHostName`–The device name as it is registered in DNS.

- `mail`–Email addresses associated with the user.
- `memberOf`–The groups that include the user.
- `objectGUID`–The group ID of the object. This property is sent to Secure Access as a hash.
- `primaryGroupId`–The primary group ID that is available for Users and Groups.
- `primaryGroupToken`–The primary group token that is available only for Groups. Passwords or password hashes are not retrieved. Secure Access uses the `primaryGroupToken` data in the access policy and configuration and reporting. This data is also required for each user or per-computer filtering.
- `sAMAccountName`–The username that you use to sign into the Cisco AD Connector.
- `userPrincipalName`–The user's principal name.

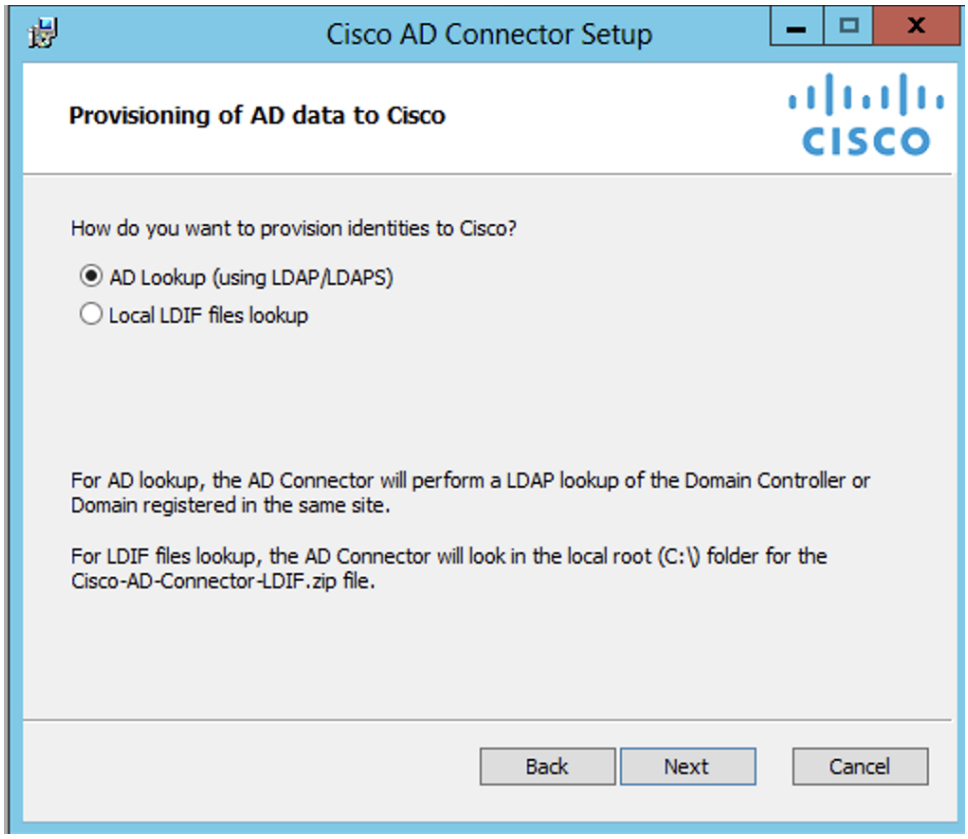
> **Note**
>
> If there are updates, the Cisco AD Connector sends the AD data every five minutes using an HTTPS connection on TCP port 443. However, it can take an hour or longer for changes to reflect in Secure Access.

3. The Cisco AD Connector stores the AD User and Group data locally in **.ldif** files.

   The local AD User and Groups data is contained within this folder: `C:\\Program Files (x86)\\Cisco\\CiscoADConnector\\ADSync`.

   Review the files in the **.ldif** files in the **ADSync** directory to confirm that the Cisco AD Connector synchronized the AD Users and Groups data to Secure Access.

> **Note**
>
> When you install the Cisco AD Connector, you have the option to turn off the local storage of `.ldif` files.



Troubleshooting

Describes Troubleshooting in Cisco Secure Access and outlines Network Requirements and Restart the Active Directory Connector. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Recommendations for troubleshooting the communications with the Cisco AD Connector.

Network Requirements

The Cisco AD Connector communicates with Secure Access and the deployed domain controllers. Ensure that you allow certain domains and services on your firewalls. For more information, see Network Requirements for Secure Access.

Port and Protocol	Source	Destination	Note
443/TCP	AD Connector	**api.sse.cisco.com** **disthost.umbrella.com**	• Initial registration with the Secure Access • Automatic updates • Health status reporting in Secure Access
80/TCP	AD Connector	[redacted]	Check for certificate revocations through the certificate revocation list (CRL).

Port and Protocol	Source	Destination	Note
80/TCP	AD Connector	commercialocspidentrust.com/	Check for certificate revocations through the Online Certificate Status Protocol (OCSP).
389/TCP 636/TCP	AD Connector	Domain controller or domain	Sync with LDAP/LDAPS

Note

The Digicert domains resolve to various IP addresses based on a CDN and are subject to change.

If you experience any issues communicating with Secure Access, we recommend that you check for any Layer-7 application proxies, which may block or drop data sent to Secure Access. A common case is the **inspect** feature on Cisco devices that communicate on DNS, HTTP, or HTTPS. For more information, see Cisco Security Appliance Command Line Configuration Guide, Version 7.2.

Restart the Active Directory Connector

You can restart the **Cisco AD Connector** service on the AD Connector server. Restarting the Cisco AD Connector triggers a full synchronization of the AD Users and Groups, not only the changes from the previous sync to Secure Access.

If your Cisco AD Connector is not in the **Okay** state, contact Support. For more information, see the contact support section in the Welcome to Secure Access topic.

Edit AD Authentication Properties

Provides instructions for completing the Edit AD Authentication Properties workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit the Authentication property for the AD users or endpoint devices in the organization.

Once you add an Active Directory (AD) integration in Cisco Secure Access, you can edit the Authentication property for the AD users or endpoint devices in the organization.

Before you begin

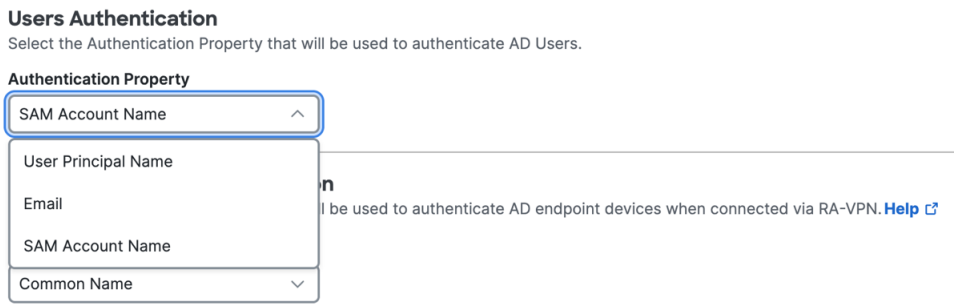
- Full Admin user role. For more information, see Manage Accounts.

Procedure

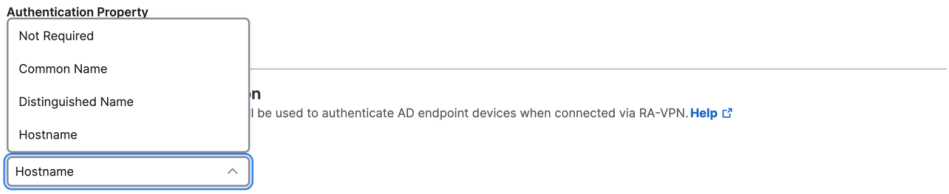
1. Navigate to **Connect > Users, Groups, and Endpoint Devices**, and click **Configuration management**.
2. Navigate to **Configurations**, and then navigate to **Directories**.
3. Expand **Active Directory**.
4. Click **Edit** (pencil icon) at the top of the **Active Directory** section on the page to edit the authentication properties for the directory integration.



5. Navigate to **Users Authentication**, and then navigate to **Authentication Property**.
   a) Select the property that all AD users in the AD directory integration will use to authenticate with Secure Access.
      - **User Principal Name**–The user principal name of the AD user.
      - **Email**–The email address of the AD user.
      - **SAM Account Name**–The SAM account name for the AD user.



6. Navigate to **Endpoint Devices Authentication**, and then navigate to **Authentication Property**.
   a) Select the property that all AD endpoint devices in the AD directory integration will use to authenticate with Secure Access or select **Not Required**.
      - **Common Name**–The common name (CN) is the unique name of the AD endpoint device within it's organizational unit (OU).
      - **Distinguished Name**–The name of the AD device that is unique in the organization.
      - **Hostname**–The hostname of the AD endpoint device.



7. Click **Save**.

Best Practices: Configuring the AD Authentication Properties

Describes Best Practices: Configuring the AD Authentication Properties in Cisco Secure Access. After a configuration change to the Authentication property, Secure Access begins the update of the Authentication property for the AD users or endpoint devices in the AD directory integration.

- After a configuration change to the Authentication property, Secure Access begins the update of the Authentication property for the AD users or endpoint devices in the AD directory integration.

> **Note**
>
> Updates to the Authentication property for the AD users or endpoint devices may take up to one hour to complete.

- We do not recommend that the organization update the Authentication property for the AD directory integration frequently. If the organization configures a series of changes to the Authentication property before the first update has completed, an error may occur.
- After you update the Authentication property for the AD endpoint devices, you must restart the AD Connector to trigger a full synchronization of AD Users, Groups, and Endpoint Devices. For more information, see Restart the Active Directory Connector.

Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications

Provides instructions for completing the Synchronize Active Directory Reporting Manager Email Addresses for DLP Notifications workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

When Secure Access detects a violation of a DLP SaaS API or Real Time rule, the system may generate a notification email for the person who triggered the violation, as well as a notification email for that person's manager. These email notifications are optional, and configurable within the rule itself (see Add a Real Time Rule to the Data Loss Prevention Policy and Add a SaaS API Rule to the Data Loss Prevention Policy.)

To support sending email notifications to an actor's manager, you must first enable synchronizing Active Directory reporting manager email addresses with Secure Access, as described in this task.

Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** and click **Configuration management**.
2. Navigate to **Configurations**, then navigate to **Directories**.
3. Expand **Active Directory**.
4. Click **Edit** (pencil icon) at the top of the **Active Directory** section of the page to edit the Additional Attributes for Data Loss Prevention.
5. Navigate to **Additional Attributes for Data Loss Prevention (DLP)**.
6. Click the toggle to enable or disable **Sync reporting manager's email**.
7. Click **Save**.

After enabling **Sync reporting manager's email** you will be able to enable sending notification email to the managers of persons who trigger violations of DLP SaaS API or Real Time rules.

AD Integration with Virtual Appliances

Describes AD Integration with Virtual Appliances in Cisco Secure Access. The integration of Microsoft Active Directory (AD) with Cisco Secure Access Virtual Appliances (VAs) provides AD user, group, or computer name information for each applicable DNS request.

The integration of Microsoft Active Directory (AD) with Cisco Secure Access Virtual Appliances (VAs) provides AD user, group, or computer name information for each applicable DNS request. Secure Access VAs forward DNS requests at the site.

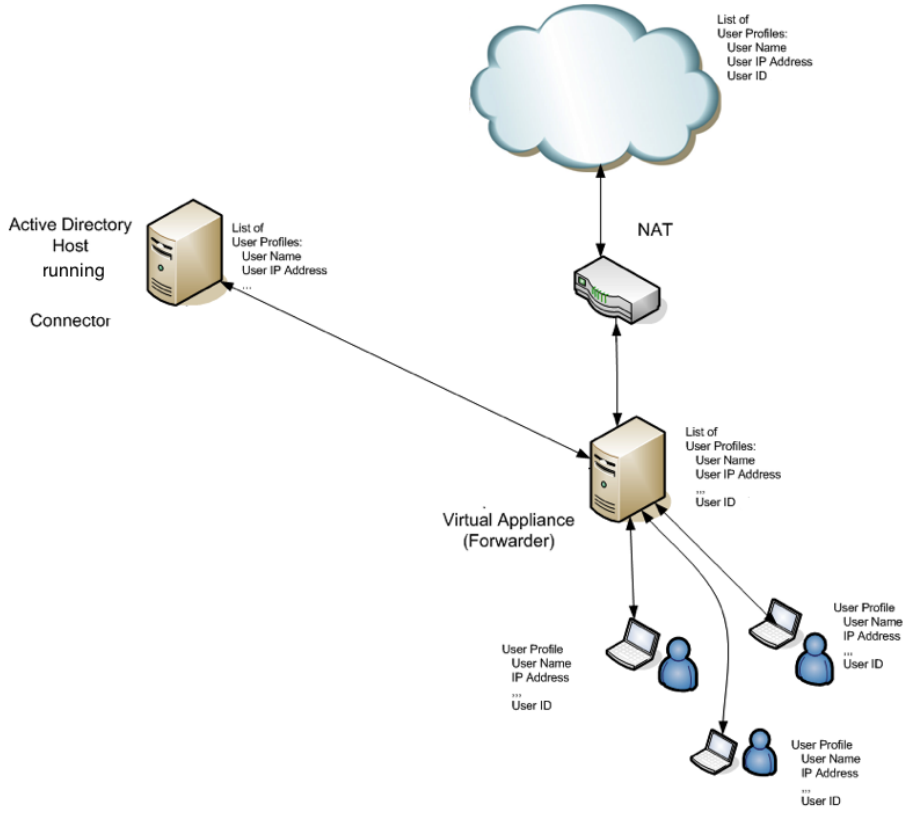
An AD site in the context of this guide means an independent location with its own domain controllers, DNS servers, and connection to the internet. For information about Secure Access Sites, see Manage Sites for AD Components and Manage Site for Virtual Appliance.

For an overview of the network topology, as well as the flow of traffic with the VA, see AD Connector Communication Flow and Troubleshooting.

Network Diagram for VA Deployments

Describes Network Diagram for VA Deployments in Cisco Secure Access. The client computers at each AD site must be set to use the VA at their respective site as their DNS resolvers.

The client computers at each AD site must be set to use the VA at their respective site as their DNS resolvers. The VA can then route DNS queries to their appropriate IP address for both internal and external resources. The VA also communicates with the AD environment to query for a list of user information to match to clients.



How to Set Up AD Components with VAs

Describes How to Set Up AD Components with VAs in Cisco Secure Access. Review the requirements for setting up the AD components in your environment.

1. Review the requirements for setting up the AD components in your environment. For more information, see Prerequisites for AD Connectors and VAs.
2. Prepare your AD Environment. For more information, see Prepare Your AD Environment.
3. Install the AD Connectors. For more information, see Connect Active Directory to VAs.
4. View the installed AD components. For more information, see View AD Components.

5. View the provisioned AD users and groups in Secure Access. For more information, see View User Details and View Group Details.

Prerequisites for AD Connectors and VAs

Describes Prerequisites for AD Connectors and VAs in Cisco Secure Access. To support the integration of Active Directory (AD) with Secure Access, review and meet the requirements for the Connector server and account, and AD deployments with Secure Access virtual appliances.

To support the integration of Active Directory (AD) with Secure Access, review and meet the requirements for the Connector server and account, and AD deployments with Secure Access virtual appliances.

Connector Server

You must configure a server that is a member of the AD domain with the following environment:

- Windows Server 2016, 2019, 2022, or 2025.
- 100MB free hard disk drive space.
- .NET Framework 4.5 or above.
- If a local anti-virus application is running, allow the **CiscoAuditClient.exe** and **CiscoAuditService.exe** processes to run on the system.

The Connector may be deployed directly on the domain controller. In this case, the domain controller must meet all prerequisites listed above. Only one connector is required to provision identities from an AD domain, with an optional second connector for redundancy if required.

Guidelines for AD Deployments with Secure Access Virtual Appliances

- For troubleshooting, install the **AD Domain Services Snap-ins and Command-line Tools** feature through the **Remote Server Administration Tools > Role Administration Tools > AD DS & AD LDS Tools > AD DS Tools**.
- If you are deploying AD with Virtual Appliances through the integration with domain controllers, you must deploy one AD Connector for each AD domain (with an optional second connector for each AD domain).
- If you have already deployed a centralized Windows Event Log Collector to which all domain controllers forward login events, and you wish to deploy AD integration with Virtual Appliances using this Windows Event Log Collector, you will need to deploy a single AD connector for all AD domains, with an optional second connector for redundancy.

Outbound Network Access to Secure Access

The Connector server requires outbound access on certain domains and URLs. If you are using a transparent HTTP web proxy, ensure that these domains and URLs on port 80/443 are excluded from the proxy, and not subject to authentication.

- For syncing, allow traffic on 443 (TCP) to **api.sse.cisco.com**.
- For Windows to perform Certificate Revocation List and Code-Signing checks, allow access to additional URLs on port 80/443 (TCP). For a complete list of ports, see AD Connector Communication Flow and Troubleshooting.
- For downloading upgrades, allow traffic on 443 (TCP) to **disthost.umbrella.com**.

Connector Account

To deploy the Connector, create a new user account in the AD domain. This account should have:

- The logon name (sAMAccountName) set to **Cisco_Connector**. You can use a custom username, but you must configure it with the required permissions.

- Select `Password never expires`.

> **Note**
>
> Passwords can not include backslashes, quotations (single or double), greater-than or less-than chevron brackets (**< >**), or colons.

- Assign `Read` and `Replicating Directory Changes` permissions. Alternatively, you can make the Connector account a member of the built-in `Enterprise Read-only Domain Controllers` group which will automatically assign these permissions.

> **Note**
>
> The Connector does an initial synchronization of the AD structure to Secure Access. After this, it detects changes to the AD structure and communicates these changes only. The detection of changes requires the `Replicating Directory Changes` permission, so the Connector cannot function without this permission. The `Replicating Directory Changes` permission is different from the `Replicating Directory Changes All` permission which enables the retrieval of password hashes. The Connector does not read password hashes and hence does not require the `Replicating Directory Changes All` permission.

Guidelines for AD Deployments with Secure Access Virtual Appliances

- The Connector account (**Cisco_Connector** or custom username) must be a member of the following built-in groups on each AD domain:
  - Enterprise Read-only Domain Controllers
  - Event Log Readers

> **Note**
>
> In a parent/child domain scenario, the `Enterprise Read-only Domain Controller` only exists in the parent domain. In this case, follow the instructions listed here to provide the required permissions for the Connector account. You must add other missing groups.

Prepare Your AD Environment

Describes Prepare Your AD Environment in Cisco Secure Access. The integration of Active Directory (AD) with a Secure Access Virtual Appliance (VA) requires that you register the deployed AD domain controllers or the Windows Event Log Collector and AD domains in Secure Access.

The integration of Active Directory (AD) with a Secure Access Virtual Appliance (VA) requires that you register the deployed AD domain controllers or the Windows Event Log Collector and AD domains in Secure Access. You must also deploy the Cisco AD Connector. For information about the AD Connector, see Manage AD Connectors.

You must have at least one VA deployed in the environment. For information about the Secure Access VAs, see Get Started with Virtual Appliances.

This guide describes how to register AD domain controllers or a centralized Windows Event Log Collector and AD domains in Secure Access.

About the AD Connector and Logon Events

Describes About the AD Connector and Logon Events in Cisco Secure Access. For each end-user on the AD domains, the AD Connector forwards the logon events to the deployed VAs.

For each end-user on the AD domains, the AD Connector forwards the logon events to the deployed VAs. The AD Connector can read logon events for users from the AD domain controllers at the site or a centralized Windows Event Log Collector. You can use an existing deployment of a centralized Windows Event Log Collector where domain controllers forward logon events for multiple AD domains or AD forests. For more information, see Support for Multiple AD Domains and AD Forests.

The domain controller or centralized Windows Event Log Collector record logon events by end users. The user's IP and username are made available through the AD Connector to the VA. The VA is a conditional DNS forwarder. The VA forwards DNS requests to the Secure Access DNS resolvers or, if bypass domains have been configured, forwards DNS requests to the organization's internal DNS servers. Secure Access applies the access rules in the policy to the DNS traffic and displays the end user identity information with the request in the reports and logs.

> **Note**
>
> You must deploy the VA, AD Connector, and domain controllers or centralized Windows Event Log Collector at the same Site registered with Secure Access. For information about Sites, see Manage Sites.

Prerequisites

Describes Prerequisites in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Additional Prerequisites for the Windows Event Log Collector

Describes Additional Prerequisites for the Windows Event Log Collector in Cisco Secure Access. The Cisco AD Connector account (Cisco_Connector or custom account as configured) should be added to the local Event Log Readers group on the Windows Event Log Collector machine.

- The Cisco AD Connector account (**Cisco_Connector** or custom account as configured) should be added to the local Event Log Readers group on the Windows Event Log Collector machine.
- On the Windows Event Log Collector machine, enable these firewall rules, which allow the server where you deployed the AD Connector to read the Windows event logs:
  - **Remote Event Log Management (NP-In)**
  - **Remote Event Log Management (RPC)**
  - **Remote Event Log Management (RPC-EPMAP)**
- Review all network access requirements. For more information, see AD Connector Communication Flow and Troubleshooting.

Integrate AD with Domain Controllers

Describes Integrate AD with Domain Controllers in Cisco Secure Access. Download the Windows Configuration script from Secure Access, and then run the script to add an AD domain controller in Secure Access.

Download the Windows Configuration script from Secure Access, and then run the script to add an AD domain controller in Secure Access.

- Support for Multiple AD Domains and AD Forests
- Verify Auditing of Logon Events on Domain Controllers
- Download the Windows Configuration Script for Domain Controllers
- Run the Configuration Script on the Domain Controllers
- Add a Domain Controller in Secure Access
- View the Registered AD Components in Secure Access

Support for Multiple AD Domains and AD Forests

Describes Support for Multiple AD Domains and AD Forests in Cisco Secure Access. Using domain controllers, you can integrate multiple AD domains or AD forests with Secure Access.

Using domain controllers, you can integrate multiple AD domains or AD forests with Secure Access. For each AD domain that integrates with Secure Access, deploy the Cisco AD Connector plus an additional AD Connector for redundancy.

Verify Auditing of Logon Events on Domain Controllers

Describes Verify Auditing of Logon Events on Domain Controllers in Cisco Secure Access. The AD integration with domain controllers requires each domain controller to audit logon events.

The AD integration with domain controllers requires each domain controller to audit logon events.

On each domain controller (excluding read-only domain controllers), enable the **Audit account logon events** to include `Success` and `Failure` if it is set to `No Auditing`.

By default, this group policy is set to log `Success` logon events and you should not modify it. Secure Access requires the **Audit account logon events** setting so that it knows whether a user has logged in successfully and can then compare that logon to subsequent events generated by that user.

If the Audit Policy is not set, the **Windows Configuration Script for Domain Controller** displays this error message:

```
"ERROR: "


--------------------------------------------------------------------------------


Your Group Policy for this Domain Controller is set to NOT audit successful
logon events!

You MUST edit the following Group Policy for all DCs:


Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events


Define that policy to audit Success attempts, gpupdate, and re-run this script!
```

Download the Windows Configuration Script for Domain Controllers

Provides instructions for completing the Download the Windows Configuration Script for Domain Controllers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Windows Configuration Script automates the permissions for the **Cisco_Connector** user.

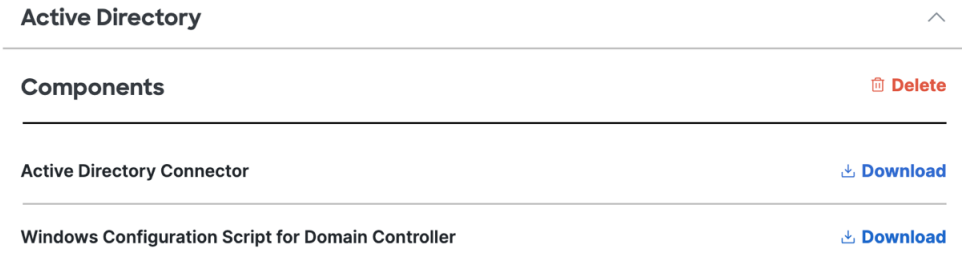
In Secure Access, download the **Windows Configuration Script for Domain Controller** script to the domain controllers in your environments.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. After an initial AD deployment, navigate to **Connect > Users and Groups > Users**, click **Configuration Management**, and expand **Active Directory**.
3. For **Windows Configuration Script for Domain Controller**, click **Download**.



4. Download and save the configuration script to a location on the machine where you plan to run it.

> **Note**
>
> The configuration script is written in Visual Basic Script and is in plain text.

Run the Windows Configuration Script for the Domain Controllers

Provides instructions for completing the Run the Windows Configuration Script for the Domain Controllers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Run the **Windows Configuration Script for Domain Controller** script on all of the domain controllers at each site, (excluding read-only domain controllers (RODCs)) and for each domain that will integrate with Secure Access. The configuration script prepares the domain controllers to communicate with the AD Connector. When you run the script, the domain controller should register with Secure Access.

> **Note**
>
> The script displays your current configuration, and then offers to auto-configure the domain controller. If the auto-configure steps are successful, the script offers to registers the domain controller with Secure Access. Registration only occurs if you accept this offer.

Repeat the steps to add your domain controllers in Secure Access. It is essential that each domain controller in each AD domain environment has the configuration script run on it in order for the service to work as expected, both for high availability and overall reliability.

> **Note**
>
> The configuration script is not an application or service. If you change the IP address or hostname of the domain controller, remove the previous instance of the domain controller and re-register the domain controller.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Procedure

1. As an administrator, open an elevated command prompt.

   > **Note**
   >
   > Before running the script, you must create the `Cisco_Connector` user account. Also, there are several Group Policies that affect system operation that may need manual configuration. The script displays the status of these settings and, if needed, provides instructions on how to change them.

2. Locate the **Windows Configuration Script for Domain Controller** file and run the script in the command prompt.

   > **Note**
   >
   > Substitute the Windows configuration script filename (including the `.wsf` file extension) in the `cscript` command.

```
cscript <Windows Configuration Script filename with extension> or cscript
<Windows Configuration Script filename with extension> --username
<sAMAccountName for custom user>
```

Add a Domain Controller in Secure Access

Provides instructions for completing the Add a Domain Controller in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

> **Note**
>
> The configuration script attempts to automatically register the domain controller with Secure Access. This requires the domain controller to support outbound connectivity to Secure Access. If your domain controller can support outbound connectivity to the Internet, ensure that network connectivity requirements are met for the domain controller to automatically register with Secure Access. For more information, see AD Connector Communication Flow and Troubleshooting.

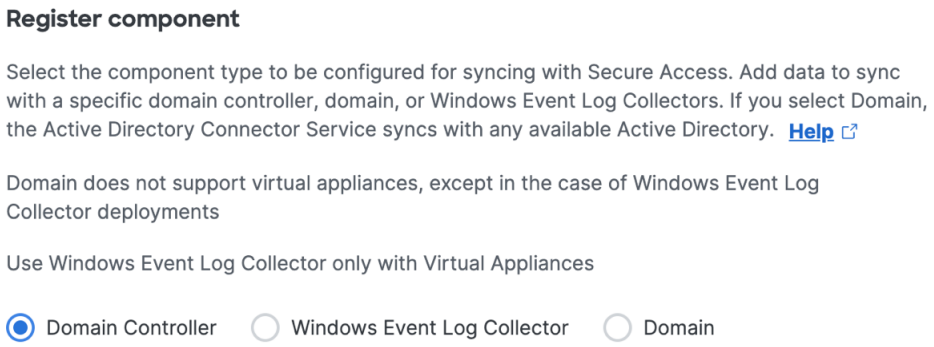
If the script did not register the domain controller with Secure Access, then add the information for each domain controller in Secure Access. After you add the domain controller, the domain controller syncs with Secure Access and you can view the status of the domain controller.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

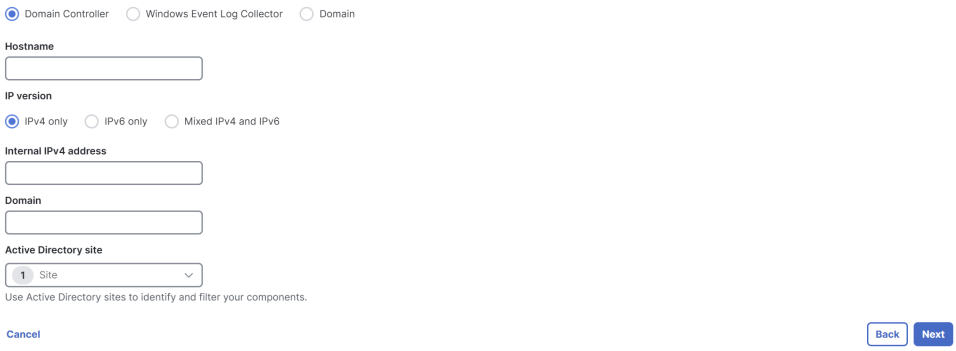
Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain Controller**.



3. Enter the details for the domain controller.
   - **Hostname**–The hostname of the server where the domain controller is deployed.
   - **IP version**–The IP address version to use. You can use **IPv4 only**, **IPv6 only**, or **Mixed IPv4 and IPv6**.
   - **Internal IPv4 address** / **Internal IPv6 address** / both –The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
   - **Domain**–The domain where the domain controller receives the events.
4. For **Active Directory site**, choose a Secure Access site to associate with the domain controller, and then click **Next**.

   For information about Sites, see Manage Sites.



5. Deploy the AD Connector.
   For more information, see Connect Active Directory to VAs.
6. On **Installed Active Directory components**, click **Done**.

View the Registered AD Components in Secure Access

Describes View the Registered AD Components in Secure Access. You can view the status for each deployed AD component in Secure Access.

You can view the status for each deployed AD component in Secure Access. Secure Access displays the hostname of the server where the domain controller is deployed and where you ran the configuration script. If you configured multiple sites and deployed VAs, make sure that the AD server is in the same site as the VAs that will receive DNS queries from the users in that AD domain.

For information about viewing the deployed AD components, see View AD Components in Secure Access.

Integrate AD with a Centralized Windows Event Log Collector

Describes Integrate AD with a Centralized Windows Event Log Collector in Cisco Secure Access. Before you begin, set up a centralized Windows Event Log Collector in your environment.

> **Note**
>
> Before you begin, set up a centralized Windows Event Log Collector in your environment. For more information, refer to Microsoft's documentation.

Add a centralized Windows Event Log Collector and AD domains in Secure Access. After you add the Windows Event Log Collector and AD domains, the AD Connector can forward the logon events to the VAs that are deployed in the environment.

Step 1 – Add the Windows Event Log Collector in Secure Access

Provides instructions for completing the Step 1 – Add the Windows Event Log Collector in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

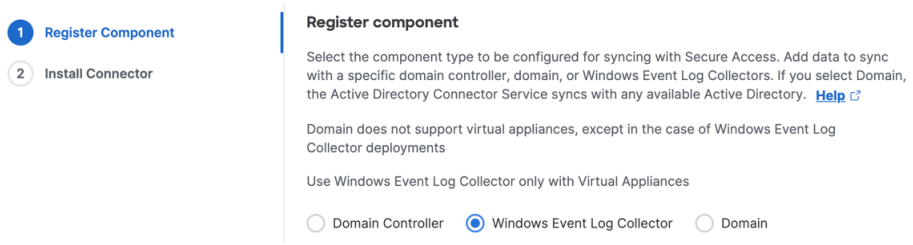
Add the configuration details for the centralized Windows Event Log Collector in Secure Access.

Before you begin

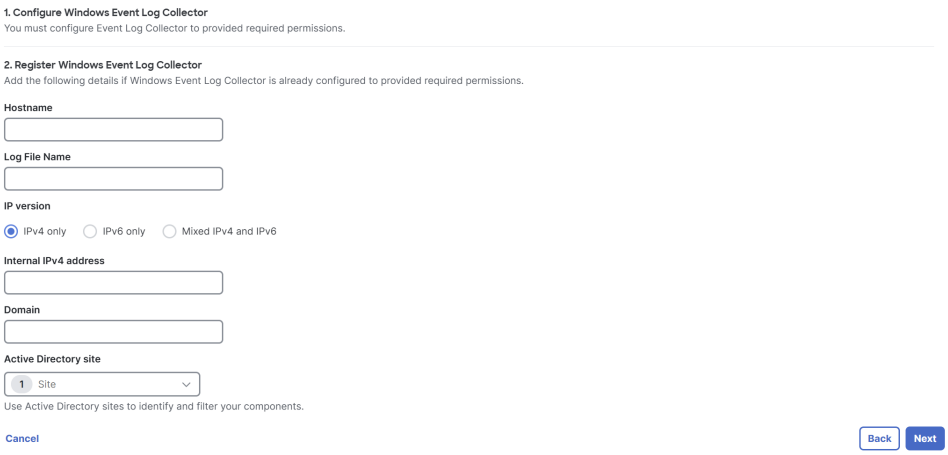
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Procedure

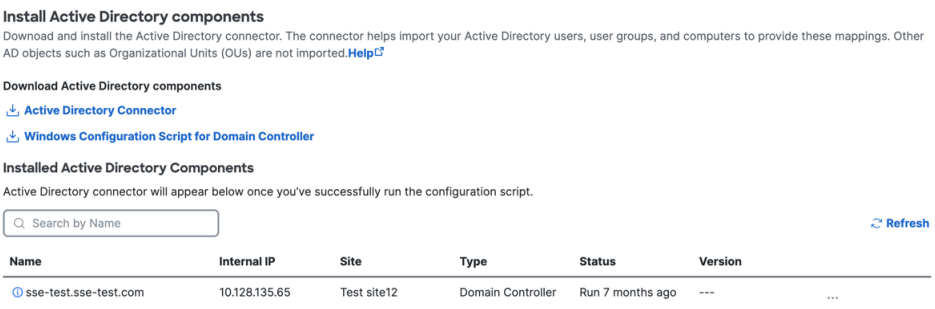
1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Windows Event Log Collector**.



3. Enter the following details for the deployed Windows Event Log Collector.
   - **Hostname**–The hostname of the server where the Windows Event Log Collector is deployed.
   - **Log File Name**–The name of the central log file for the Windows Event Log Collector.
   - **IP version**–The IP address version to use. You can use **IPv4 only**, **IPv6 only**, or **Mixed IPv4 and IPv6**.
   - **Internal IPv4 address** / **Internal IPv6 address** / both –The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
   - **Domain**–The domain where the Windows Event Log Collector receives the events.
4. For **Active Directory site**, select a Secure Access site that is associated with the Windows Event Log Collector, and then click **Next**.



5. Deploy the AD Connector. For more information, see Connect Active Directory to VAs.
6. On **Installed Active Directory components**, click **Done**.



Step 2 – Add the AD Domains in Secure Access

Provides instructions for completing the Step 2 – Add the AD Domains in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

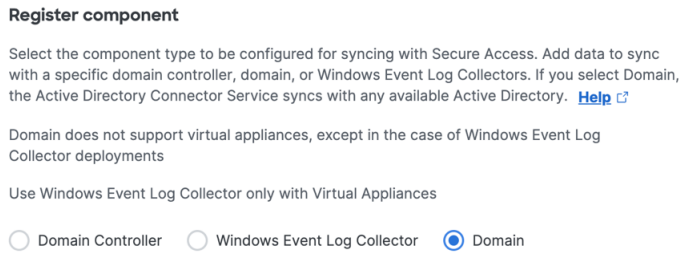
In Secure Access, add the AD domain where logon events occur and are sent to the Windows Event Log Collector. You must register each AD domain to enable the AD Connector to get the list of AD users and groups from the AD domains.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Procedure

1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Domain**.



3. For **Domain**, enter the AD domain.
4. For **Active Directory site**, choose a Secure Access site where the VA and domain controller are also deployed, and then click **Next**. For information about Sites, see Manage Sites.



5. On **Installed Active Directory components**, click **Done**.

Connect Active Directory to VAs

Describes Connect Active Directory to VAs in Cisco Secure Access. The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD.

The Cisco Active Directory (AD) Connector integrates Cisco Secure Access with your instance of Microsoft AD. Before you can provision users and groups from Active Directory, connect your instance of AD to Secure Access by deploying an AD Connector.

Install the AD Connector in the same Site as your deployed Secure Access Virtual Appliances.

The Cisco Active Directory (AD) Connector monitors one or more domain controllers in your environment.

- The AD Connector listens to user and computer logins through the security event logs, and then transmits IP-to-user and IP-to-computer mappings to your deployed Secure Access Virtual Appliances (VAs).
- The AD Connector synchronizes user-to-group, computer-to-group and group-to-group memberships with Secure Access, which enables you to create and enforce group-based settings and view user, computer, and group-based reports.

The AD Connector helps import your Active Directory (AD) users, groups and computers to provide these mappings.

> **Note**
>
> Only one AD Connector is required for each Secure Access Site. For redundancy, add an optional second AD Connector. If you are onboarding multiple AD domains through domain controller integrations, one AD Connector is required per AD domain per Umbrella site, with an optional second connector for redundancy if required.

This guide describes the steps to install the Cisco AD Connector for LDAP or LDAPS, and provision users and groups from your instance of Microsoft AD to Secure Access.

How to Configure the Setup of the AD Connector

Provides instructions for completing the How to Configure the Setup of the AD Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The deployment of the AD Connector has various components. You can configure the Cisco AD Connector to provision users and groups from Microsoft AD using LDAP or LDAPS (domain controller or domain).

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors and VAs.
- (Optional) Configure Authentication for the AD Connectors and VAs.
- Add the AD components in Secure Access. For more information, see Prepare Your AD Environment.

Procedure

1. (Optional) Configure authentication for the AD Connectors and Secure Access Virtual Appliances (VAs) in your environment.

   For more information, see Configure Authentication for AD Connectors and VAs on page 695

2. Add a domain controller or domain in Secure Access for LDAP or LDAPS deployments.

   For more information, see Prepare Your AD Environment.

(Optional) Specify AD Groups in Selective Sync File

Describes (Optional) Specify AD Groups in Selective Sync File in Cisco Secure Access. You can specify the AD Groups for the purpose of creating access rules in Secure Access.

You can specify the AD Groups for the purpose of creating access rules in Secure Access. Users and computers belonging to these Groups synchronize to Secure Access.

Supported Organizational Units

```
CN=My Group,OU=Organizational Unit,DC=sample,DC=local
```

Unsupported Organizational Units

```
OU=My OU,OU=Organizational Unit,DC=sample,DC=local
```

Sample File Entries

```
CN=Engineering,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Sales,CN=Builtin,DC=ciscoumbrella,DC=com
```

```
CN=Marketing,CN=Builtin,DC=ciscoumbrella,DC=com
```

Total Number of Groups Selected for Synchronization

Groups specified in the selective sync file and all of their subgroups–should not exceed 15,000. Also, these Groups should not be nested within more than five OU levels. Selective synchronization fails in both cases. If you can not meet either of these requirements, we recommend that you do not use the selective sync file. Instead, you can do a full AD tree synchronization.

Rename Selective Sync File After Upgrading to AD Connector v1.14.4

Describes Rename Selective Sync File After Upgrading to AD Connector v1.14.4 in Cisco Secure Access. If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file C:\CiscoUmbrellaADGroups.dat to C:\CiscoADGroups.dat.

If you use selective sync and upgrade the Cisco AD Connectors to v1.14.4 or later, you must rename the current selective sync file **C:\CiscoUmbrellaADGroups.dat** to **C:\CiscoADGroups.dat**.

> **Note**
>
> The selective sync file–previously named **CiscoUmbrellaADGroups.dat**–is not recognized by the Cisco AD Connector v1.1.4.4 or later.

After you rename the selective sync file, Secure Access automatically reads the selective sync file (**C:\CiscoADGroups.dat**) and syncs the Users in the specific Groups from AD to Secure Access. You are not required to restart the AD Connector service.

Create AD Groups in a Selective Sync File

Provides instructions for completing the Create AD Groups in a Selective Sync File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors and VAs.
- (Optional) Configure Authentication for the AD Connectors and VAs.
- Add the AD components in Secure Access. For more information, see Prepare Your AD Environment.

Procedure

1. Identify the AD Groups of interest.

   Users and computers belonging to these Groups synchronize to Secure Access. For each sub-tree, only the parent group needs to be specified. All AD groups, users, and computers that are part of this parent group are automatically included.

   > **Note**
   >
   > If you enabled `Selective Sync`, AD Users and Computers that are not members of Groups specified in **CiscoADGroups.dat** or their subgroups are not synchronized to Secure Access and are completely exempt from Secure Access access rules and reports.

2. Create a **CiscoADGroups.dat** file in the **C:** drive of each machine where the connector is installed.

   The connector only reads the **C:\CiscoADGroups.dat** file. If the file is incorrectly named or is not present in the **C:** drive, all groups are imported to Secure Access.

3. List the AD groups that need to be synchronized in `distinguished name` (DN) format in this file.
4. Ensure that there are no blank lines anywhere in the file.

   > **Note**
   >
   > If you are running multiple AD Connectors, the file **C:\CiscoADGroups.dat** should be present on each system running the connector and should be identical on each system.

Step 1 – Add the Windows Event Log Collector in Secure Access

Provides instructions for completing the Step 1 – Add the Windows Event Log Collector in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

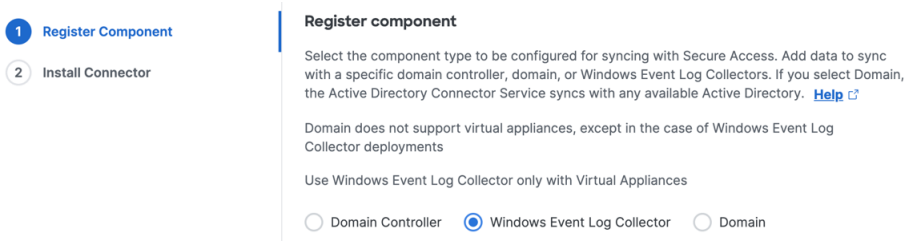
Add the configuration details for the centralized Windows Event Log Collector in Secure Access.

Before you begin

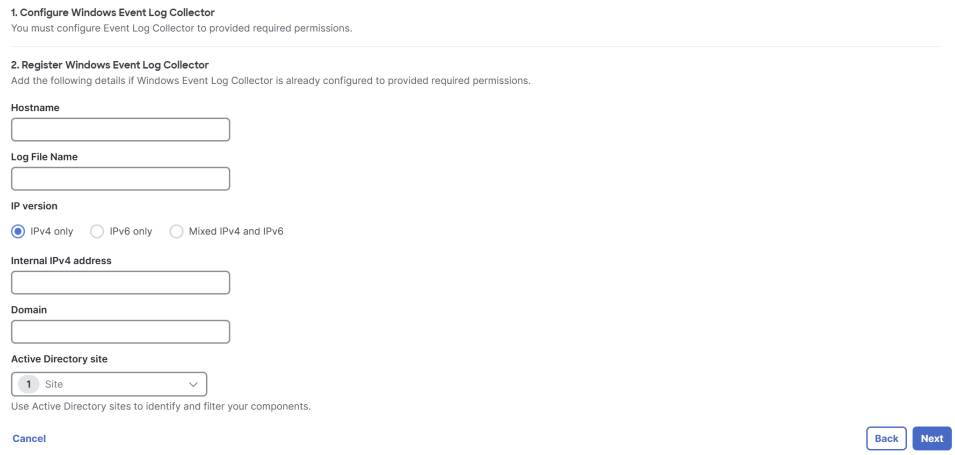
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the AD Connector, see Prerequisites for AD Connector and VAs.
- Deploy at least one Secure Access Virtual Appliance. For more information, see Get Started with Virtual Appliances.

Procedure

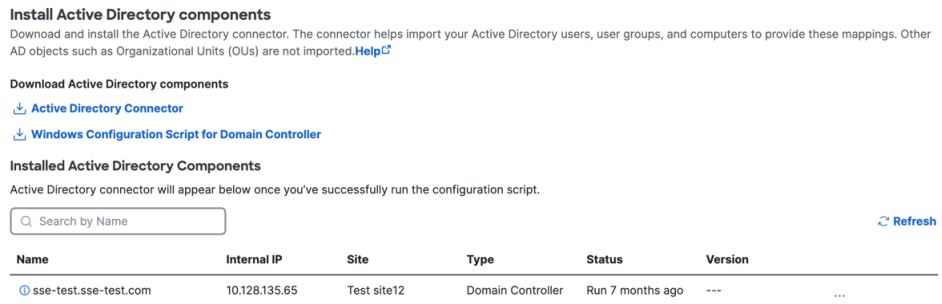
1. Navigate to **Connect > Users and Groups > Users**, click **Configuration Management > Integrate directories**, and then click **Active Directory**.
2. Click **Next**, and then choose **Windows Event Log Collector**.



3. Enter the following details for the deployed Windows Event Log Collector.
   - **Hostname**–The hostname of the server where the Windows Event Log Collector is deployed.
   - **Log File Name**–The name of the central log file for the Windows Event Log Collector.
   - **IP version**–The IP address version to use. You can use **IPv4 only**, **IPv6 only**, or **Mixed IPv4 and IPv6**.
   - **Internal IPv4 address** / **Internal IPv6 address** / both –The private IP address of the server where the domain controller is deployed. This field becomes available based on the IP version selection.
   - **Domain**–The domain where the Windows Event Log Collector receives the events.
4. For **Active Directory site**, select a Secure Access site that is associated with the Windows Event Log Collector, and then click **Next**.



5. Deploy the AD Connector. For more information, see Connect Active Directory to VAs.
6. On **Installed Active Directory components**, click **Done**.



Step 2 – Download the Active Directory Connector

Provides instructions for completing the Step 2 - Download the Active Directory Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Download the AD Connector from Secure Access to your server.

> **Note**
>
> When you download the AD Connector software package, and if you did not configure API key credentials for the AD Connectors, Secure Access displays a warning message. We recommend that you configure API keys for your AD Connectors. For more information, see Configure Authentication for AD Connectors and VAs.

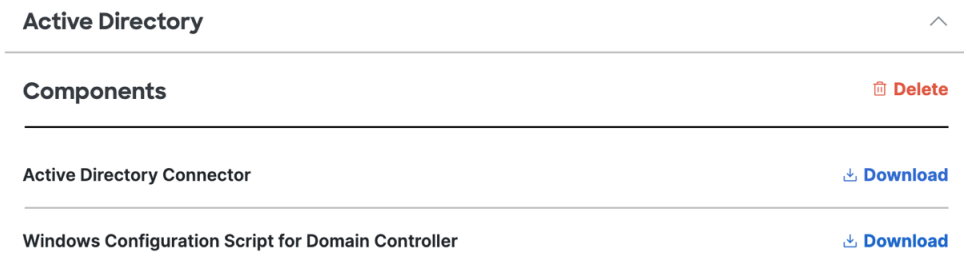
> **Note**
>
> You must download the ZIP file to the local machine where you plan to run it, or copy it locally from another machine. We do not recommend that you install the AD Connector from a network drive or run the **setup.msi** directly from the compressed file.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors and VAs.
- (Optional) Configure Authentication for the AD Connectors and VAs.
- Add the AD components in Secure Access. For more information, see Prepare Your AD Environment.

Procedure

1. Configure a server to run the AD Connector, and then sign in to Secure Access on that server.
2. Navigate to **Connect > Users and Groups > Users** and click **Provision Users**, or navigate to **Connect > Users and Groups > Groups** and click **Provision Groups**.
3. For **Provisioning Method**, click **Active Directory** or expand **Active Directory**.
4. For **Active Directory Connector**, click **Download** to save the AD Connector deployment package to the server. The deployment package is named: **OpenDNSAuditClient_vX.X.X.zip**.



Step 3 - Install the Active Directory Connector

Provides instructions for completing the Step 3 - Install the Active Directory Connector workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

As an administrator, extract the contents of the AD Connector ZIP file to a folder on the server, and then navigate to that folder.

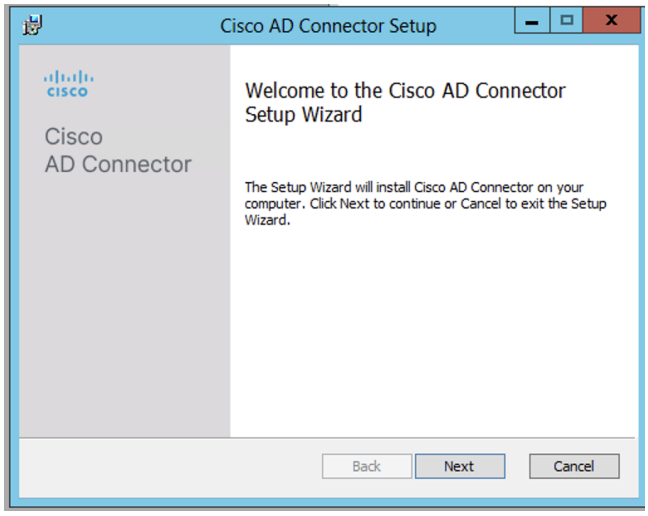
> **Note**
>
> If you run the AD Connector installer from the root directory of your server, you may encounter installation errors.

Before you begin

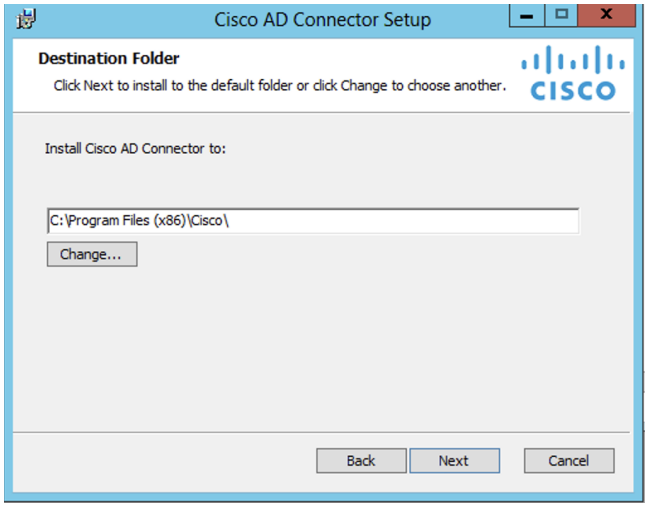
- Full Admin user role. For more information, see Manage Accounts.
- For information about the requirements for deploying the Cisco AD Connector, see Prerequisites for AD Connectors and VAs.
- (Optional) Configure Authentication for the AD Connectors and VAs.
- Add the AD components in Secure Access. For more information, see Prepare Your AD Environment.

Procedure

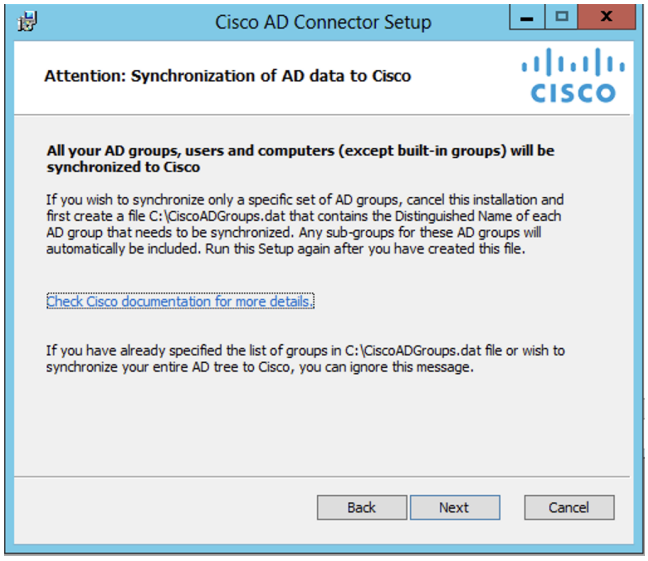
1. Run **setup.msi**, and then in the **Cisco AD Connector Setup** wizard, click **Next**.



2. Choose the directory on the server to install the Cisco AD Connector.



3. Confirm that you permit your AD Users and Groups to sync to Secure Access from the Cisco AD Connector.



4. Add your Active Directory credentials. Enter the **Username** of the Connector user (**Cisco_Connector** or custom username) and the **Password**.
5. Follow the remaining prompts in the setup, and when finished click **Finish**.

What to do next

- For more information, see View AD Components in Secure Access.

Change Connector Account Password

Describes Change Connector Account Password in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- For more information, see Change the Connector Account Password.

Configure Updates to AD Connectors

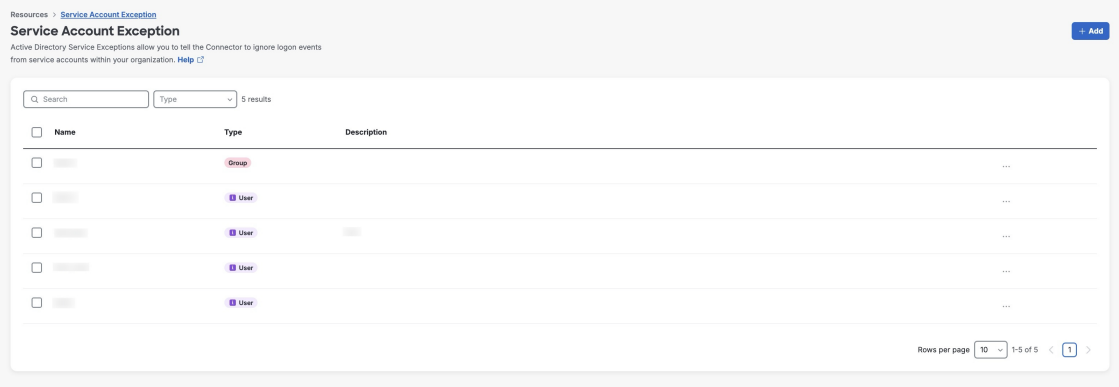
Describes Configure Updates to AD Connectors in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- For more information, see Configure Updates on AD Connectors.

Configure Active Directory User Exceptions in Secure Access

Describes Configure Active Directory User Exceptions in Secure Access. Many organizations use service accounts in order to perform scheduled tasks or automatic updates.

Many organizations use service accounts in order to perform scheduled tasks or automatic updates. If a user logs in while a service account is performing a scheduled task, the login event will be attributed to the service account. The result is that the policy for the service account will be applied instead of the user who is actively logged in and using the computer. The Active Directory User Exception should be applied to service accounts within your organization so that their login events to your Domain Controllers are ignored by the Cisco AD Connector.



Active Directory user exceptions are best used with:

- Service accounts that perform scheduled tasks: for example, software backups
- Service accounts that need to log in to the network to perform updates: for example, anti-virus clients
- Adding the IPs of RODCs which mirror events

> **Note**
>
> Do not use this feature with any user accounts you wish to have the login events recorded for, or accounts whose activity you wish to see in the reporting and that should have policy applied to it.

Set up an AD User Exception

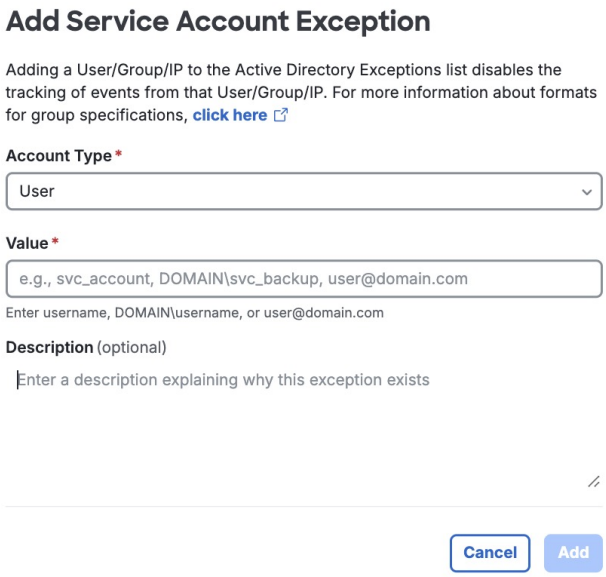
Provides instructions for completing the Set up an AD User Exception workflow in Cisco Secure Access. You must have at least one virutal appliance already associated with your Active Directory Connector server and account.

Before you begin

You must have at least one virtual appliance already associated with your Active Directory Connector server and account. See Prerequisites for AD Connectors and VAs for more information.

Procedure

1. Navigate to **Resources** > **Service Account Exception** and click **Add**.
2. Under **Account Type** choose **User**.



3. Under **Value** enter the AD Username or login (**sAMAccountName**) for the account in the format "Username" (not "Username@domain").

   This is not necessarily the same account name as the one displayed in the AD Users Identities in the dashboard. Confirm the account username in the Active Directory Users and Computers snap-in, not the Secure Access dashboard.

4. Enter an optional description and click **Create**. Note that in multi-AD domain environments, any user exception (sAMAccountName) configured is blocked for all AD domains.

Set up an AD Group Exception

Provides instructions for completing the Set up an AD Group Exception workflow in Cisco Secure Access. You must have at least one virutal appliance already associated with your Active Directory Connector server and account.

You can add Active Directory Groups to the exception list. The Cisco AD Connector will ignore login events generated by all users and computers belonging to the specified group and any sub-groups and exclude them from the AD mappings. This can be used for AD groups that comprise only service accounts, so that the individual service accounts need not be specified as exceptions.

Before you begin

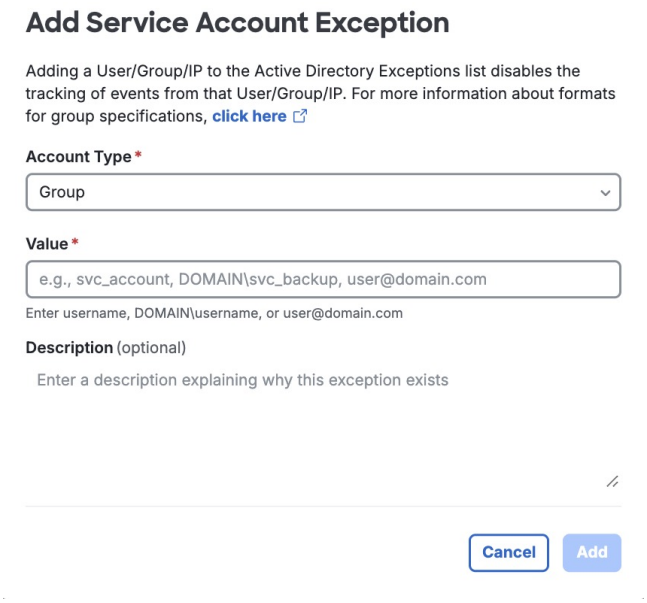
You must have at least one virtual appliance already associated with your Active Directory Connector server and account. See Prerequisites for AD Connectors and VAs for more information.

Adding Active Directory Organization Units (OUs) is **not** supported.

Procedure

---

1. Navigate to **Resources** > **Service Account Exception** and click **Add**.
2. Under **Account Type** choose **Group**.



3. Under **Value** enter the Distinguished Name (DN) for the AD group that you want to add as an exception. For example, enter the AD group name as `CN=Engineering,CN=Builtin,DC=mydomain,DC=com`.

   This is not the same format as the one displayed in the AD Groups Identities in the Umbrella Dashboard. Please confirm the group DN in the Active Directory Users and Computers snap-in, not the Umbrella Dashboard. The group DN is case sensitive. You can also use this Powershell command to confirm the distinguished name for AD groups: `Get-ADGroup -Identity <ADGroupName>`.

4. Enter an optional description and click **Create**.

Set up AD IP Address Exception

Provides instructions for completing the Set up AD IP Address Exception workflow in Cisco Secure Access. You must have at least one virutal appliance already associated with your Active Directory Connector server and account.

IP addresses can also be added to the Exceptions list. The Cisco AD Connector will ignore all the events generated by the configured IP to exclude it from the AD mappings. An example use case would be the IP address of a Netscaler server or a RODC that mirrors events.

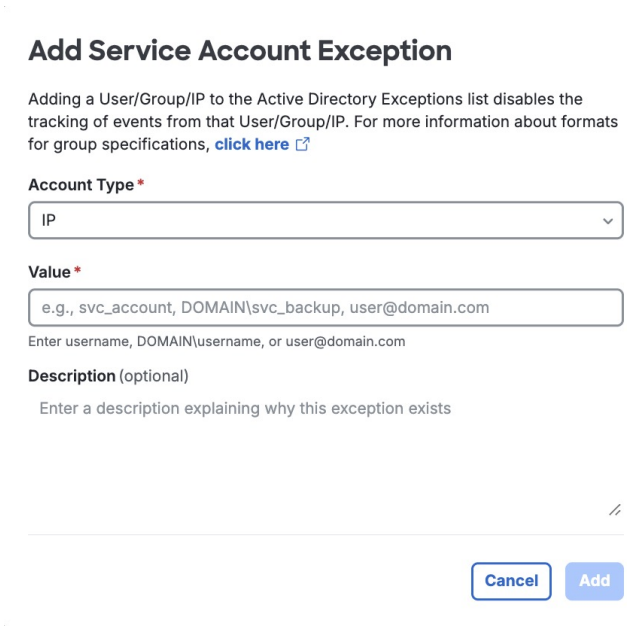
Before you begin

You must have at least one virtual appliance already associated with your Active Directory Connector server and account. See Prerequisites for AD Connectors and VAs for more information.

Procedure

---

1. Navigate to **Resources** > **Service Account Exception** and click **Add**.
2. Under **Account Type** choose **IP**.



3. Under **Value** enter the IP address.

   IP address ranges are not supported. Only individual IP addresses, such as `10.20.30.40`, are supported.

4. Enter an optional description and click **Create**.

Multiple AD Domains with Secure Access Sites

Describes Multiple AD Domains with Secure Access Sites. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Cisco Secure Access Sites let administrators create separate Secure Access deployments. Each Secure Access Site is an isolated deployment where components only communicate with other components in the same Secure Access Site. Secure Access Sites are a container to isolate sections of a large multi-site network into groups which only sync to the other components in the container. For example, Secure Access sites may be North America, Asia, and Europe or Northeast, California, Atlanta office, South Region, and London, and each Secure Access Site may be one or a combination of Active Directory (AD) sites.

This is useful in AD environments containing locations with high-latency connections, or in environments with locations whose internal IP space overlaps.

Active Directory Sites and Secure Access Sites

Describes Active Directory Sites and Secure Access Sites. A site represents a set of computers connected by a high-speed network, such as a local area network (LAN).

A site represents a set of computers connected by a high-speed network, such as a local area network (LAN). Typically, all computers in the same physical site reside in the same building or perhaps the same campus network. AD and Umbrella both use the term "sites", and while related, have slightly different meanings.

Active Directory Sites and Services

- For AD, a site object represents the actual directory data that is replicated between domain controllers.
- AD sites are used to manage the objects that represent the site, and the servers that reside in the site.

Secure Access Sites

- A Secure Access Site refers to a set of components—Virtual Appliances (VAs), Cisco AD Connectors, and domain controllers—that communicate only with each other.
- A Secure Access Site is more than a label and is more like a container. A Secure Access Site is not the same as an AD site. Multiple AD sites can be part of an Secure Access Site, but one AD site should not be split into multiple Secure Access Sites.
- A site must have a minimum of two VAs, and one connector and domain controller for an AD integration.

Because Secure Access Sites act as isolated deployments, each Secure Access Site must have a minimum of two VAs. If AD integration is also being used, each site must additionally contain a minimum of one AD connector and all domain controllers against which a user in that location authenticates.

When to Use Secure Access Sites

- You need to limit WAN traffic between locations and are using AD sites to limit authentication to local servershttp://technet.microsoft.com/en-us/library/cc782048(v=ws.10).aspx.
- Your locations communicate between a NAT device, which causes the internal IP address of an end machine to be lost when communicating between locations.
- Your locations use overlapping internal IP ranges.
- You have locations which have high-latency connections between them—for example, branches in different continents. High latency connections, especially between the connector and the VAs, can result in delays to updates for user mappings.

Caveats

The isolation of the components in a given Secure Access Site means that a specific VA will only be aware of users who have authenticated against domain controllers assigned to the same Secure Access Site. As a result, we do not recommend using multiple Secure Access Sites in a single AD site, even if that AD site spans multiple geographical locations. In such a scenario, users in a location may still authenticate against a DC in a different location, and thus the Secure Access components may miss user mappings.

Use Secure Access Sites

Describes Use Secure Access Sites and outlines Active Directory Only. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Configure individual Secure Access Sites as if they are complete deployments. Ensure that there are at least two VAs, one AD server and one AD Connector assigned to each site. Verify a complete, functioning deployment at each site before moving on to the next site. For more information, see Manage Site for VA.

Active Directory Only

If you change the location of a Secure Access VA, the AD Connector, or domain controller after you've installed the connector service, you must Stop/Start the AD Connector service on each connector for the Sites through the Services management tool in Windows.

23 User Authentication Profiles

Topics:

- Manage User Authentication Profiles
- About Single Sign-On for Users
- Edit an SSO Authentication Profile
- Delete SSO Authentication Profile

Provides an overview of User Authentication Profiles in Cisco Secure Access, including Manage User Authentication Profiles, About Single Sign-On for Users, and Edit an SSO Authentication Profile. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage User Authentication Profiles

Describes Manage User Authentication Profiles in Cisco Secure Access. Cisco Secure Access supports the use of Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) to authenticate users.

Cisco Secure Access supports the use of Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) to authenticate users. Secure Access requires that users are authenticated before they can connect to internet-bound destinations through the Secure Access Secure Web Gateway (SWG) or connect with Secure Access Zero Trust Access (ZTA) to private destinations.

To get started, add a single sign-on (SSO) authentication profile in Secure Access for each user authentication IdP integration. You must associate one of the organization's configured provisioning profiles (user directory) with the SSO authentication profile.

Add User Authentication Profiles

When you configure a user authentication profile, associate a provisioning profile for a cloud IdP with the user authentication profile. You can only assign one unique provisioning IdP in the user authentication profile.

- For more information, see Add SSO Authentication Profiles.

About Single Sign-On

- For more information, see About Single Sign-On for Users.

View User Authentication Profiles

After you add a user authentication profile in Secure Access, you can view the list of configured user authentication profiles for the organization. For more information, see View SSO Authentication Profiles.

Edit a User Authentication Profile

After you add a user authentication profile, you can edit the profile in Secure Access. For more information, see Edit an SSO Authentication Profile.

Delete a User Authentication Profile

After you add a user authentication profile, you can remove the profile in Secure Access. For more information, see Delete an SSO Authentication Profile.

Requirements for Configuring SSO Authentication Profiles

Describes Requirements for Configuring SSO Authentication Profiles in Cisco Secure Access. When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile.

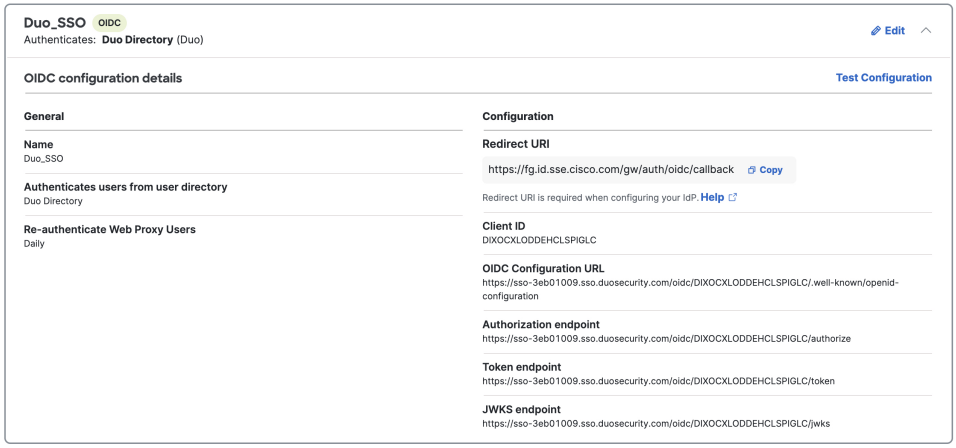
When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

About the Default Provisioning Profile

Describes About the Default Provisioning Profile in Cisco Secure Access. If you previously integrated an SSO IdP that supported SSO authentication but Secure Access did not have the option to assign a user directory to the integration, Secure Access will associate the Default Profile for this integration.

If you previously integrated an SSO IdP that supported SSO authentication but Secure Access did not have the option to assign a user directory to the integration, Secure Access will associate the Default Profile for this integration.

The Default Profile describes the integration of an existing IdP in Secure Access using the organization's ID and the SCIM token that you generated for the IdP integration.



Add SSO Authentication Profiles

Provides instructions for completing the Add SSO Authentication Profiles workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

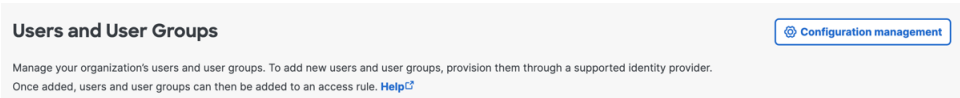
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

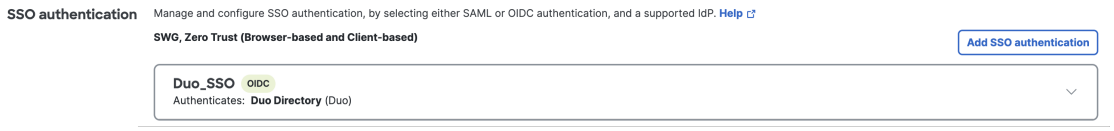
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

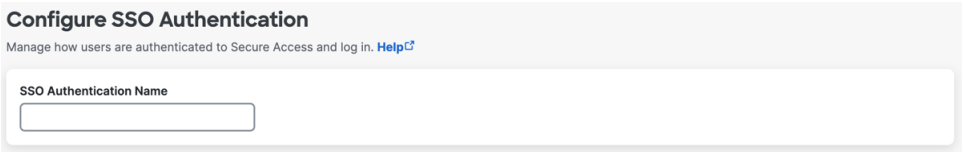
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



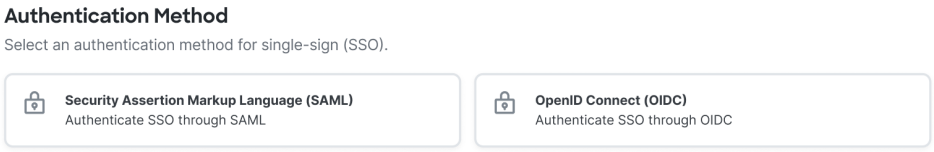
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



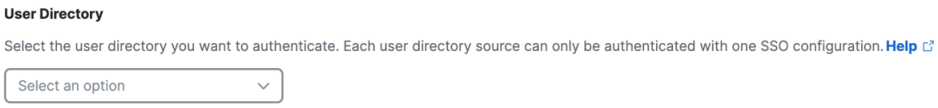
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

View SSO Authentication Profiles

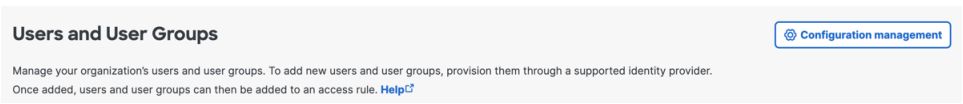
Provides instructions for completing the View SSO Authentication Profiles workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

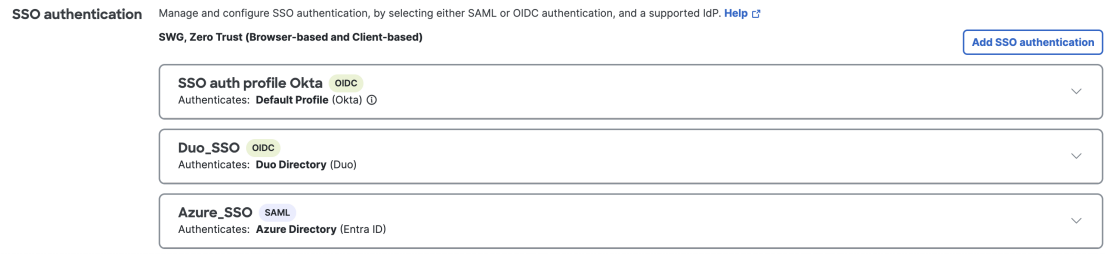
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



2. Navigate to **SSO authentication**. Secure Access lists the configured SSO authentication profiles.



About Single Sign-On for Users

Describes About Single Sign-On for Users in Cisco Secure Access. When a user connects to a destination through the Cisco Secure Access Secure Web Gateway (SWG) or with Zero Trust Access, Secure Access presents a sign-in dialog window.

When a user connects to a destination through the Cisco Secure Access Secure Web Gateway (SWG) or with Zero Trust Access, Secure Access presents a sign-in dialog window.

Secure Access requests that the user enter their single sign-on (SSO) credentials in the dialog window. After Secure Access validates the user's credentials, the user is connected to the destination.

Sign-On for Provisioned Users

Describes Sign-On for Provisioned Users in Cisco Secure Access. An administrator provisions the organization's users and groups in the Secure Access and adds a user authentication profile in Secure Access.

An administrator provisions the organization's users and groups in the Secure Access and adds a user authentication profile in Secure Access.

Scenario

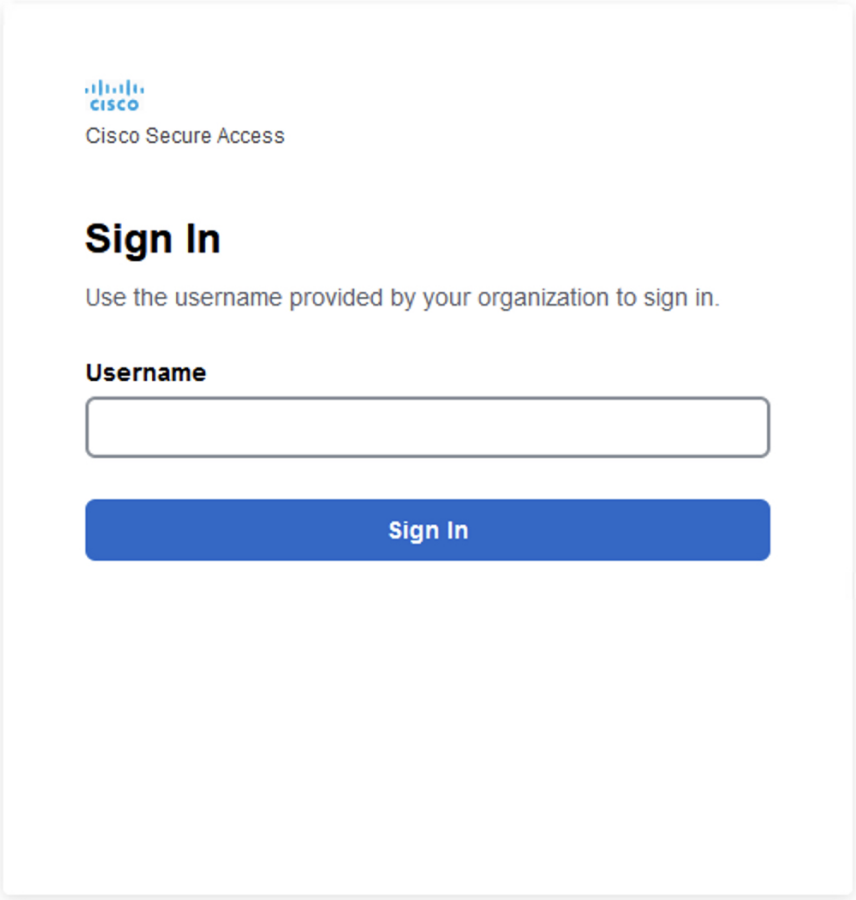
Describes Scenario in Cisco Secure Access. A user attempts to connect to a web destination that is protected by the Secure Access Secure Web Gateway (SWG) or connects to a private destination through Secure Access Zero Trust Access.

A user attempts to connect to a web destination that is protected by the Secure Access Secure Web Gateway (SWG) or connects to a private destination through Secure Access Zero Trust Access.

Sample Sign-On Window

Describes Sample Sign-On Window in Cisco Secure Access. Secure Access presents a SSO dialog window that requires the provisioned user to enter their SSO credentials.

Secure Access presents a SSO dialog window that requires the provisioned user to enter their SSO credentials.



Sign-On for Non-Provisioned Users

Describes Sign-On for Non-Provisioned Users in Cisco Secure Access. A user is not provisioned in the Secure Access organization through an identity provider (IdP) or other method.

A user is not provisioned in the Secure Access organization through an identity provider (IdP) or other method.

Scenario

Describes Scenario in Cisco Secure Access. A user attempts to connect to a web destination that is protected by the Secure Access Secure Web Gateway (SWG) or connects to a private destination through Secure Access Zero Trust Access.

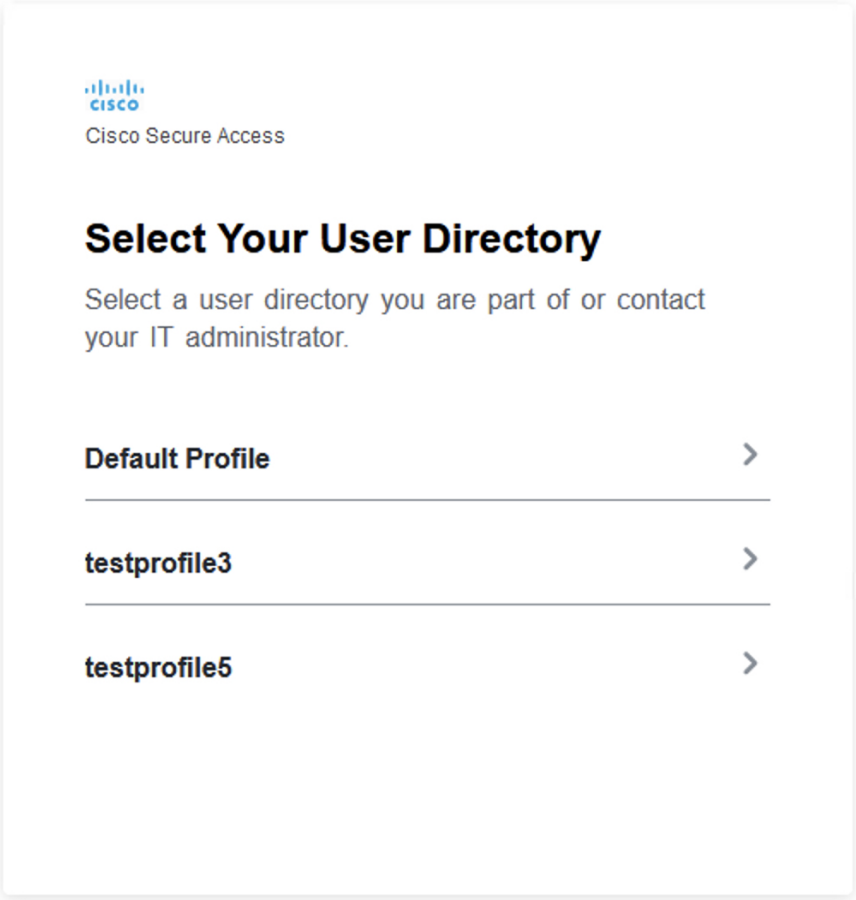
A user attempts to connect to a web destination that is protected by the Secure Access Secure Web Gateway (SWG) or connects to a private destination through Secure Access Zero Trust Access.

Sample Sign-On Window

Describes Sample Sign-On Window in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Secure Access presents a dialog window. The user must:

- Choose a user directory for a configured provisioning profile.
- Enter their SSO credentials to sign into Secure Access.



Edit an SSO Authentication Profile

Describes Edit an SSO Authentication Profile in Cisco Secure Access. After you add an SSO authentication profile in Cisco Secure Access, you can modify the name and settings of the profile.

After you add an SSO authentication profile in Cisco Secure Access, you can modify the name and settings of the profile. The user authentication profile describes the settings that are required to integrate a single sign-on (SSO) authentication identity provider (IdP) with Secure Access. An integrated SSO IdP authenticates user requests for destinations through the Secure Access Secure Web Gateway (SWG) and connections to private destinations with Zero Trust Access.

(OIDC Only) Get Metadata for OIDC Configuration URL

Describes (OIDC Only) Get Metadata for OIDC Configuration URL in Cisco Secure Access. For the integration of Microsoft Entra ID SSO authentication, see Get Entra ID OIDC Configuration URL.

- For the integration of Microsoft Entra ID SSO authentication, see Get Entra ID OIDC Configuration URL.
- For the integration of Okta SSO authentication, see Get Okta OIDC Configuration URL.

Edit SAML User Authentication Profile

Update the settings for the SAML user authentication profile.

After you add an SSO authentication profile in Cisco Secure Access, you can modify the name and settings of the profile. The user authentication profile describes the settings that are required to integrate a single sign-on (SSO) authentication

identity provider (IdP) with Secure Access. An integrated SSO IdP authenticates user requests for destinations through the Secure Access Secure Web Gateway (SWG) and connections to private destinations with Zero Trust Access.

If multiple SSO profiles are available you can move, or unassign, the default profile as the designated option for the **Authenticates users from user directory** setting.

> **Note**
>
> If the SAML configuration using the Default Profile under the **Authenticates users from user directory** setting is changed to a new user SSO authentication profile the system-provided default profile is permanently deleted and cannot be used again. You must manually recreate the configuration to retain it.

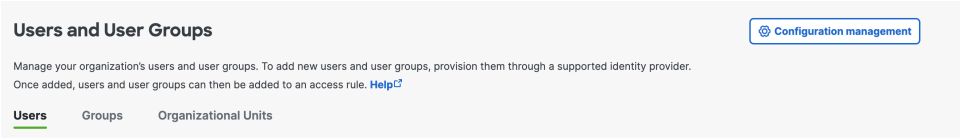
Update the settings for the SAML user authentication profile.

Before you begin

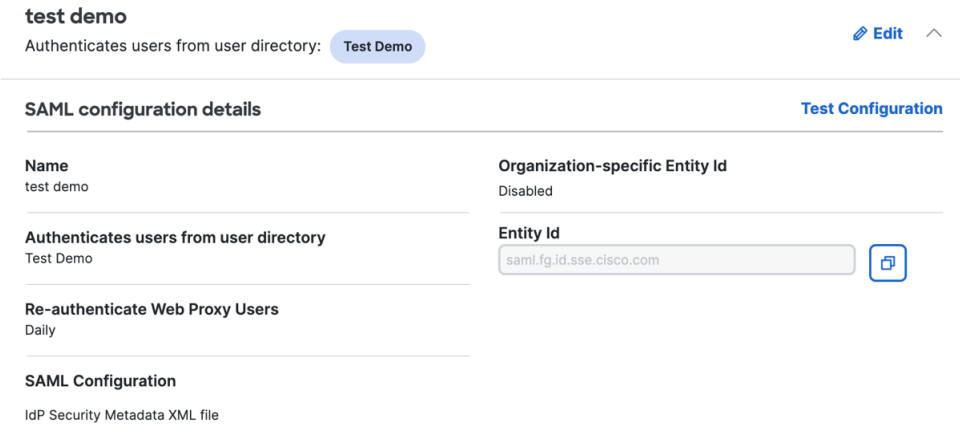
- Full Admin user role. For more information, see Manage Accounts.

Procedure

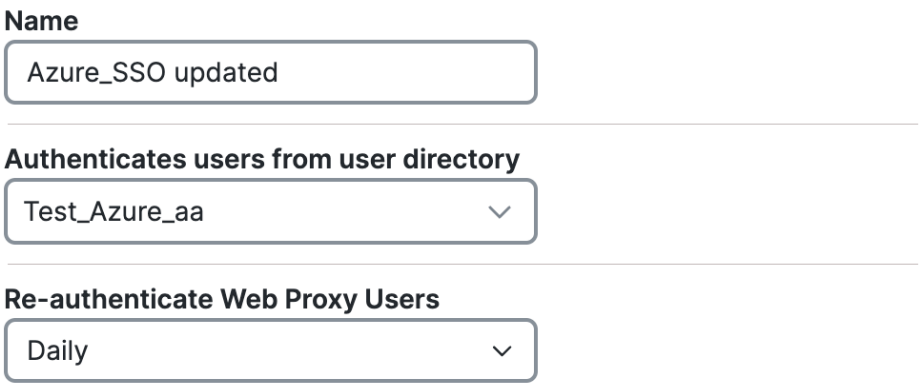
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



2. Navigate to **SSO authentication**, and then expand an SAML user authentication profile.
3. Click **Edit**.



4. For **Name**, update the name of the profile.
5. For **Authenticates users from user directory**, choose the name of an integrated user directory for the provisioning IdP.



6. For **Re-authenticate Web Proxy Users**, choose the frequency that Secure Access requires SSO authentication.
7. For **SAML Configuration**, select the type of the configuration.
   - For **IdP Security Metadata XML file**, upload the SAML Metadata XML file.
   - For **Manual Input**, enter the SAML Metadata attributes.
8. Click **Save**.

Edit OIDC User Authentication Profile

Update the settings for the OIDC user authentication profile.

After you add an SSO authentication profile in Cisco Secure Access, you can modify the name and settings of the profile. The user authentication profile describes the settings that are required to integrate a single sign-on (SSO) authentication identity provider (IdP) with Secure Access. An integrated SSO IdP authenticates user requests for destinations through the Secure Access Secure Web Gateway (SWG) and connections to private destinations with Zero Trust Access.

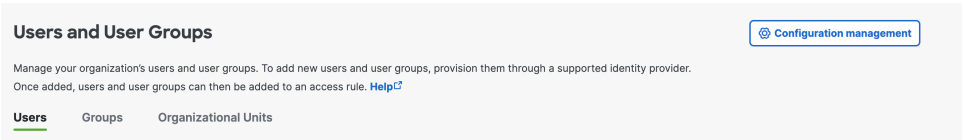
Update the settings for the OIDC user authentication profile.

Before you begin

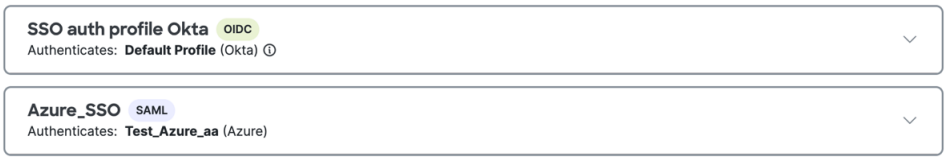
- Full Admin user role. For more information, see Manage Accounts.

Procedure

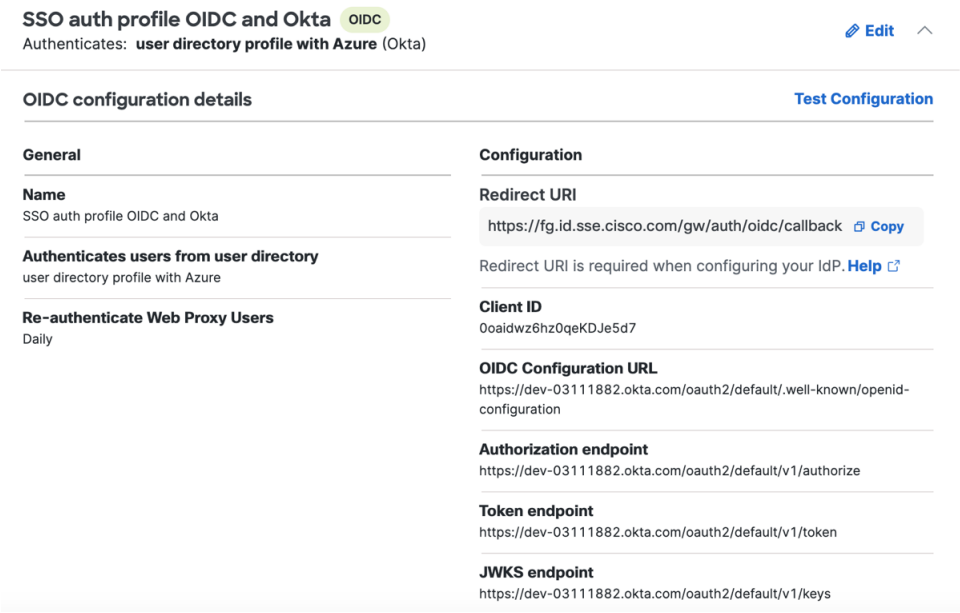
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



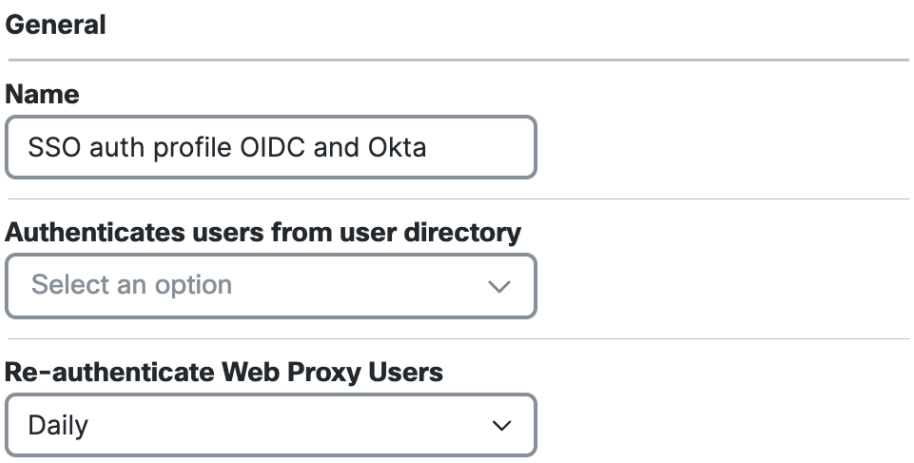
2. Navigate to **SSO authentication**, and then expand an OIDC user authentication profile.



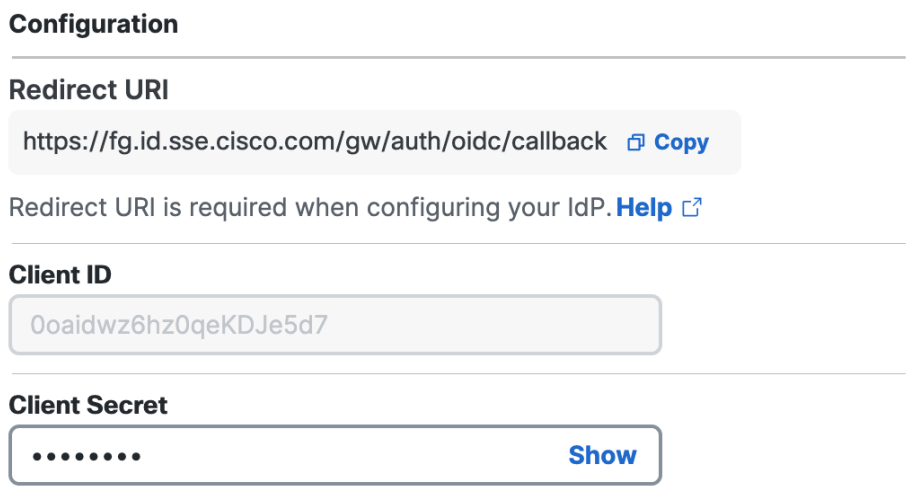
3. Click **Edit**.



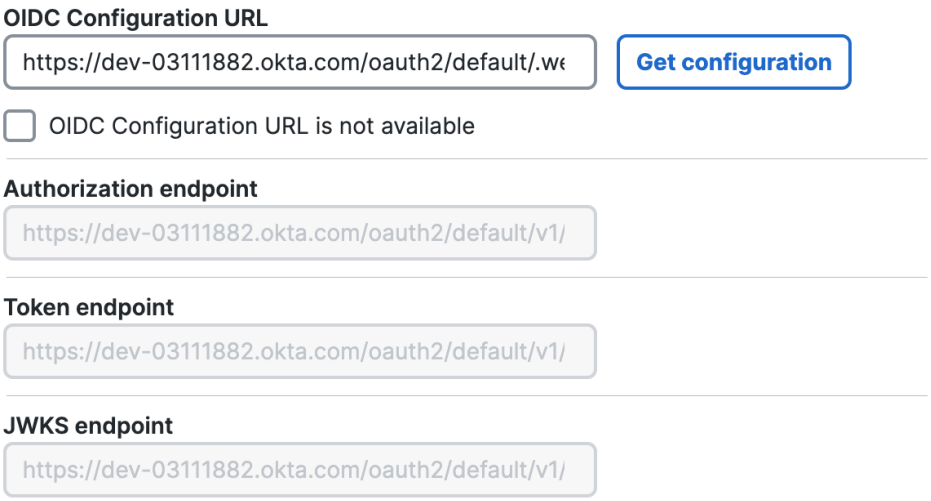
4. For **Name**, update the name of the profile.
5. For **Authenticates users from user directory**, choose the name of an integrated user directory for the provisioning IdP.



6. For **Re-authenticate Web Proxy Users**, choose the frequency that Secure Access requires SSO authentication.
7. For **Client Secret**, enter the new client secret that you generated in your instance of the SSO authentication IdP.



8. For **OIDC Configuration URL**, enter the configuration URL for the SSO authentication IdP.



9. Complete the configuration of the **Authorization endpoint**, **Token endpoint**, **JWKS endpoint** fields.
   a) Click **Get configuration**.

      Secure Access uses the **OIDC Configuration URL** to populate the settings for the integration's endpoint-related fields.

   b) Check **OIDC Configuration URL is not available**, and then enter the authorization endpoint fields manually.
10. Click **Save**.

Delete SSO Authentication Profile

Describes Delete SSO Authentication Profile in Cisco Secure Access. After you add a single sign-on (SSO) authentication profile in Cisco Secure Access, you can remove the profile.

After you add a single sign-on (SSO) authentication profile in Cisco Secure Access, you can remove the profile. An integrated SSO IdP authenticates user requests for destinations through the Secure Access Secure Web Gateway (SWG) and connections to private destinations with Zero Trust Access. When you delete the SSO authentication profile, users can no longer use the SSO IdP to authenticate and get access to destinations.

Delete SAML User Authentication Profile

Provides instructions for completing the Delete SAML User Authentication Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

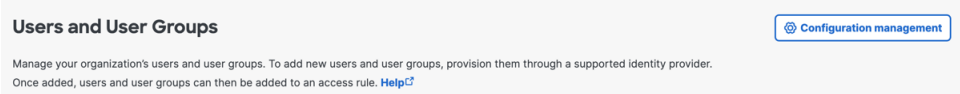
Remove the integration of an SSO authentication IdP in Secure Access.

Before you begin

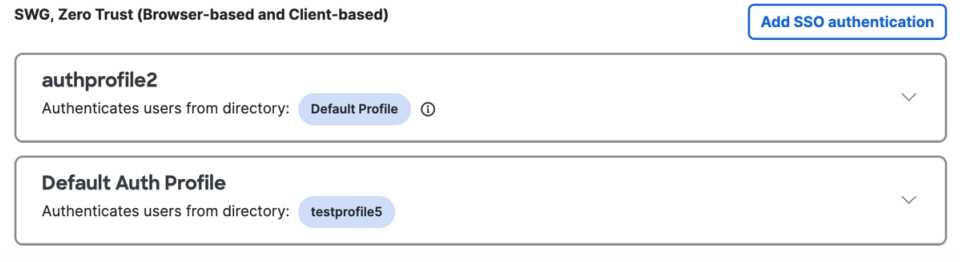
- Full Admin user role. For more information, see Manage Accounts.

Procedure

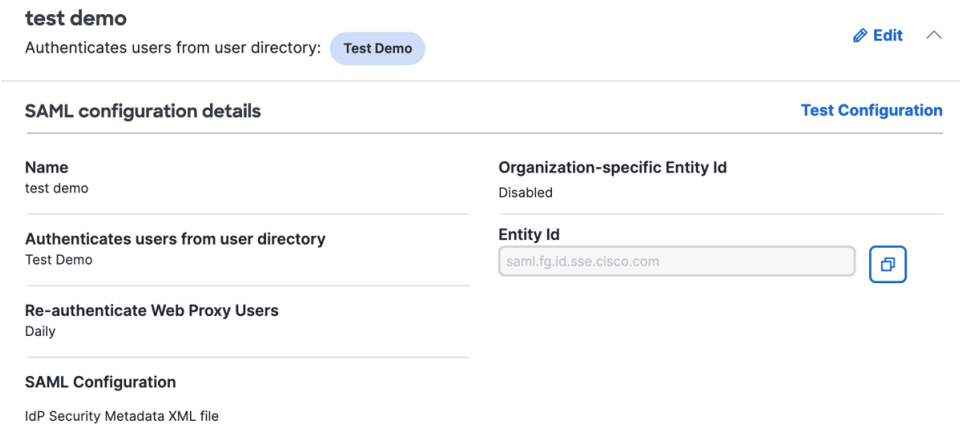
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



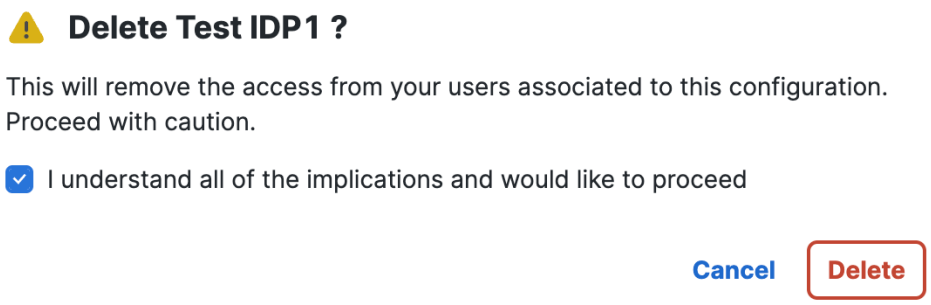
2. On **Configuration Management**, navigate to **SSO authentication**, and then expand a user authentication profile.



3. Click **Edit**, and then click **Delete**.



4. Check **I understand all of the implications and would like to proceed**, and then click **Delete** to remove the SSO authentication IdP in Secure Access.



Delete OIDC User Authentication Profile

Provides instructions for completing the Delete OIDC User Authentication Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

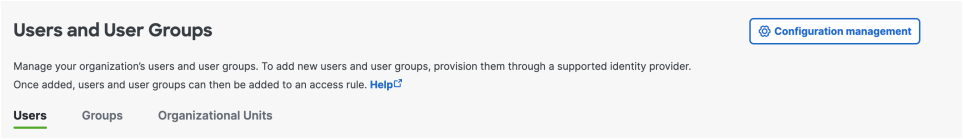
Remove the integration of an SSO authentication IdP in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

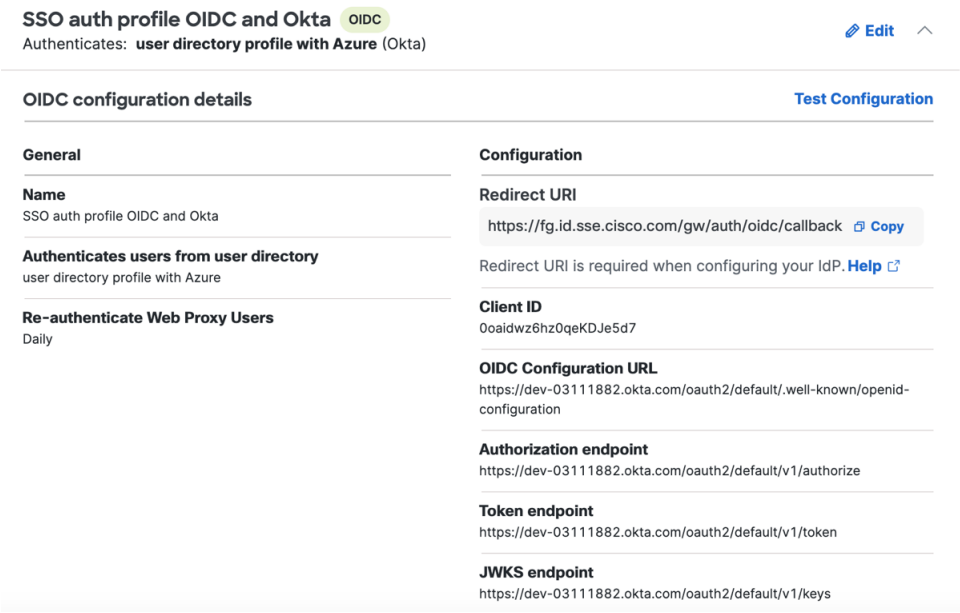
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



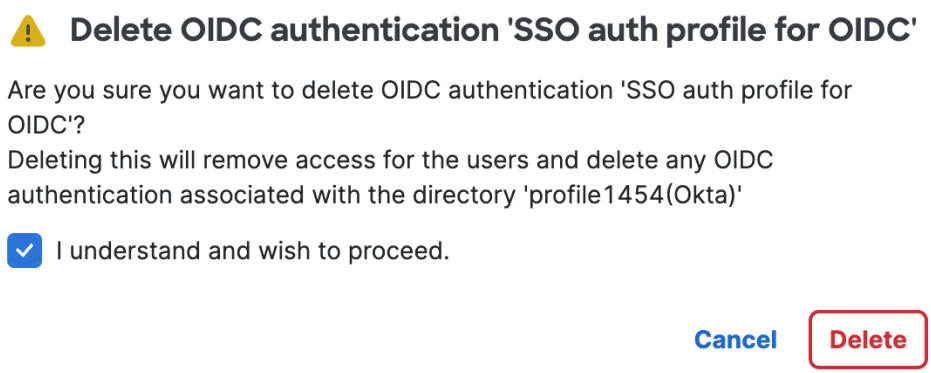
2. On **Configuration Management**, navigate to **SSO authentication**, and then expand an SSO authentication profile.



3. Click **Edit**, and then click **Delete**.



4. Check **I understand all of the implications and would like to proceed**, and then click **Delete** to remove the SSO authentication IdP in Secure Access.



24 Integrations with Open ID Connect Identity Providers

Topics:

- Configure Integrations with OIDC Identity Providers
- Configure Duo for OpenID Connect
- Configure Okta for OpenID Connect
- Configure Microsoft Entra ID for OpenID Connect

Provides an overview of Integrations with Open ID Connect Identity Providers in Cisco Secure Access, including Configure Integrations with OIDC Identity Providers, Configure Duo for OpenID Connect, and Configure Okta for OpenID Connect. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Configure Integrations with OIDC Identity Providers

Describes Configure Integrations with OIDC Identity Providers in Cisco Secure Access. Cisco Secure Access enables you to connect securely to the internet, web destinations in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications.

Cisco Secure Access enables you to connect securely to the internet, web destinations in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications. To create more granular access rules and to authenticate users connecting on networks or network tunnels or with Zero Trust Access (ZTA), you can integrate an OpenID Connect (OIDC) identity provider (IdP) with Secure Access.

Secure Access supports OIDC for single sign-on (SSO) authentication of users through the integration with Okta and Microsoft Entra ID.

Once users in your organization are configured to use SSO through an IdP, the IdP manages all authentication requests. A user authenticates to the SSO authentication IdP, automatically signs in to Secure Access, and is authorized to connect to the requested destination.

Configure Identity Providers for OIDC Authentication

Follow the procedure in the configuration guides to integrate an SSO authentication IdP for Open ID Connect with Secure Access.

- Configure Duo for OpenID Connect
- Configure Okta for OpenID Connect
- Configure Microsoft Entra ID for OpenID Connect

Secure Access Redirect URI

The Secure Access **Redirect URI** is used when you set up the integration of Secure Access for OIDC in the SSO authentication IdP app.

```
https://fg.id.sse.cisco.com/gw/auth/oidc/callback
```

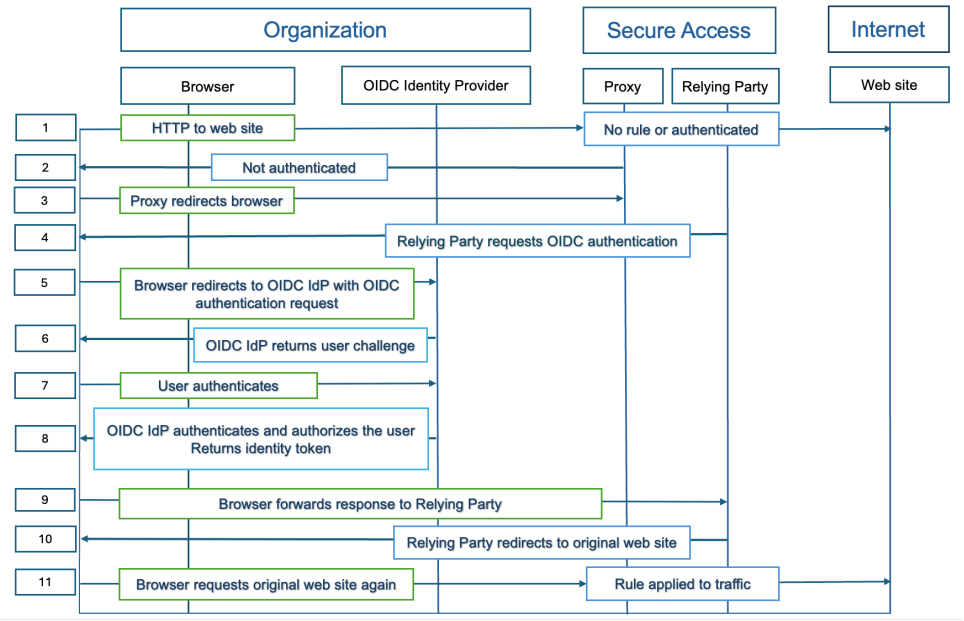
About Using OpenID Connect with Secure Access

Describes About Using OpenID Connect with Secure Access. OpenID Connect (OIDC) is an identity protocol that extends the OAuth 2.0 protocol.

OpenID Connect (OIDC) is an identity protocol that extends the OAuth 2.0 protocol. The OIDC authentication flow describes the authentication of a request for a destination by the user.

The OIDC authentication flow with Secure Access is described as follows:

- A user requests a web site. Secure Access (proxy) receives the request and determines if the user is authenticated to get the destination. If the user is not authenticated, the browser redirects the request to the Relying party (Secure Access). The Relying party requests that the OIDC IdP authenticate the user.
- Then, the OIDC IdP returns a challenge to the user and the user authenticates to the OIDC IdP. If valid, the OIDC IdP returns an identity token to the user. The user's browser forwards the response to the Relying party, and then the Relying party redirects the original request for the web destination to Secure Access.
- If the rules in the organization's Access policy match the traffic, Secure Access applies the rules and ensures that the connection to the web site is secure.



Use Cases – SSO Authentication

Describes Use Cases - SSO Authentication in Cisco Secure Access. Secure Access supports the OIDC protocol to authenticate users and provide seamless connections to web resources and private resources from user devices.

Secure Access supports the OIDC protocol to authenticate users and provide seamless connections to web resources and private resources from user devices.

Secure Internet Access—Networks and Network Tunnels

- Secure web gateway–The Cisco Secure Access Secure Web Gateway (SWG) uses OIDC to authenticate and authorize web requests from user devices sent over networks and network tunnels. Internet traffic is protected by the Secure Access DNS and Web security layers. The Secure Access SWG is not an open proxy. Secure Access must trust the source that forwards web traffic to it, whether the source is a network or network tunnel.

Zero Trust Access with the Cisco Secure Client

- Secure Access Zero Trust Access (ZTA) connections can use OIDC to authenticate and authorize requests to an organization's private resources from a user device where the Cisco Secure Client is deployed.

Zero Trust Access with an Unmanaged Device

- Secure Access Zero Trust Access (ZTA) can use OIDC to authenticate and authorize requests to an organization's private resources from an unmanaged device.

Configure Duo for OpenID Connect

Describes Configure Duo for OpenID Connect in Cisco Secure Access. Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled.

Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled. Secure Access can also use OIDC to authenticate requests for private resources from user devices that connect with Zero Trust Access (ZTA).

To enable Secure Access to authenticate with OIDC, you must set up the integration of an OIDC identity provider (IdP) in Secure Access. Add Duo as a cloud identity provider (IdP) to provision your organization's users and groups from Duo to Secure Access and use Duo IdP for authentication. Then add the Duo OIDC IdP metadata to Secure Access.

For information about adding Duo as an IdP to Secure Access, see Provision Users and Groups from Duo on page 657.

Note

You cannot use the Duo SAML app to integrate OIDC with Secure Access. For more information, see Configure Duo Security for SAML on page 812.

Configure Duo SSO authentication through OIDC in Secure Access

Provides instructions for completing the Configure Duo SSO authentication through OIDC in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

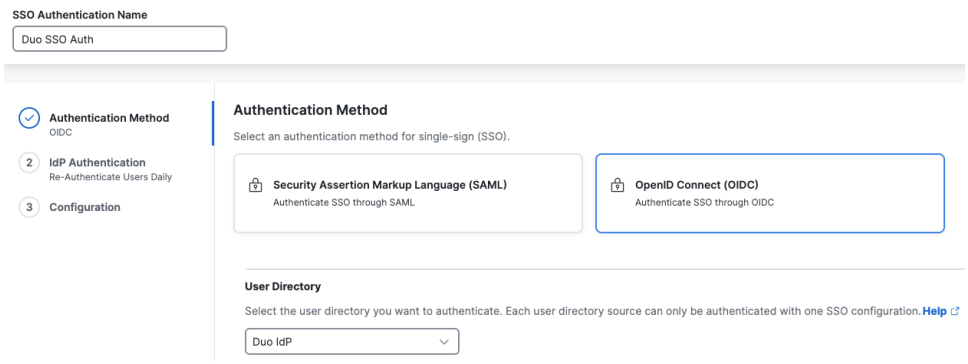
Use your Duo IdP directory in Secure Access to configure Duo SSO in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- A Single Sign-On application in Duo for Generic OpenID Connect (OIDC) Relying Parties.
- Duo added as an IdP to Secure Access. For more information, see Provision Users and Groups from Duo on page 657.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices** > **Configuration management** > **SSO authentication**.
2. Click **Add SSO authentication**.
3. Enter an **SSO Authentication Name**.
4. Under **Authentication Method**, perform the following:
   a. Choose **OpenID Connect (OIDC)**.
   b. **User Directory:** Select your Duo IdP directory.
   c. Click **Next**.



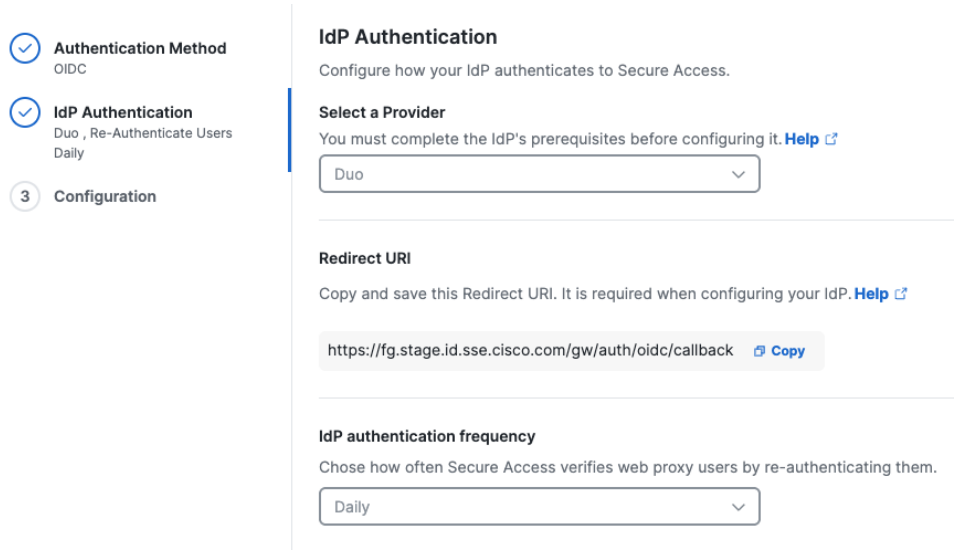
5. Under **IdP Authentication**, perform the following:

a. **Select a Provider:** Select Duo.

b. **Redirect URI:** Copy and save this Redirect URI. It is required when configuring Duo.

c. **IdP authentication frequency:** Choose how often Secure Access verifies web proxy users by re-authenticating them. Options are Daily, Weekly, Monthly, Never.

d. Click **Next**.



6. **Configuration:** Provide the necessary details to complete the OIDC authentication process for Duo. For more information, see Duo Single Sign-On for Generic OpenID Connect (OIDC) Relying Parties.

   a. The **Client ID** from the Duo OIDC application.

   b. The **Client Secret** from the Duo OIDC application.

   c. **OIDC Configuration URL:** Enter the **Discovery URL** from the Duo OIDC application, then click **Get configuration** to populate endpoint details in the fields below.

   d. Click **Done**.

View Provisioned Users and Groups in Secure Access

Provides instructions for completing the View Provisioned Users and Groups in Secure Access workflow in Cisco Secure Access. Navigate to Connect Users, Groups, and Endpoint Devices to view the users and groups provisioned from Entra ID.

Procedure

Navigate to **Connect** > **Users, Groups, and Endpoint Devices** to view the users and groups provisioned from Entra ID.

- For more information, see View User Details.
- For more information, see View Groups and Organizational Unit Details.

Configure Okta for OpenID Connect

Describes Configure Okta for OpenID Connect in Cisco Secure Access. Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled.

Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled. Secure Access can also use OIDC to authenticate requests for private resources from user devices that connect with Zero Trust Access (ZTA).

To enable Secure Access to authenticate with OIDC, you must set up the integration of an OIDC identity provider (IdP) in Secure Access. On the organization's instance of Okta, configure an Okta ID OIDC app. Then to complete the integration, add the OIDC IdP metadata in Secure Access.

For information about provisioning users from Okta to Secure Access, see Provision Users and Groups from Okta.

Note: You cannot use the Okta SAML app to integrate OpenID Connect with Secure Access.

Verify the UPN and preferred_username Mapping

Describes Verify the UPN and preferred_username Mapping in Cisco Secure Access. In the Okta OIDC app, verify that the user principal name (UPN) maps to the preferred_username attribute.

In the Okta OIDC app, verify that the user principal name (UPN) maps to the `preferred_username` attribute. The Okta OIDC IdP app must send the UPN for the **preferred_username** claim in the ID token.

For information about provisioning users and groups in Secure Access, see Provision Users and Groups from Okta.

Step 1 – Choose an Authentication Method

Provides instructions for completing the Step 1 – Choose an Authentication Method workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

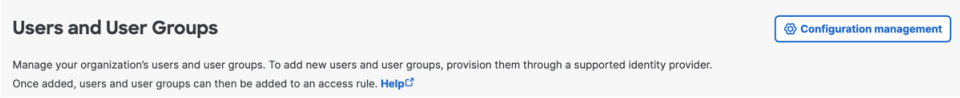
For the authentication method, choose **OpenID Connect (OIDC)**. For more information, see Add SSO Authentication Profiles.

Before you begin

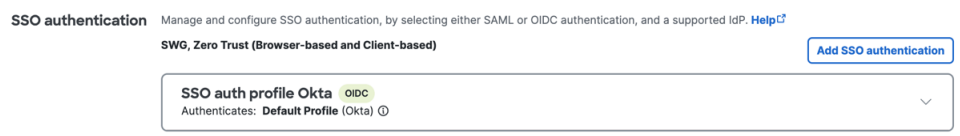
- Full Admin user role. For more information, see Manage Accounts.

Procedure

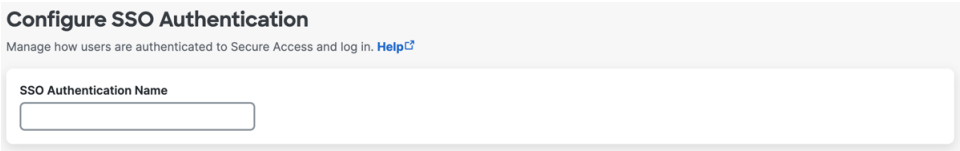
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



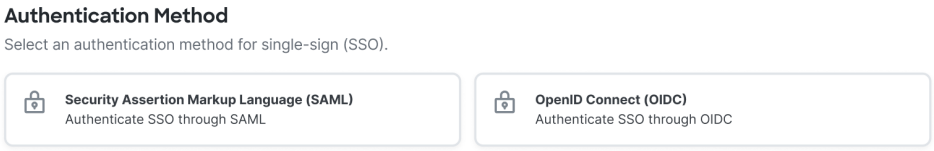
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



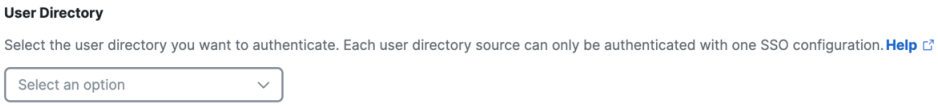
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.

Step 2 – Add an Identity Provider

Provides instructions for completing the Step 2 – Add an Identity Provider workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Select the SSO authentication IdP, enter the redirect URI for the Relying party (Secure Access), and optionally choose how often a user will be asked to authenticate with Secure Access.

Save the **Redirect URI** and use this URI to configure the Okta OpenID Connect app integration. For information about the Redirect URI, see Configure Integrations with OIDC Identity Providers.

Before you begin

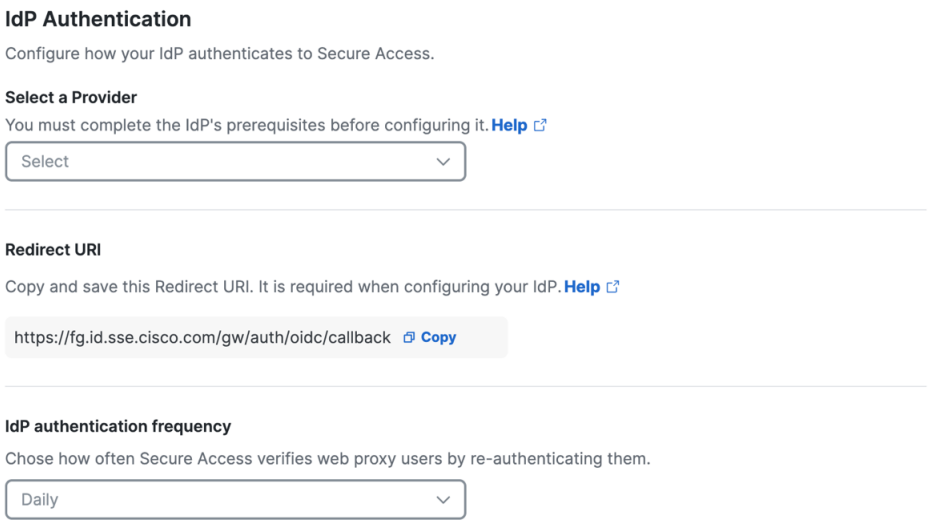
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. For **Select a Provider**, choose **Okta**.
2. For **Redirect URI**, click **Copy**.

   Save the URI (**https://fg.id.sse.cisco.com/gw/auth/oidc/callback**).

   You will use this URI when you set up the integration of Secure Access in the Okta OIDC app.



3. (Optional) For **IdP authentication frequency**, choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   The time intervals are: **Daily**, **Weekly**, or **Monthly**.

4. Click **Next**.

Step 3 – Configure the Identity Provider's OIDC Metadata

Describes Step 3 – Configure the Identity Provider's OIDC Metadata in Cisco Secure Access. For information about configuring the Okta OIDC app, see the Okta documentation.

For information about configuring the Okta OIDC app, see the Okta documentation.

- Step 3a – Add the Secure Access Redirect URI in Okta
- Step 3b – Configure the Core Grants in Okta
- Step 3c – Get the Okta OIDC Client ID and Secret
- Step 3d – Get the Okta OIDC Configuration URL

Step 3a – Add the Secure Access Redirect URI in Okta

Provides instructions for completing the Step 3a – Add the Secure Access Redirect URI in Okta workflow in Cisco Secure Access. Configure an Okta OpenID Connect app integration in your instance of Okta.

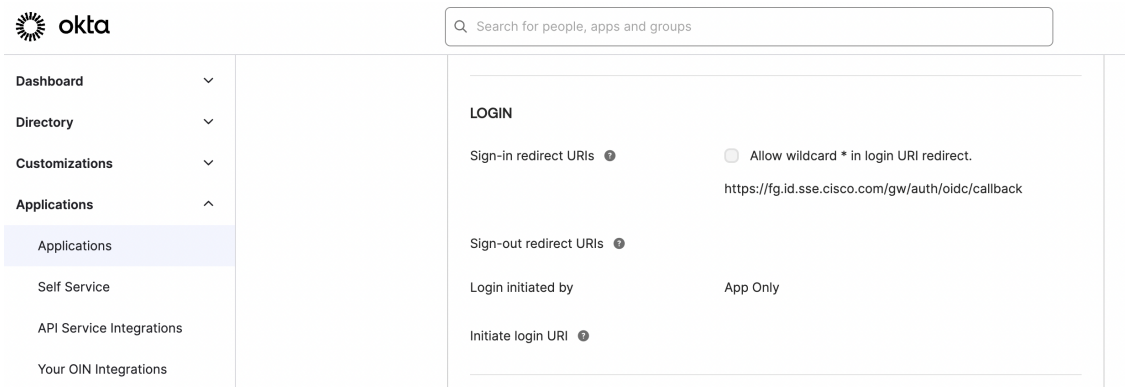
Before you begin

- Configure an Okta OpenID Connect app integration in your instance of Okta. For information about configuring an OIDC app, see the Okta documentation.

Procedure

1. Sign into your instance of Okta and navigate to the Okta OIDC app.
2. Navigate to **Applications > Login**.
3. For **Sign-in redirect URIs**, enter the Secure Access **Redirect URI** that you copied from Secure Access in Step 2.

   For more information, see Step 2 – Add an Identity Provider.



Step 3b – Configure the Core Grants in Okta

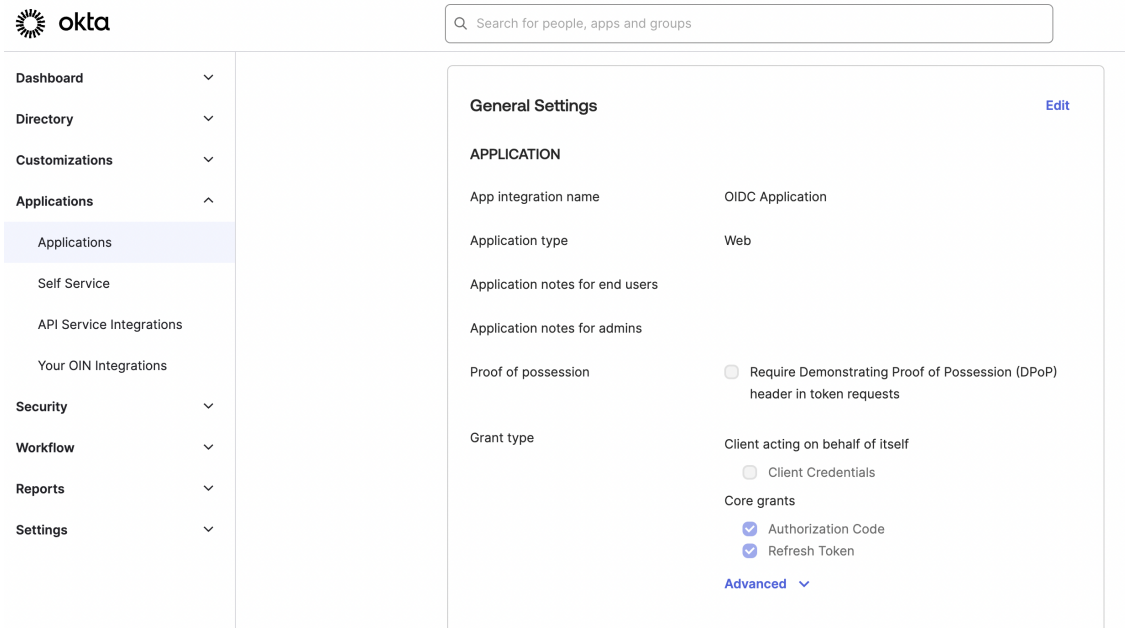
Provides instructions for completing the Step 3b - Configure the Core Grants in Okta workflow in Cisco Secure Access. Configure an Okta OpenID Connect app integration in your instance of Okta.

Before you begin

- Configure an Okta OpenID Connect app integration in your instance of Okta. For information about configuring an OIDC app, see the Okta documentation.

Procedure

1. Sign into your instance of Okta and navigate to the Okta OIDC app.
2. Navigate to **Applications > General Settings**.
3. For **Application**, navigate to **Grant type**, and then click **Authorization Code** and **Refresh Token**.



Step 3c – Get the Okta OIDC Client ID and Secret

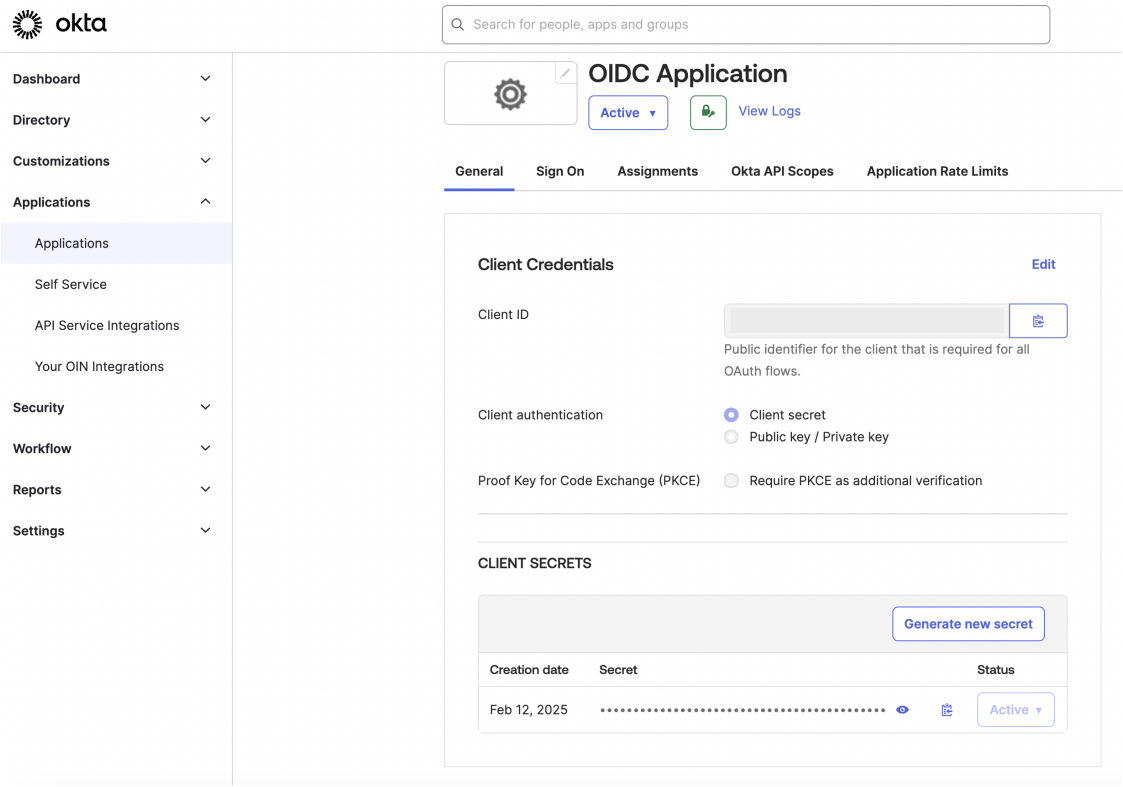
Provides instructions for completing the Step 3c - Get the Okta OIDC Client ID and Secret workflow in Cisco Secure Access. Configure an Okta OpenID Connect app integration in your instance of Okta.

Before you begin

- Configure an Okta OpenID Connect app integration in your instance of Okta. For information about configuring an OIDC app, see the Okta documentation.

Procedure

1. Sign into your instance of Okta and navigate to the Okta OIDC app.
2. Navigate to **Applications > OIDC Application**, and then navigate to **General**.



3. Navigate to **Client Credentials**, and then copy the **Client ID**.
   You will use the **Client ID** to configure the integration of the Okta OIDC IdP in Secure Access.
4. Navigate to **Client Secrets**, click **Generate new secret**, and then copy the client secret.
   You will use the **Secret** to configure the integration of the Okta OIDC IdP in Secure Access.

Step 3d – Get the Okta OIDC Configuration URL

Provides instructions for completing the Step 3d - Get the Okta OIDC Configuration URL workflow in Cisco Secure Access. Configure an Okta OpenID Connect app integration in your instance of Okta.

Get the domain for your instance of Okta and the authorization server ID, and then create the Okta OIDC Configuration URL.

Before you begin

- Configure an Okta OpenID Connect app integration in your instance of Okta. For information about configuring an OIDC app, see the Okta documentation.

Procedure

1. Sign into your instance of Okta and navigate to the Okta OIDC app.
2. Navigate to **Security > API > default**, and then navigate to **Settings** to view the **Metadata URI**.
3. Get your Okta domain (`yourOktaDomain`) and the authorization server ID (`authorizationServerId`).
4. Create the OIDC configuration URL substituting your Okta metadata in the URL.

```
https://{yourOktaDomain}/oauth2/{authorizationServerId}/.well-known/openid-configuration
```

Step 4 – Add the OIDC Metadata in Secure Access

Provides instructions for completing the Step 4 - Add the OIDC Metadata in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

> **Note**
>
> If you update the Client Secret in the Okta OIDC app, you must reenter the **Client Secret** in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

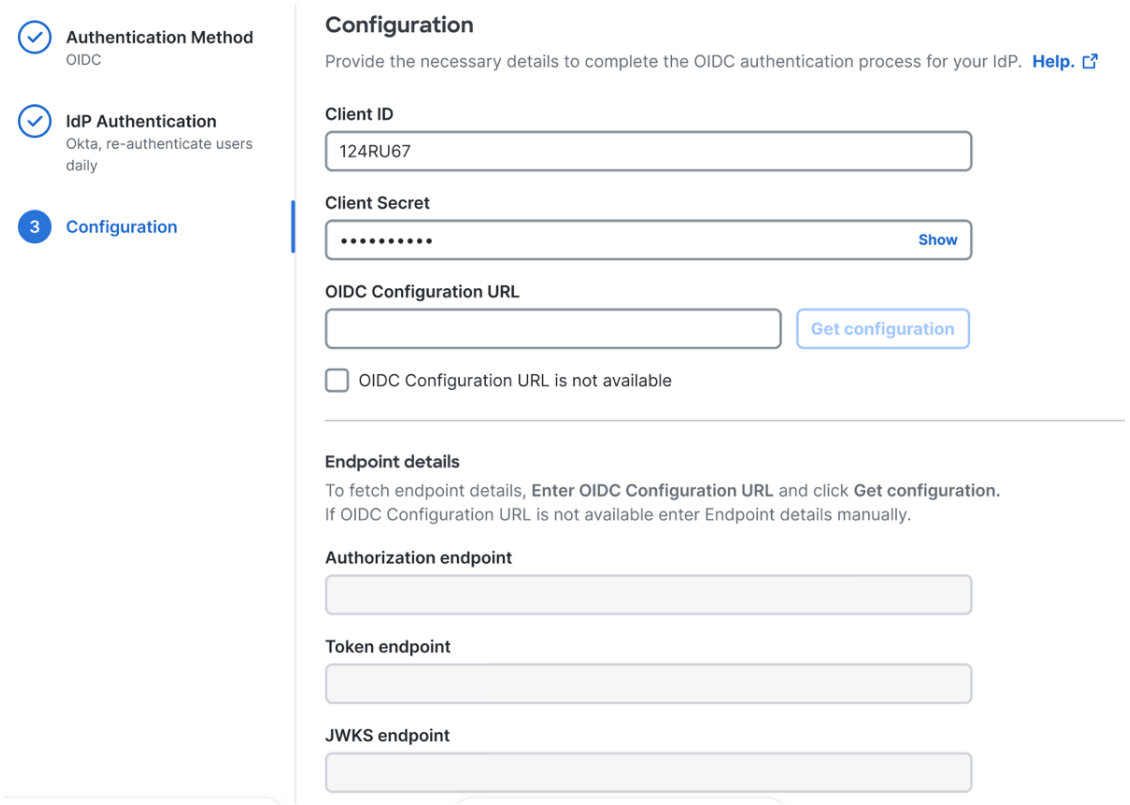
1. In Secure Access, complete the configuration of the Okta OIDC IdP integration.
2. Gather your Okta Client ID and secret.
   For more information, see Step 3c - Get the Okta OIDC Client ID and Secret.
3. For **Client ID**, enter the client ID that you generated in the Okta OIDC app.
4. For **Client Secret**, enter the client secret that you generated in the Okta OIDC app.
5. Get your Okta OIDC configuration URL.
   For more information, see Step 3d - Get the Okta OIDC Configuration URL.
6. For **OIDC Configuration URL**, enter the OIDC configuration URL that you created with the metadata from the Okta app.

   > **Note**
   >
   > After you enter the OIDC configuration URL, Secure Access enables the **Get configuration** button.

7. (Optional) Click **OIDC Configuration URL is not available** if the OIDC URL is not known.

8. For **Authorization endpoint**, **Token endpoint**, and **JWKS endpoint**, click **Get configuration** to use the OIDC configuration URL to retrieve the OIDC authorization API endpoint.

> **Note**
>
> If the OIDC configuration URL is not available, enter the values for **Authorization endpoint**, **Token endpoint**, and **JWKS endpoint** manually.



9. Click **Done**.

Configure Microsoft Entra ID for OpenID Connect

Describes Configure Microsoft Entra ID for OpenID Connect in Cisco Secure Access. Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled.

Secure Access supports the use of the OpenID Connect (OIDC) protocol to authenticate and authorize requests from user devices on networks or network tunnels with internet security enabled. Secure Access can also use OIDC to authenticate requests for private resources from user devices that connect with Zero Trust Access (ZTA).

To enable Secure Access to authenticate with OIDC, you must set up the integration of an OIDC identity provider (IdP) in Secure Access. On the organization's instance of Entra ID, configure an Entra ID OIDC app. Then to complete the integration, add the OIDC IdP metadata in Secure Access.

For information about provisioning an organization's users from Entra ID in Secure Access, see Provision Users and Groups from Microsoft Entra ID.

> **Note**
>
> You cannot use the Microsoft Entra ID SAML app to integrate OpenID Connect with Secure Access.

Bypass Domains from SSL Decryption

We recommend that you bypass certain domains on the secure web gateway. For more information, see Manage Internet Security Bypass.

To exclude a domain from Secure Access SSL Decryption, add the following domain names to the list of bypassed domains:

- **login.live.com**
- **login.microsoftonline.com**
- **msauth.net**
- **msftauth.net**

Step 1 – Choose an Authentication Method

Provides instructions for completing the Step 1 – Choose an Authentication Method workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

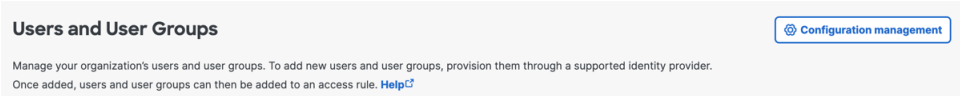
For the authentication method, choose **OpenID Connect (OIDC)**. For more information, see Add SSO Authentication Profiles.

Before you begin

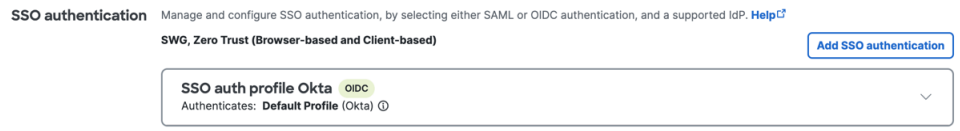
- Full Admin user role. For more information, see Manage Accounts.

Procedure

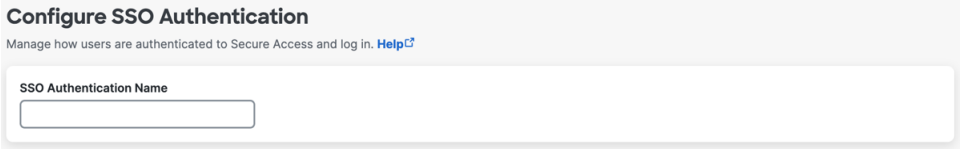
1. Navigate to **Connect > Users and User Groups**, and then click **Configuration management**.



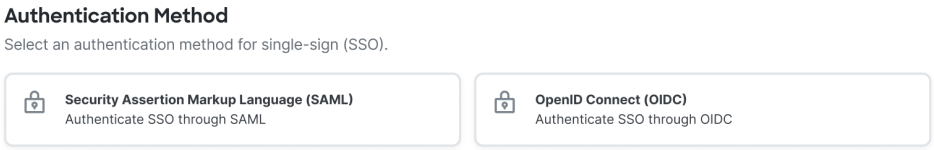
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



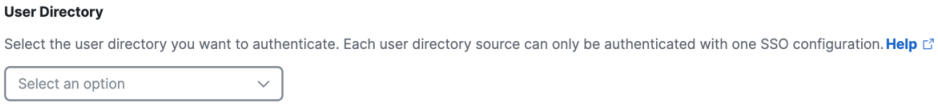
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.

Step 2 – Add an Identity Provider

Provides instructions for completing the Step 2 – Add an Identity Provider workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Select the Azure SSO authentication IdP, copy the redirect URI for the Relying party (Secure Access), and optionally choose how often a user will be required to authenticate with Secure Access.

Save the **Redirect URI** and use this URI to configure the Entra ID OIDC app. For information about the Secure Access Redirect URI, see Configure Integrations with OIDC Identity Providers.

Before you begin

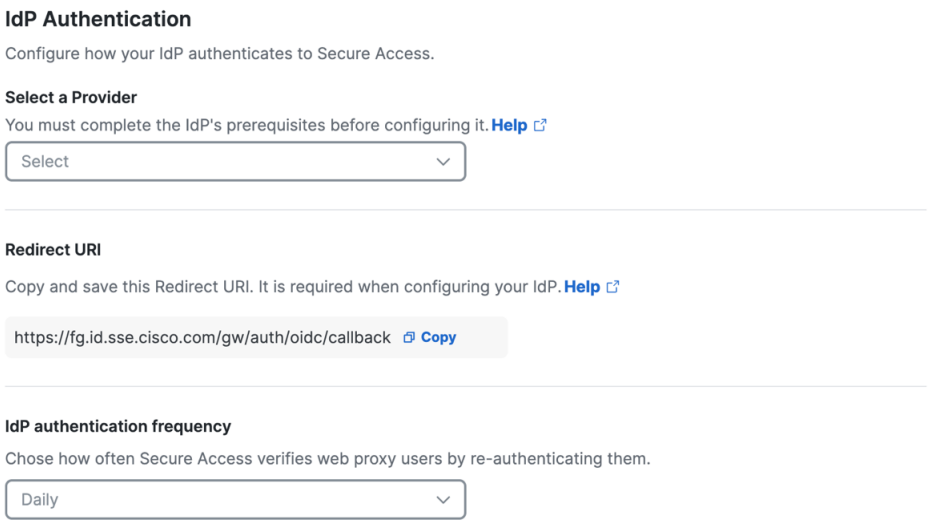
- Full Admin user role. For more information, see Manage Accounts.
- Configure an OpenID Connect app integration in your instance of Microsoft Entra ID. For information about configuring an OIDC app with Entra ID, see the Microsoft Entra ID documentation.

Procedure

1. For **Select a Provider**, choose **Azure**.
2. For **Redirect URI**, click **Copy**.

   Save the URI (**https://fg.id.sse.cisco.com/gw/auth/oidc/callback**).

   You will use this URI when you set up the integration of Secure Access in the Entra ID OIDC app.



3. (Optional) For **IdP authentication frequency**, choose a time interval when a user must authenticate with Secure Access, or select **Never**.

   The time intervals are: **Daily**, **Weekly**, or **Monthly**.

4. Click **Next**.

Step 3 – Configure the Identity Provider's OIDC Metadata

Describes Step 3 – Configure the Identity Provider's OIDC Metadata in Cisco Secure Access. For information about configuring an Entra ID OIDC application, see the Microsoft Entra ID documentation.

For information about configuring an Entra ID OIDC application, see the Microsoft Entra ID documentation.

- Step 3a – Add the Secure Access Redirect URI in Entra ID
- Step 3b – Get the Client ID and Secret for Entra ID OIDC
- Step 3c – Get the Tenant ID for Entra ID OIDC

Step 3a – Add the Secure Access Redirect URI in Entra ID

Provides instructions for completing the Step 3a – Add the Secure Access Redirect URI in Entra ID workflow in Cisco Secure Access. Configure an OpenID Connect app integration in your instance of Microsoft Entra ID.

Add the Secure Access Redirect URI in the Entra ID OIDC app.

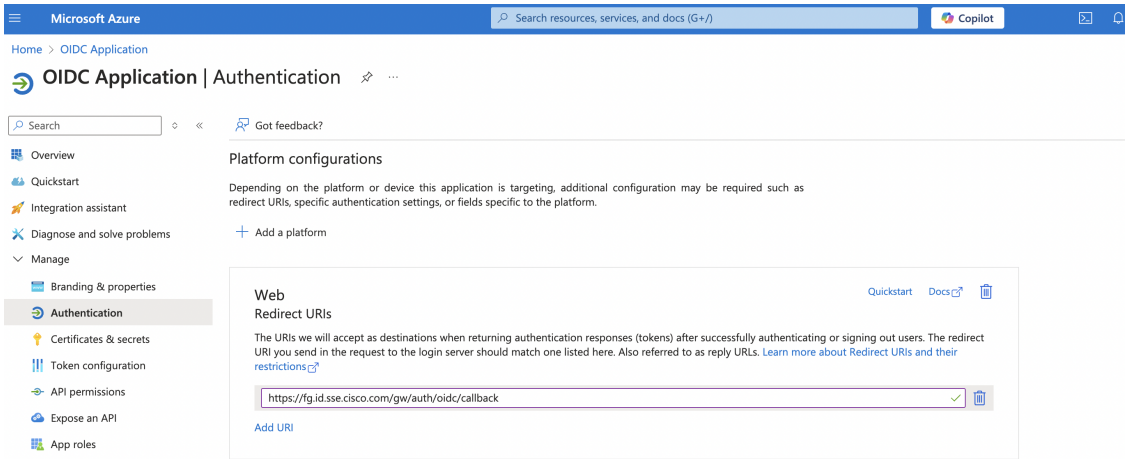
Before you begin

- Configure an OpenID Connect app integration in your instance of Microsoft Entra ID. For information about configuring an OIDC app with Entra ID, see the Microsoft Entra ID documentation.

Procedure

1. Sign into your instance of Entra ID, and navigate to the Entra ID OIDC Application.
2. Navigate to **OIDC Application > Manage > Authentication**.
3. Navigate to **Platform configurations > Web**.
4. For **Redirect URIs**, enter the Secure Access **Redirect URI** that you copied in Step 2.

   For more information, see Step 2 – Add an Identity Provider.



Step 3b – Get the Client ID and Secret for Entra ID OIDC

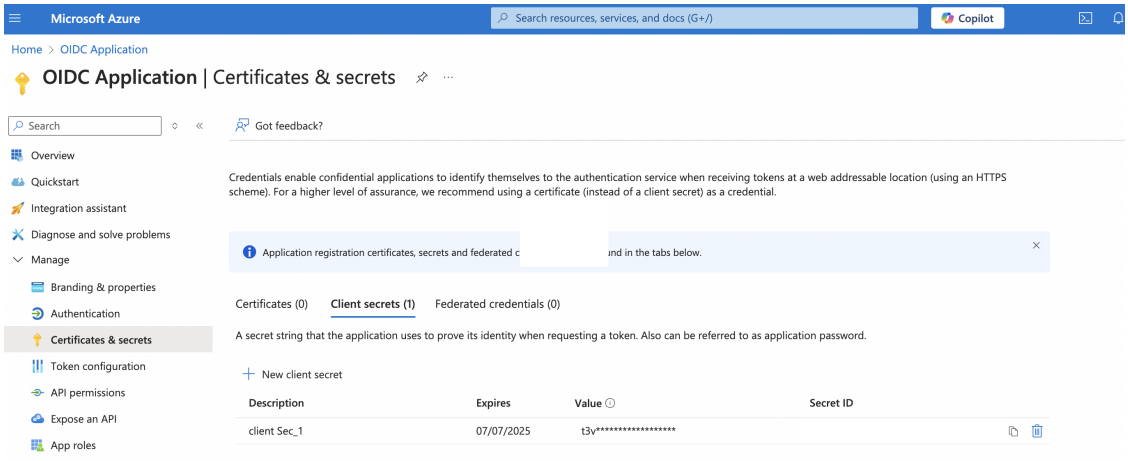
Provides instructions for completing the Step 3b – Get the Client ID and Secret for Entra ID OIDC workflow in Cisco Secure Access. Configure an OpenID Connect app integration in your instance of Microsoft Entra ID.

Before you begin

- Configure an OpenID Connect app integration in your instance of Microsoft Entra ID. For information about configuring an OIDC app with Entra ID, see the Microsoft Entra ID documentation.

Procedure

1. Sign into your instance of Entra ID, and navigate to the Entra ID OIDC Application.
2. Navigate to **OIDC Application > Overview**, and then copy your application **ID**.
   You will use the application ID to configure the client ID for the IdP integration in Secure Access.
3. Navigate to **OIDC Application > Manage > Certificates and secrets**.
4. Click **Client secrets**.
5. Navigate to **Value** and copy the secret.
   You will use the secret to configure the client secret for the IdP integration in Secure Access.



Step 3c – Get the Tenant ID for Entra ID OIDC

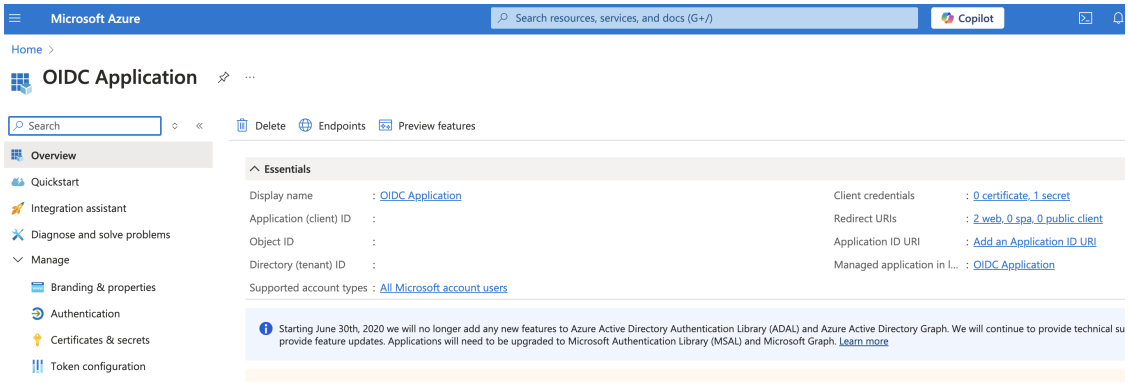
Provides instructions for completing the Step 3c - Get the Tenant ID for Entra ID OIDC workflow in Cisco Secure Access. Configure an OpenID Connect app integration in your instance of Microsoft Entra ID.

Before you begin

- Configure an OpenID Connect app integration in your instance of Microsoft Entra ID. For information about configuring an OIDC app with Entra ID, see the Microsoft Entra ID documentation.

Procedure

1. Sign into your instance of Entra ID, and navigate to the Entra ID OIDC Application.
2. Navigate to **OIDC Application > Overview**, and then navigate to **Essentials**.
3. Navigate to **Directory** to get your tenant ID.



4. Create the OIDC configuration URL substituting your tenant ID for `tenantId` in the URL.

```
https://login.microsoftonline.com/{tenantId}/v2.0/.well-known/openid-configuration
```

5. When you set up the Entra ID integration in Secure Access, add the OIDC configuration URL that you created.

Step 4 – Add the OIDC Metadata in Secure Access

Provides instructions for completing the Step 4 - Add the OIDC Metadata in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Secure Access, complete the configuration of the Entra ID OIDC IdP integration.

> **Note**
>
> If you update the client's secret in the Entra ID OIDC app, you must reenter the **Client Secret** in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Gather your Entra ID Client ID and secret.
   For more information, see Step 3b – Get the Client ID and Secret for Entra ID OIDC.
2. For **Client ID**, enter the application ID from the Entra ID ODIC app.
3. For **Client Secret**, enter the client's Secret that you generated in the Entra ID OIDC app.
4. Get your Entra ID OIDC configuration URL.
   For more information, see Step 3c – Get the Tenant ID for Entra ID OIDC.
5. For **OIDC Configuration URL**, enter the OIDC configuration URL that you created with the metadata from the Entra ID app.

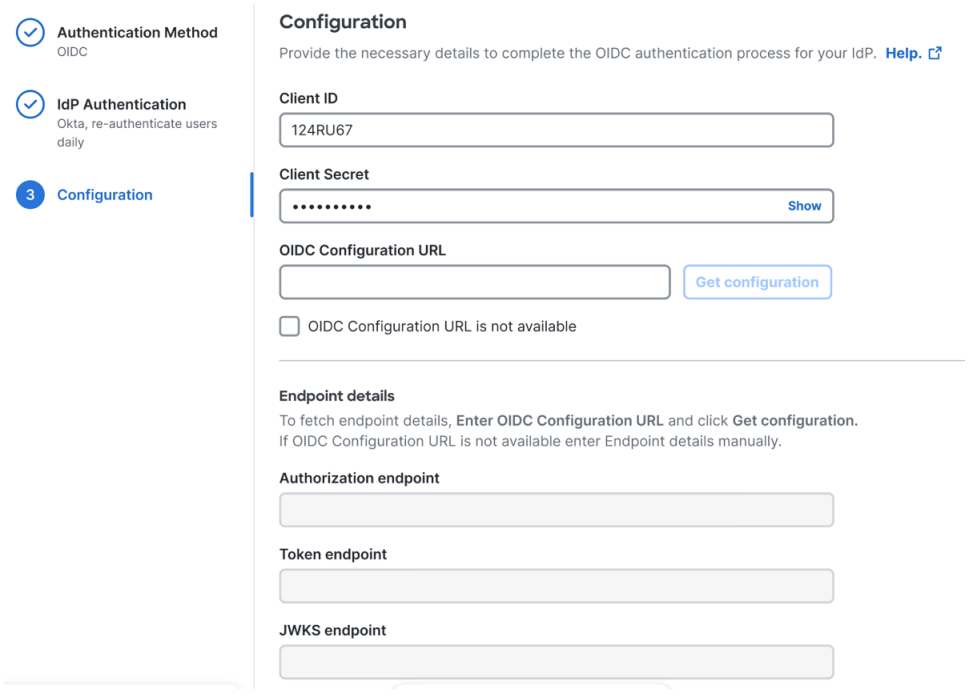
   Note

   After you enter the OIDC configuration URL, Secure Access enables the **Get configuration**.

6. (Optional) Click **OIDC Configuration URL is not available** if the OIDC URL is not known.
7. For **Authorization endpoint**, **Token endpoint**, and **JWKS endpoint**, click **Get configuration** to use the OIDC configuration URL to retrieve the OIDC authorization API endpoint data.

   Note

   If the OIDC configuration URL is not available, enter the values for **Authorization endpoint**, **Token endpoint**, and **JWKS endpoint** manually.



8. Click **Done**.

25 Integrations with SAML Identity Providers

Topics:

- Configure Integrations with SAML Identity Providers
- Configure Microsoft Entra ID for SAML
- Configure Okta for SAML
- Configure AD FS for SAML
- Configure Duo Security for SAML
- Configure Ping Identity for SAML
- Configure OpenAM for SAML
- SAML Certificate Renewal Options
- Test SAML Identity Provider Integration

Provides an overview of Integrations with SAML Identity Providers in Cisco Secure Access, including Configure Integrations with SAML Identity Providers, Configure Microsoft Entra ID for SAML, and Configure Okta for SAML. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Configure Integrations with SAML Identity Providers

Describes Configure Integrations with SAML Identity Providers in Cisco Secure Access. Cisco Secure Access enables you to connect securely to the internet, web resources in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications.

Cisco Secure Access enables you to connect securely to the internet, web resources in private and public clouds, your organization's on-premises private resources, and Software as a Service (SaaS) applications. To create more granular access rules and to authenticate users connecting from networks or network tunnels or with Zero Trust Access (ZTA), you can integrate a Security Assertion Markup Language (SAML) identity provider (IdP) in Secure Access. The SAML IdP provides single sign-on (SSO) authentication for users and Secure Access establishes a trust relationship with the IdP.

Secure Access integrates with various SAML 2.0 IdPs: Azure Active Directory (Azure AD), Duo, Okta, Ping Identity, Active Directory Federation Services (AD FS), and OpenAM.

Once users in your organization are configured to use SSO, the SAML IdP manages all authentication requests. A user authenticates to the SSO IdP, automatically signs in to Secure Access, and is authorized to connect to certain resources.

For more information, see Use Cases – SSO Authentication.

Configure Identity Providers for SAML Authentication

- Configure Microsoft Entra ID for SAML
- Configure Okta for SAML
- Configure AD FS for SAML
- Configure Duo Security for SAML
- Configure Ping Identity for SAML
- Configure OpenAM for SAML

Test the Identity Provider Integration

To complete the integration of an SAML IdP with Secure Access, evaluate the single sign-on authentication through the IdP. For more information, see Test SAML Identity Provider Integration.

View the SAML Certificates in Secure Access

Once you have completed the integration of an SAML IdP in Secure Access, you can manage the root certificates used in SAML authentication for Secure Access and the SAML IdP. For more information, see Manage Certificates.

Use Cases – SSO Authentication

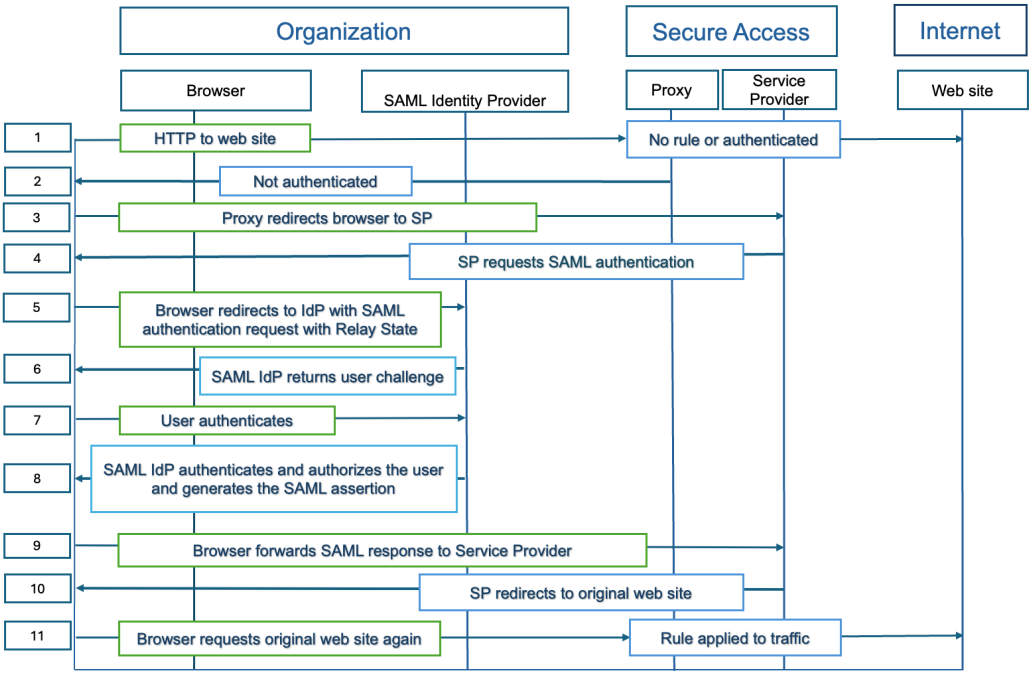
Describes Use Cases – SSO Authentication in Cisco Secure Access. Secure Access uses SAML authentication to provide seamless connections to web resources and private resources from user devices.

Secure Access uses SAML authentication to provide seamless connections to web resources and private resources from user devices.

Secure Internet Access—Networks and Network Tunnels

- Secure web gateway—The Cisco Secure Access secure web gateway (SWG) uses SAML to authenticate and authorize web requests from user devices sent over networks and network tunnels. Internet traffic is protected by the Secure Access DNS and Web security layers. The Secure Access SWG is not an open proxy. Secure Access must trust the source that forwards web traffic to it, whether the source is a network or network tunnel.

- SAML uses a cookie surrogate. When a browser sends an HTTP request, Secure Access checks if the request contains the HTTP Cookie header. If the cookie is not set, Secure Access can not authenticate the user.
- Web Security SAML Data Flow.



Zero Trust Access with the Cisco Secure Client

- Secure Access Zero Trust (ZT) uses SAML to authenticate and authorize requests to an organization's private resources from a user device where the Cisco Secure Client is deployed.

Zero Trust Access with an Unmanaged Device

- Secure Access Zero Trust (ZT) uses SAML to authenticate and authorize requests to an organization's private resources from an unmanaged device.

Prerequisites for SAML Authentication

Describes Prerequisites for SAML Authentication in Cisco Secure Access. SAML transfers data between the identity provider and the service provider; authentication is required to protect both the user's identity and the user's access to resources through single sign-on actions.

SAML transfers data between the identity provider and the service provider; authentication is required to protect both the user's identity and the user's access to resources through single sign-on actions. The minimizes the amount of times a user has to validate their functions and actions within the organization's environment and also protects the environment from outside users. Setting up SAML for your account can take up to an hour to establish, including any the post-procedure steps.

To configure the integration of a Security Assertion Markup Language (SAML) identity provider (IdP) with Cisco Secure Access, you **must** meet the requirements outlined in this guide.

SAML Authentication Overview

Configuring SAML goes through a variety of steps and time depending on the type of Identity Provider (IdP) you have available. Some IdPs require more steps to securely configure the integration between applications which can take

anywhere from a few hours to a day based on the complexity of IdP requirements; you can read more per IdP with the following links.

In general, the SAML authentication process is as follows:

1. Complete the prerequisites to prepare your network environment for SAML integration.
2. Add an SSO Authentication profile in Secure Access.
3. Add the SAML IdP of your choice to Secure Access.
4. If applicable, add IdP metadata to Secure Access.
5. While optional, we encourage you to configure certificate renewal options and testing the SAML integration between Secure Access and the IdP you configured.

Secure Access currently supports SAML integration with the following IdPs:

- Microsoft Entra
- Okta
- AD FS
- Duo Security
- Ping Identity
- OpenAM

Secure Access Service Provider Metadata

- Secure Access Entity ID–**saml.fg.id.sse.cisco.com**
- Secure Access Entity URL–**fg.id.sse.cisco.com/gw/auth/acs/response**

Requirements

- Full Admin user role. For more information, see Manage Accounts.
- Provision users and groups from your organization in Secure Access. The users and groups must match the identities obtained from SAML. For more information, see Manage Users and Groups.
- Download your IdP SAML metadata file in XML format.
- The SAML metadata must have a signing key.
- Configure SAML with an identity provider (IdP) that supports SAML 2.0 POST profiles.
- Ensure that traffic to your IdP URL is bypassed on the SWG to avoid an authentication loop. For more information, see Manage Domains.
- Enable cookies for your browser. For more information, see your browser's documentation.
- Install the Cisco Secure Access root certificate on all client machines egressing from networks or network tunnels where SAML is enabled. For more information, see Manage Certificates.
- If you use AD FS for SAML, we recommend that you bypass web traffic to the **id.sse.cisco.com** domain on the Secure Access secure web gateway (SWG). For other IdPs, send **id.sse.cisco.com** requests to the SWG, not directly to the internet. For more information about bypassing domains and Secure Access Web security, see Manage Domains.

> **Note**
>
> We **strongly** recommend upgrading your SAML to SAML v 2.0 for a more robust authentication tool. To reconfigure SAML in Secure Access, upload IdP metadata containing at least one public key. If the IdP provider does *not* contain the `KeyDescriptor` element, configure SAML 2.0 with Step 6 – Add Okta Metadata in Secure Access on page 797. Without SAML 2.0 the service provider does not verify incoming SAML responses are signed with the configured IdP and this can open your environment to malicious attacks.

Enable SAML and Decryption in the Security Profile

- To obtain the user identity of a device through SAML, enable SAML in the Secure Access security profile for internet access. For more information, see Manage Security Profiles.
- Enable decryption in the Secure Access security profile for internet access. Secure Access must inspect the Cookie HTTP header to read the SAML cookie. The SAML cookie acts as the authentication token or surrogate. For more information, see Manage Security Profiles.

Encrypted SAML Assertions

Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

- Secure Access requires encryption of the whole SAML assertion. Secure Access does not support configuring the IdP to specify EncryptedAttribute or EncryptedID.
- Secure Access requires SAML assertions encrypted using the key downloaded from **Connect > Users and Groups > Configuration Management**.
- Secure Access requires SAML assertions encrypted in sign-then-encrypt order, and will not support SAML assertions encrypted in encrypt-then-sign order.

Configure Microsoft Entra ID for SAML

Describes Configure Microsoft Entra ID for SAML in Cisco Secure Access. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled. Secure Access can also authenticate and authorize requests to private resources from user devices with Zero Trust Access (ZTA) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Microsoft Entra ID SAML IdP with Secure Access by uploading the Entra ID XML metadata file to Secure Access, or alternately add the Entra ID metadata in Secure Access manually.

For information about provisioning an organization's users from Entra ID in Secure Access, see Provision Users and Groups from Microsoft Entra ID.

Prerequisites

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Bypass Domains from SSL Decryption

We recommend that you bypass certain domains on the secure web gateway. For more information, see Manage Internet Security Bypass.

To exclude a domain from Secure Access SSL Decryption, add the following domain names to the list of bypassed domains:

- **login.live.com**
- **login.microsoftonline.com**
- **msauth.net**
- **msftauth.net**

Procedure

- Step 1 - Add an Authentication Profile in Secure Access
- Step 2 - Add SAML Identity Provider in Secure Access
- Step 3 - Add the Identity Provider's SAML Metadata to Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 - Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

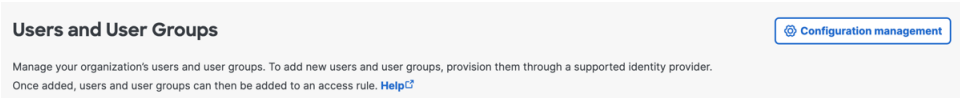
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

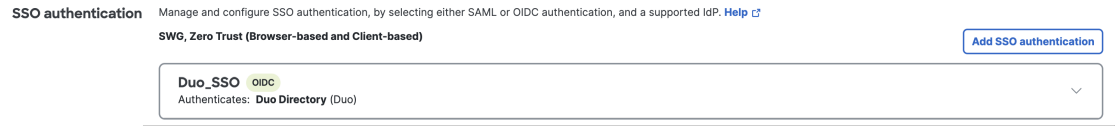
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

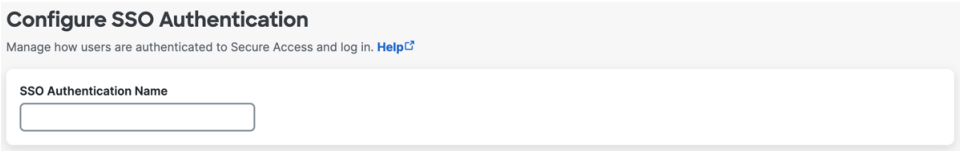
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



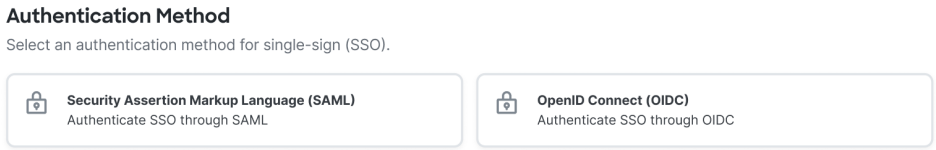
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



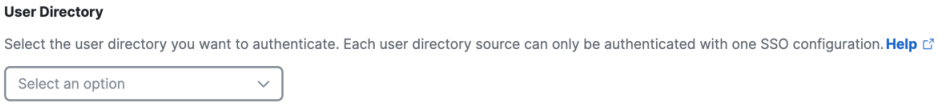
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

Step 2 – Add SAML Identity Provider in Secure Access

Provides instructions for completing the Step 2 - Add SAML Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

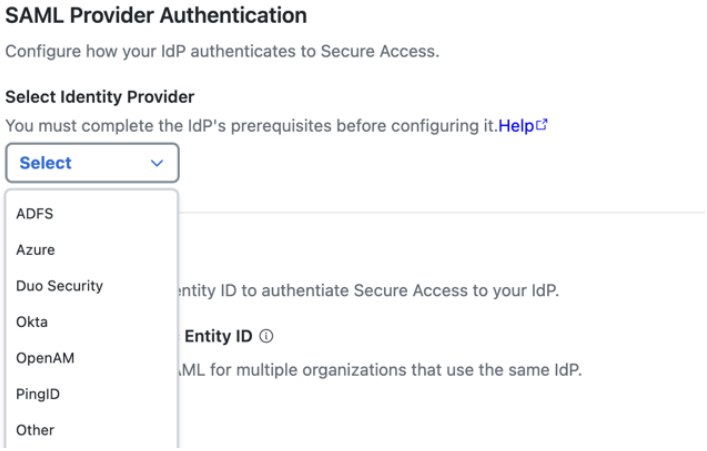
For IdP Authentication, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP. For more information, see Configure Integrations with OIDC Identity Providers and Configure Integrations with SAML Identity Providers respectively.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. Select an **Identity Provider**.

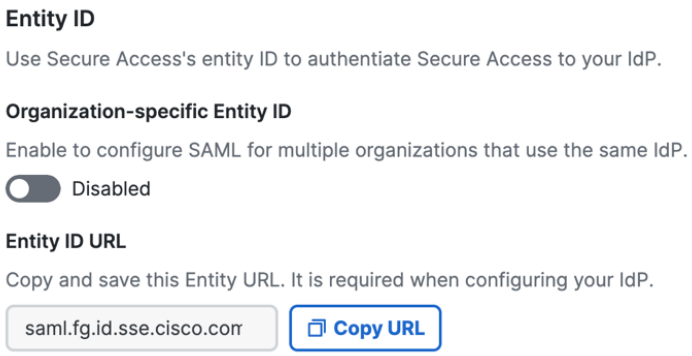


3. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.
4. For **Entity ID URL**, click **Copy URL**.

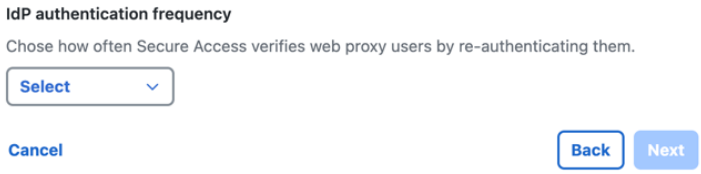
   Save the Secure Access metadata URL in your local environment.

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**.

> **Note**
>
> Use the Secure Access SP metadata URL to configure the SAML IdP app integration.



5. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.



6. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes Step 3 - Add the Identity Provider's SAML Metadata to Secure Access. Download the Secure Access metadata files and use the service provider file to configure your instance of Entra ID.

Download the Secure Access metadata files and use the service provider file to configure your instance of Entra ID.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

- Step 3a - Download the Secure Access Service Provider files
- Step 3b - Add the Secure Access Service Provider Metadata to Entra ID
- Step 3c - Add the SAML IdP Metadata to Secure Access

Step 3a – Download the Secure Access Service Provider files

Provides instructions for completing the Step 3a - Download the Secure Access Service Provider files workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

> **Note**
>
> Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

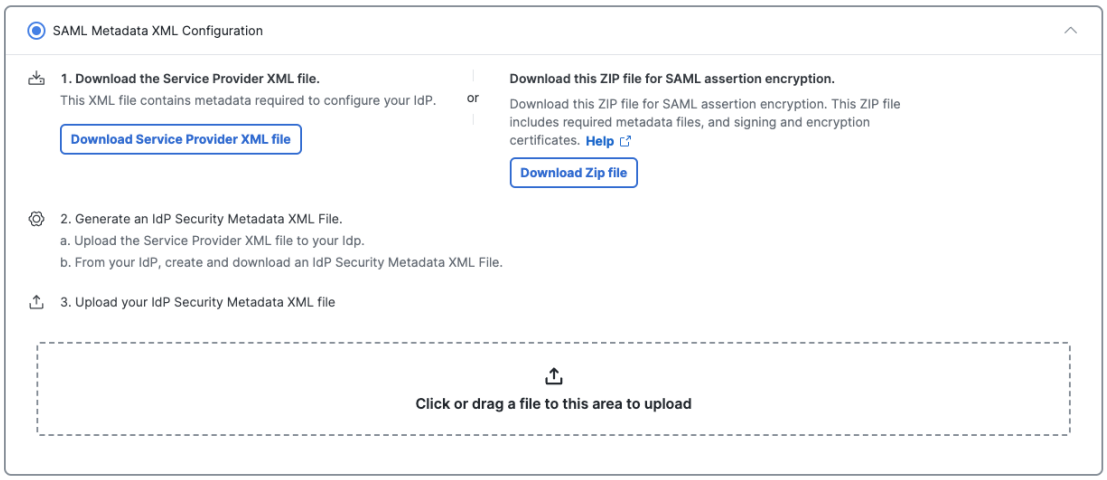
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

1. Check **SAML Metadata XML Configuration** or **Manual Configuration**.
2. Choose between unencrypted or encrypted SAML assertions.
   a) Click **Download Service Provider XML file** for the metadata XML file with the Secure Access root certificate that supports unencrypted SAML assertions.
   b) Click **Download Zip file** for the metadata XML file and signing and encryption certificate files required for encrypted SAML assertions.

      This metadata XML file includes the root certificate metadata for both the signing and the encryption certificates.



3. Open the **Cisco_SSE_SP_Metadata** XML file.
4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save.
   Use the certificate file in the next step when you create the app integration in the SAML IdP.

Step 3b – Add Secure Access Service Provider Metadata to Entra ID

Provides instructions for completing the Step 3b – Add Secure Access Service Provider Metadata to Entra ID workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Configure Secure Access as a generic SAML 2.0 service provider application for Entra ID. Add the Secure Access service provider metadata to Entra ID, then download the IdP metadata file from Azure to finish configuring Secure Access in the next step.

Contact Microsoft for assistance. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to Microsoft documentation.

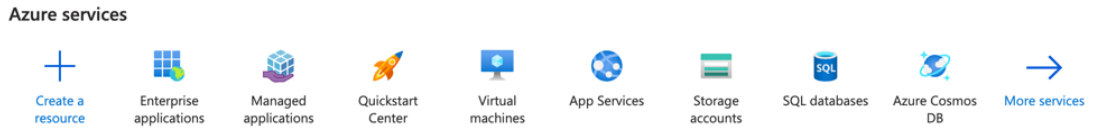
To configure the generic SAML Entra ID application, extract the **EntityID** and **AssertionConsumerService** values from the Secure Access metadata file and add these to the applicable fields in Entra ID:

Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

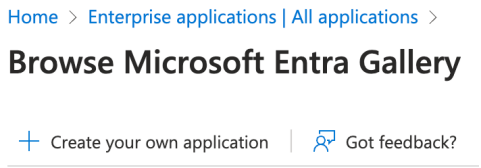
1. Sign in to Azure and navigate to **Azure services > Enterprise Applications**.



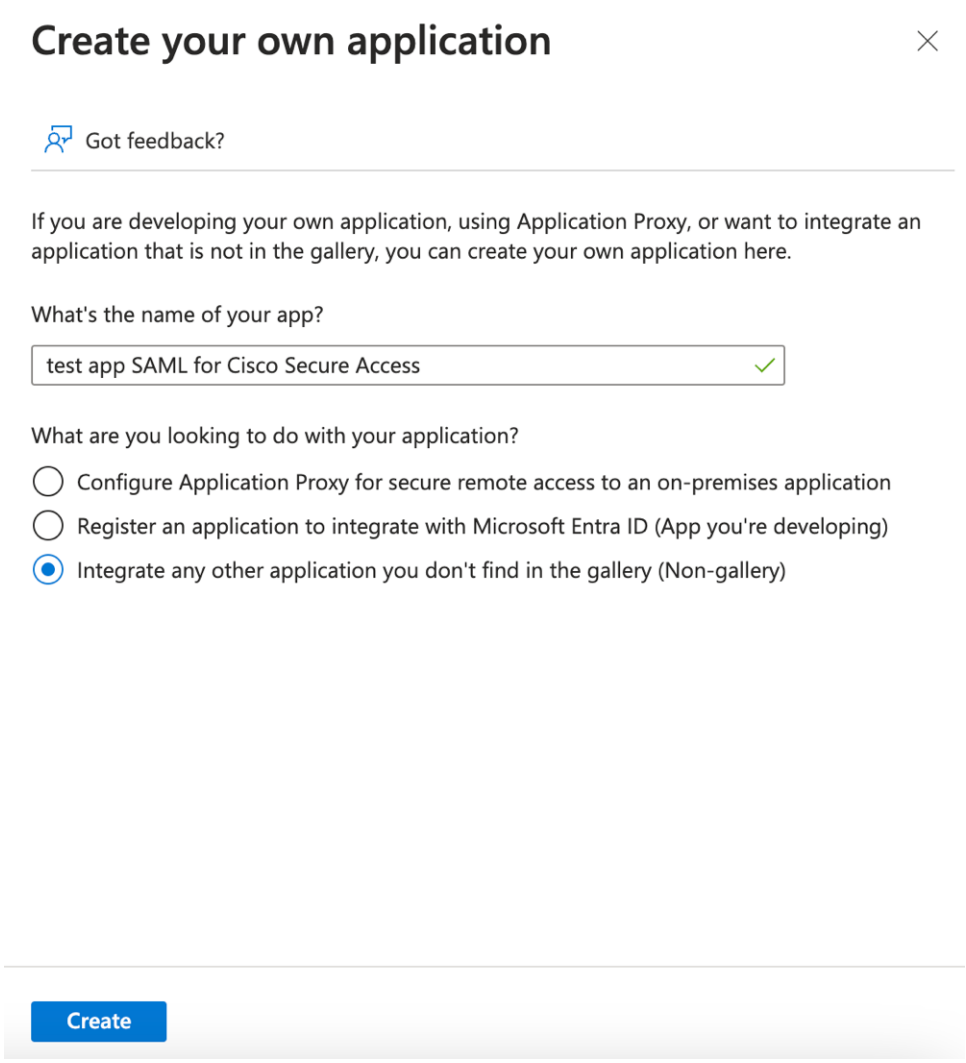
2. Select **New Application**.



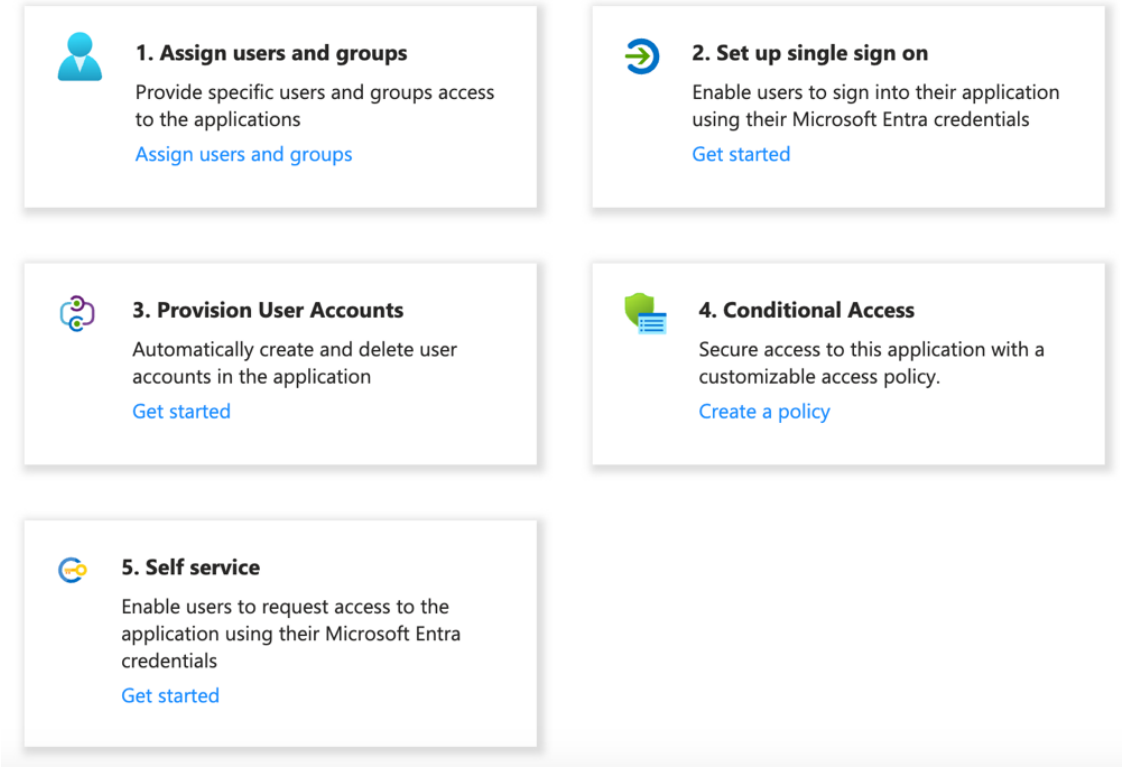
3. Select **Create your own Application**.



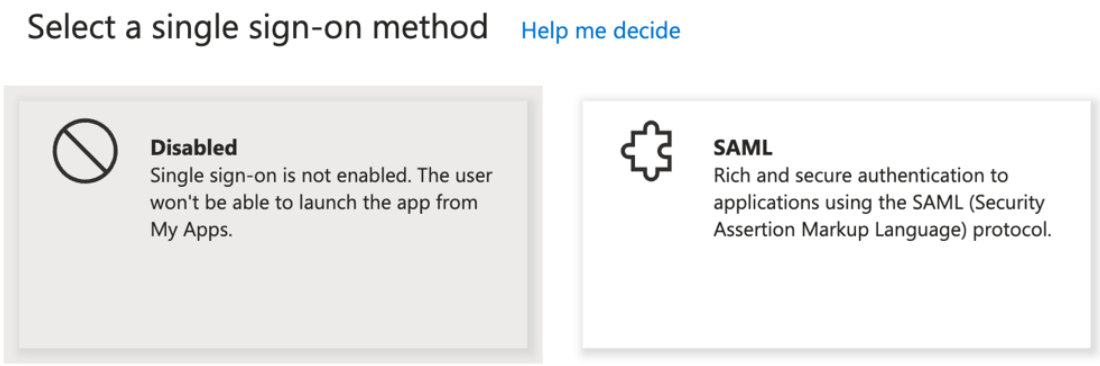
4. Give the new application a meaningful name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and then click **Create**.



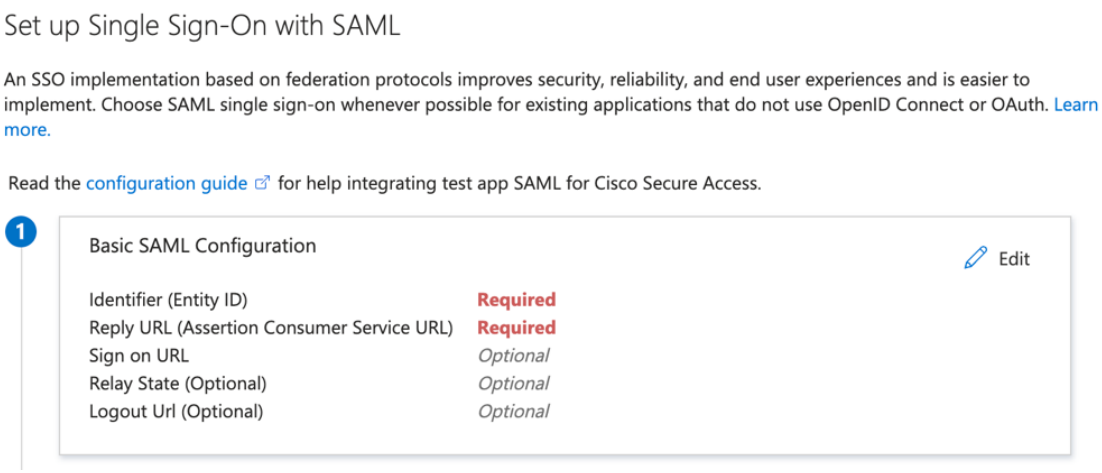
5. Navigate to **Getting Started**, and then click **Set up single sign on**.



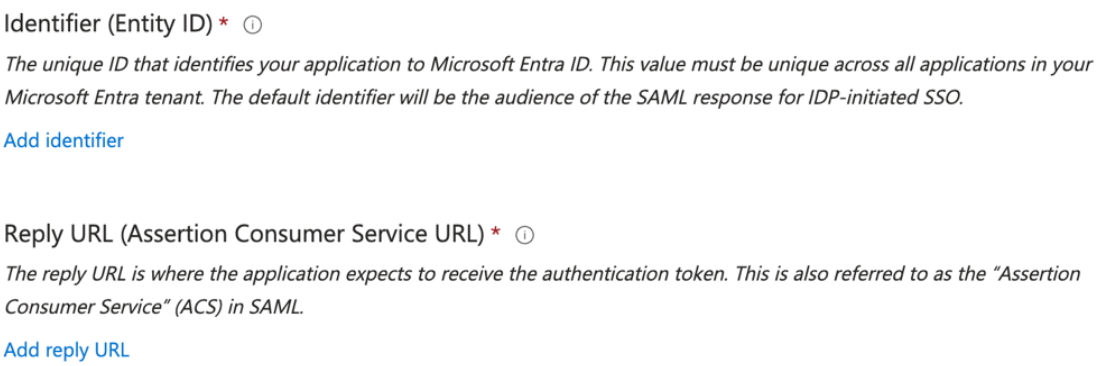
6. Click **SAML** to select the sign-on method.



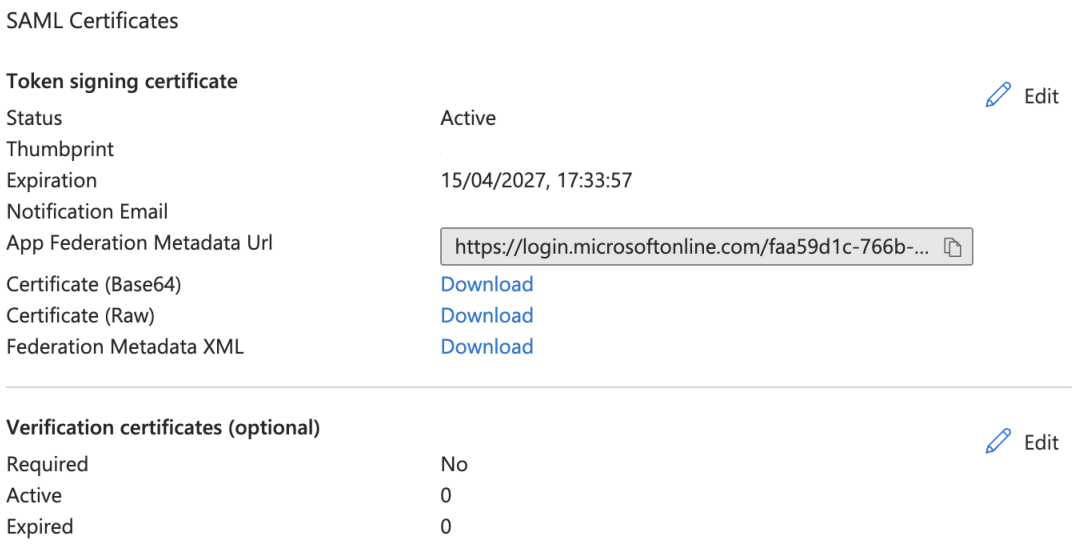
7. For **Basic SAML Configuration**, click **Edit**.
   a) For **Identifier (Entity ID)** (Microsoft Entra ID), click **Add identifier** and enter **saml.fg.id.sse.cisco.com** in the text area.



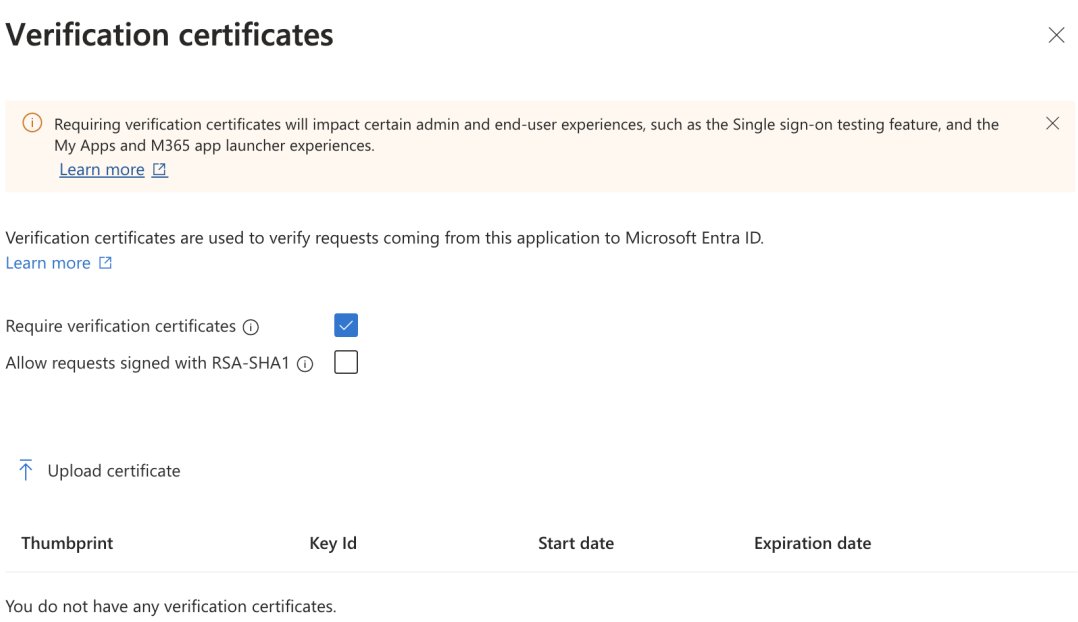
b) For **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL** and enter **https://fg.id.sse.cisco.com/gw/auth/acs/response**.



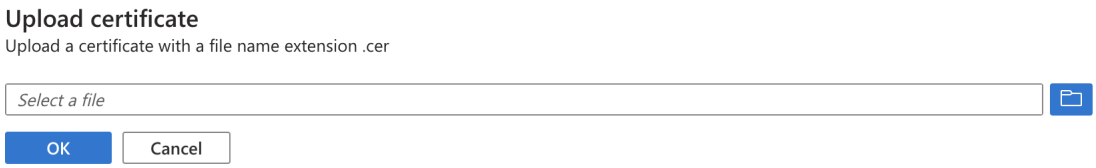
8. Navigate to **SAML Certificates**, and then **Verification certificates (optional)**.



9. Click **Edit**.
10. Chose **Require verification certificatess** and then click **Upload certificate**.



11. Upload the root certificate that you downloaded from the **Cisco_SSE_SP_Metadata** XML file, and then click **OK**.



12. Navigate to **SAML Certificates > Token signing certificate**.
13. For **Federation Metadata XML**, click **Download**.
14. Save the **Federation Metadata XML** file to your system and use the file to upload the configured Entra ID SAML attributes to Secure Access.

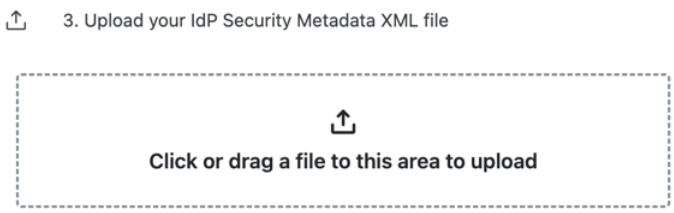
Step 3c – Add the Entra ID SAML Metadata to Secure Access

Provides instructions for completing the Step 3c - Add the Entra ID SAML Metadata to Secure Access workflow in Cisco Secure Access. If you selected SAML Metadata XML Configuration in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click Done.

Procedure

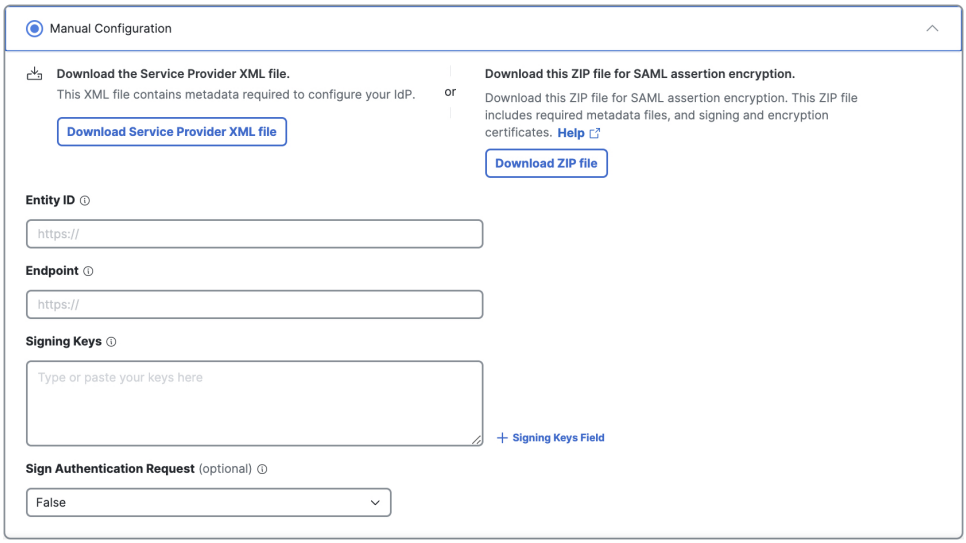
---

1. If you selected **SAML Metadata XML Configuration** in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click **Done**.



2. If you selected **Manual Configuration** in Step 3a, enter your SAML IdP metadata for the Secure Access settings, then click **Done**.

- **Entity ID**–A globally unique name for an identity provider.
- **Endpoint**–The URL used to communicate with your identity provider.
- **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
- **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



a) On Entra ID, copy the value of **Microsoft Entra Identifier**. Navigate to Secure Access and and enter the value in **Entity ID** .
b) On Entra ID, copy the value of **Login URL**. Navigate to Secure Access and enter the value in **Endpoint**.
c) On Entra ID, Copy the value of **Signing Certificate**. Navigate to Secure Access and enter the value in **Signing Keys**.
d) (Optional) Navigate to Secure Access and choose whether to sign the authentication request.
e) On Secure Access, click **Done**.

Configure Okta for SAML

Describes Configure Okta for SAML in Cisco Secure Access. Secure Access uses the Security Assertion Markup Language (SAML) to authenticate web requests from user devices on networks and network tunnels with web security enabled.

Secure Access uses the Security Assertion Markup Language (SAML) to authenticate web requests from user devices on networks and network tunnels with web security enabled. Secure Access also uses SAML to authenticate requests to private resources from user devices with Zero Trust Access (ZTA) enabled.

To support SAML authentication, you must configure the integration of an SAML identity provider (IdP) in Secure Access. In Okta, add the Secure Access service provider metadata. Then, add the Okta SAML IdP metadata in the Secure Access SSO authentication profile.

For information about provisioning users from Okta to Secure Access, see Provision Users and Groups from Okta.

Prerequisites

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

- Step 1 – Add an Authentication Profile in Secure Access
- Step 2 – Add Okta SAML Identity Provider in Secure Access
- Step 3 – Download the Secure Access Service Provider Files
- Step 4 – Configure Okta with the Secure Access SAML Metadata
- Step 5 – Get Metadata from Okta App Integration
- Step 6 – Add Okta Metadata in Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 – Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

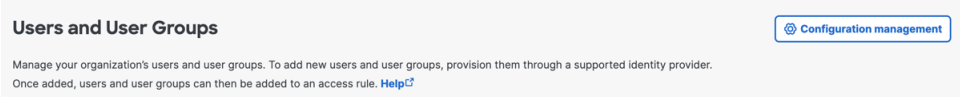
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

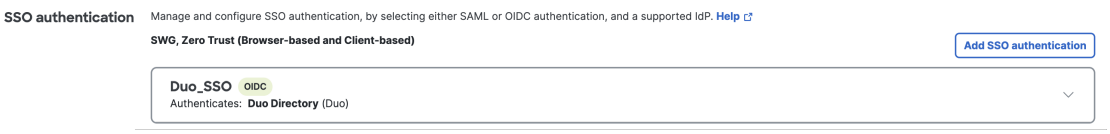
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

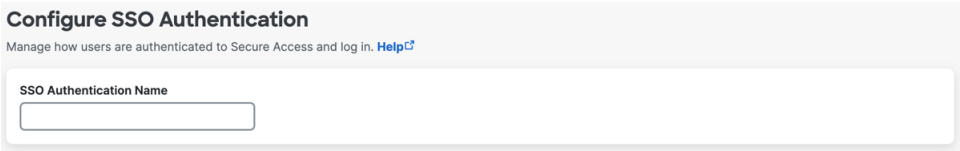
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



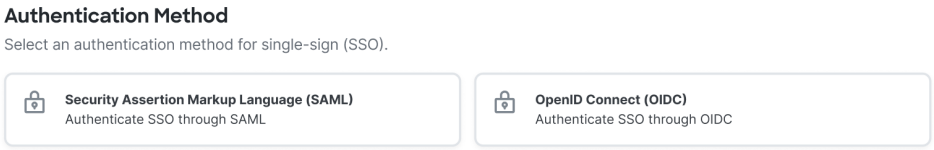
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



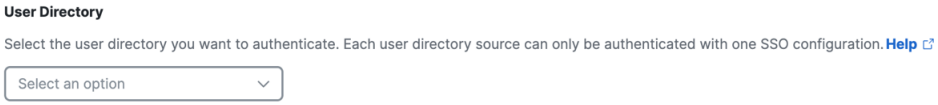
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

Step 2 – Add Okta SAML Identity Provider in Secure Access

Provides instructions for completing the Step 2 - Add Okta SAML Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

In the SSO authentication profile, select the Okta SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

> **Note**
>
> Communication for this procedure flows one-way from the Okta application to Secure Access there is no bi-directional flow of data.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. (Optional) Enable an organization-specific entity ID.

   Choose **Organization-specific Entity ID** when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.

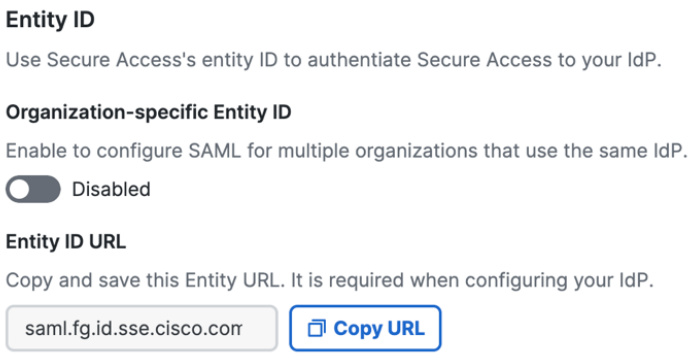
3. For **Entity ID URL**, click **Copy URL**.

   Save the Secure Access metadata URL in your local environment.

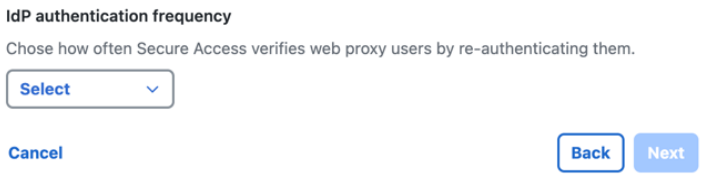
   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. For more information see Configure the Cisco User Management Connector App in Okta on page 662.

   For Cisco Secure Access Control Server (ACS), the `EntityID` is **https://fg.id.sse.cisco.com/gw/auth/acs/response**.

   > **Note**
   >
   > Use the Secure Access SP metadata URL to configure the SAML IdP app integration.

4. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.

5. Click **Next**.

Step 3 – Download the Secure Access Service Provider Files

Provides instructions for completing the Step 3 - Download the Secure Access Service Provider Files workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Download the Secure Access metadata files and use the service provider file to configure your instance of Okta.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

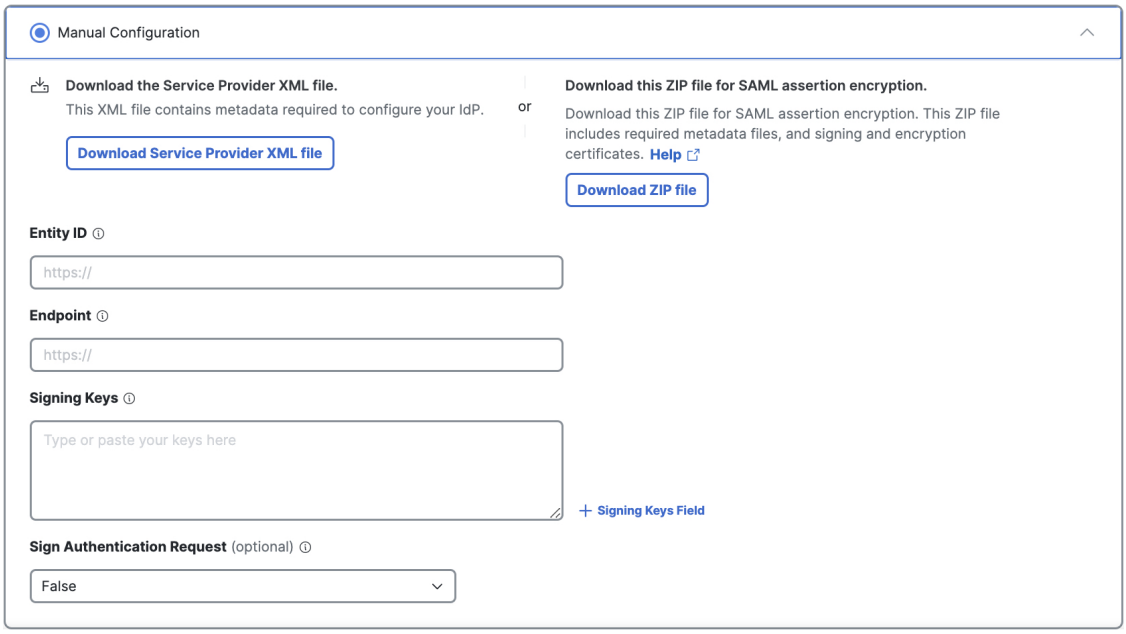
> **Note**
>
> Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. Check **Manual Configuration**.



2. Download the service provider files.
   a) Click **Download Service Provider XML file** for the metadata XML file.
   b) (Optional) To enable Secure Access to sign or encrypt the SAML communications, click **Download Zip file**.
3. Open the **Cisco_SSE_SP_Metadata** XML file.
   a) The value of the `entityID` field is `saml.fg.id.sse.cisco.com`, which is the same value that you copied in Step 2 - Select Okta SAML Identity Provider in Secure Access.
   b) Copy the value of `Location`, `https://fg.id.sse.cisco.com/gw/auth/acs/response`.

c) If you require a signing certificate, copy the value of `X509Certifcate`.

4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save. Use the certificate file in the next step when you create the app integration in Okta.

Step 4 – Configure Okta with the Secure Access SAML Metadata

Provides instructions for completing the Step 4 - Configure Okta with the Secure Access SAML Metadata workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

> **Note**
>
> Your instance of the Okta SAML IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

Add the Secure Access service provider metadata to your instance of Okta. You must configure Secure Access as a generic SAML 2.0 application within Okta. Okta does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** values from the Secure Access metadata file and add these values in Okta.

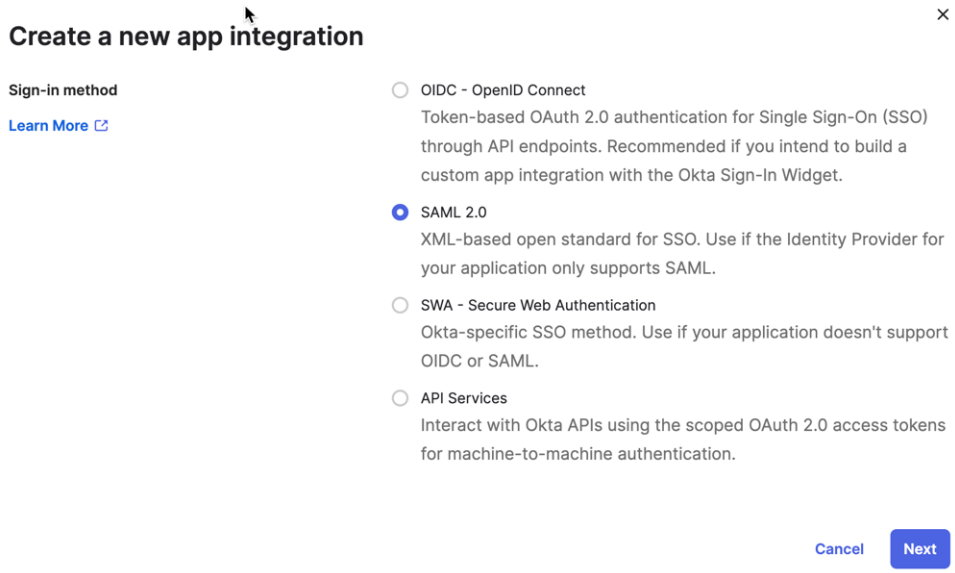
> **Note**
>
> If you have general questions about the Okta SAML IdP, we recommend that you contact Okta.

Before you begin

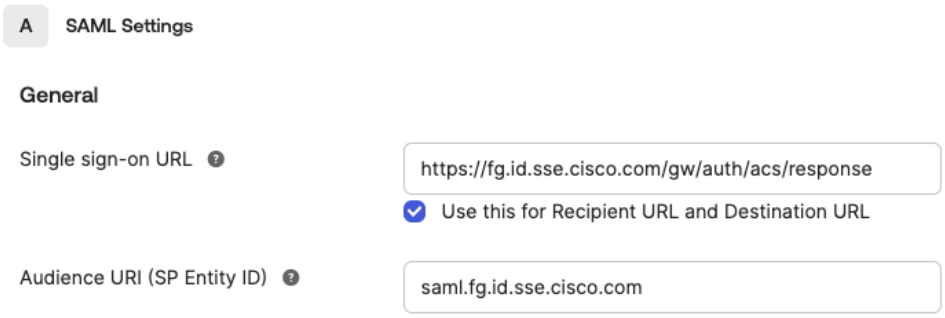
For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

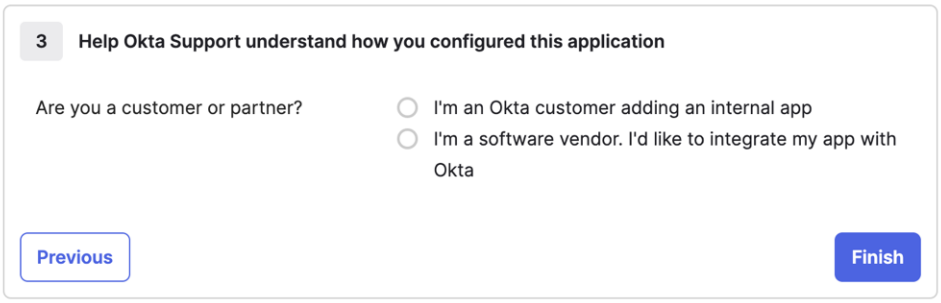
1. Sign in to your instance of Okta, then navigate to **Applications** > **Create a new app integration**.



2. Click **SAML 2.0**, and then click **Next**.
3. For **General Settings**, add a name for the app integration, and then click **Next**.
4. For **SAML Settings > General**, enter the Secure Access service provider metadata URL and the certificates from the file that you downloaded in Step 3 - Download the Secure Access Okta Service Provider Files.
   - For **Single sign-on URL**, add `https://fg.id.sse.cisco.com/gw/auth/acs/response`.
   - For **Audience URI (SP Entity ID)**, add `saml.fg.id.sse.cisco.com`, or the organization-specific entity ID.
   - For **Name ID format**, choose **EmailAddress**.



5. (Optional) Click **Show Advanced Settings**.
6. (Optional) For **Signature Certificate**, upload the root certificate that you downloaded from the **Cisco_SSE_SP_Metadata** XML file. Click **Preview the SAML Assertion** to show the created metadata file, and then click **Next**.
7. Click **I'm an Okta customer adding an internal app**.



8. Click **Finish**.

Step 5 – Get Metadata from Okta App Integration

Provides instructions for completing the Step 5 – Get Metadata from Okta App Integration workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Get and save the Okta metadata created in the Okta app integration. You will add the metadata for the Okta SAML IdP in your Secure Access SSO authentication profile for Okta.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. On Okta, navigate to **Sign on < Settings > Metadata details**.



2. For **Metadata URL**, copy the Okta SAML IdP metadata URL.
3. Click **More Details**.
4. For **Sign on URL**, copy the Okta SAML IdP sign-on URL.
5. For **Signing Certificate**, copy or download the Okta certificate.

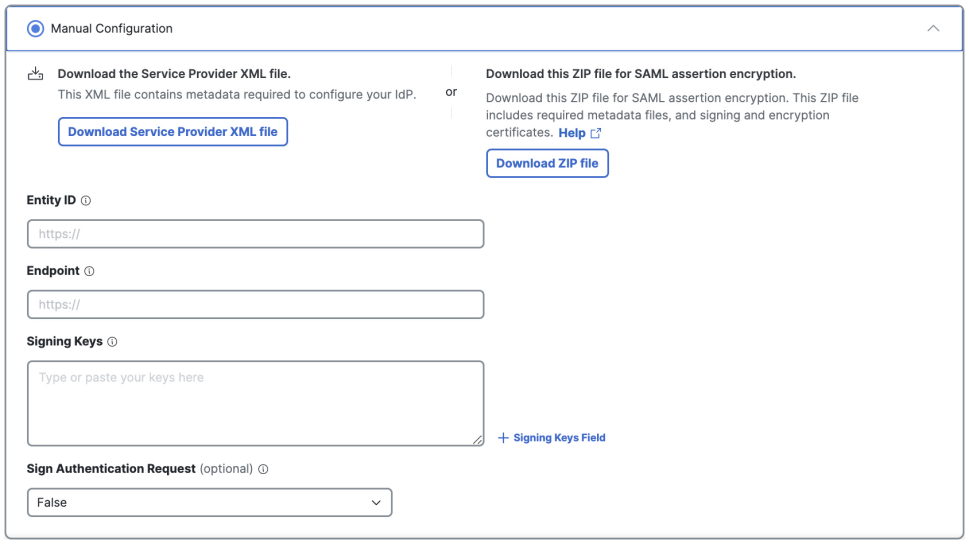
Step 6 – Add Okta Metadata in Secure Access

Provides instructions for completing the Step 6 - Add Okta Metadata in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

First, get the Okta SAML IdP's metadata in Okta. For more information, see Get Metadata from Okta App Integration.

Then, in Secure Access, enter the Okta SAML IdP metadata from the Okta app integration.

- **Entity ID**–The Entity ID for the Okta SAML IdP.
- **Endpoint**–The metadata URL used to communicate with your Okta SAML IdP.
- **Signing Keys**–The Okta SAML IdP's x.509 certificate that is used to sign the authentication request.
- **Signed Authentication Request**–Choose whether to sign the authentication request for the Okta SAML IdP.



Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. For **Entity ID** , enter the Okta app integration's value of **Metadata URL**.
2. For **Endpoint**, enter the Okta app integration's value of **Sign on URL**.
3. For **Signing Keys**, enter the Okta app integration's value of **Signing Certificate**.
4. (Optional) For **Signed Authentication Request**, choose whether to sign the authentication request.
5. Click **Done**.

Configure AD FS for SAML

Describes Configure AD FS for SAML in Cisco Secure Access and outlines Prerequisites and Procedure. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Access (ZTA) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure Active Directory Federation Services (AD FS) with Secure Access by uploading the AD FS XML metadata file to Secure Access, or alternatively add the AD FS metadata in Secure Access manually.

For information about provisioning users from AD FS to Secure Access, see Provision Users and Groups from Active Directory.

Prerequisites

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.
- We recommend that you bypass web traffic to the **id.sse.cisco.com** domain on the Secure Access secure web gateway (SWG).

Procedure

- Step 1 - Add an Authentication Profile in Secure Access
- Step 2 - Add AD FS SAML Identity Provider in Secure Access
- Step 3 - Add the Identity Provider's SAML Metadata to Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 - Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

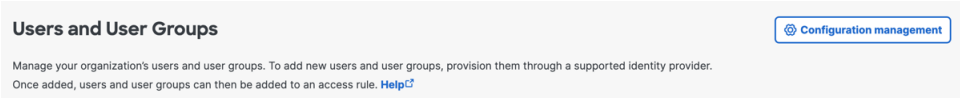
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

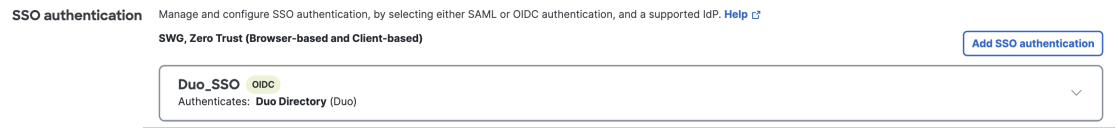
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

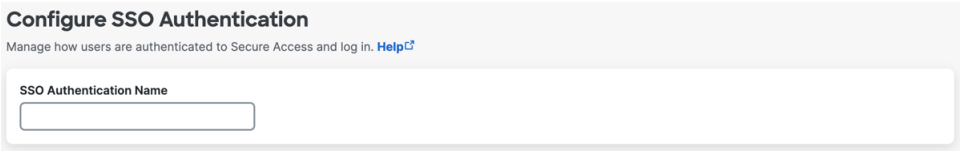
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



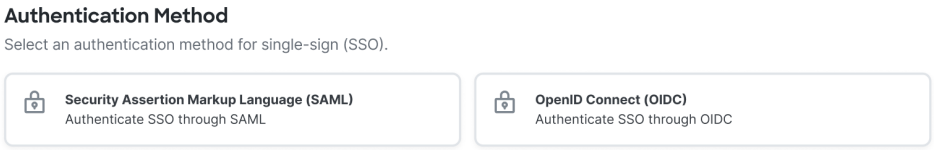
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



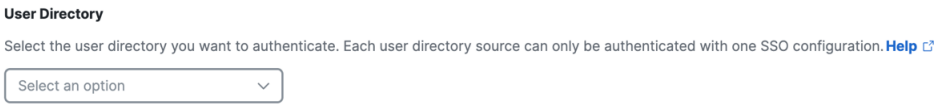
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

Step 2 – Add AD FS Identity Provider in Secure Access

Provides instructions for completing the Step 2 – Add AD FS Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

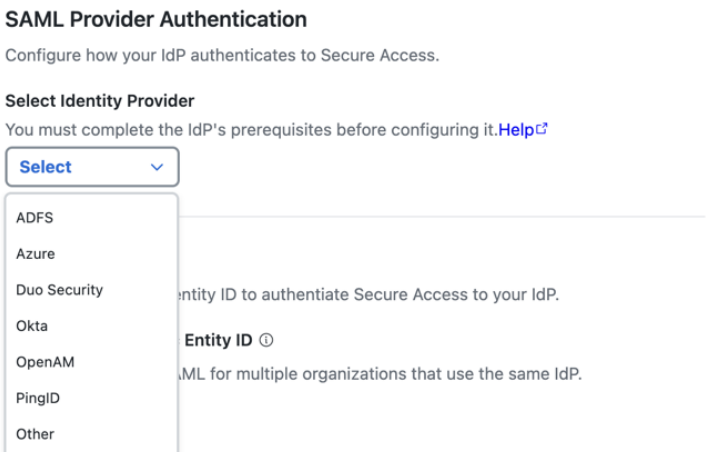
In the SSO authentication profile, select the SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. Select an **Identity Provider**.



3. (Optional) Enable an organization-specific entity ID.

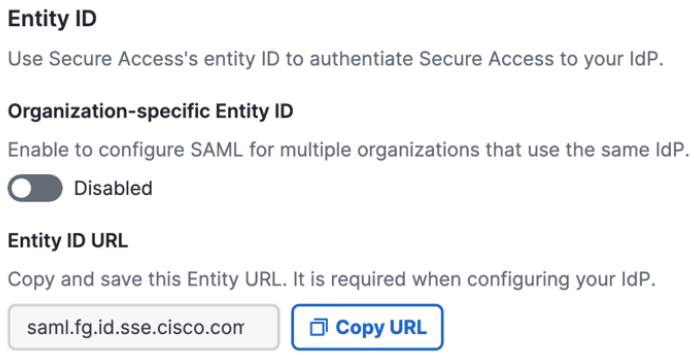
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.

4. For **Entity ID URL**, click **Copy URL**.

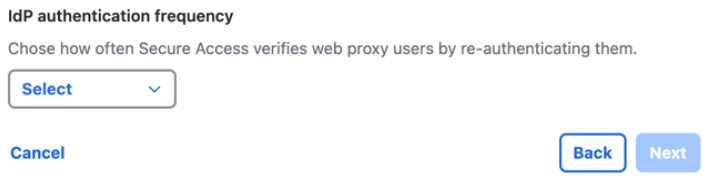
   Save the Secure Access metadata URL in your local environment.

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**.

> **Note**
>
> Use the Secure Access SP metadata URL to configure the SAML IdP app integration.



5. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.



6. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes Step 3 – Add the Identity Provider's SAML Metadata to Secure Access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of AD FS.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of AD FS.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

- Step 3a – Download the Secure Access Service Provider files
- Step 3b – Add the Secure Access Service Provider Metadata to AD FS
- Step 3c – Add the SAML IdP Metadata to Secure Access

Step 3a – Download the Secure Access Service Provider files

Provides instructions for completing the Step 3a – Download the Secure Access Service Provider files workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

> **Note**
>
> Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

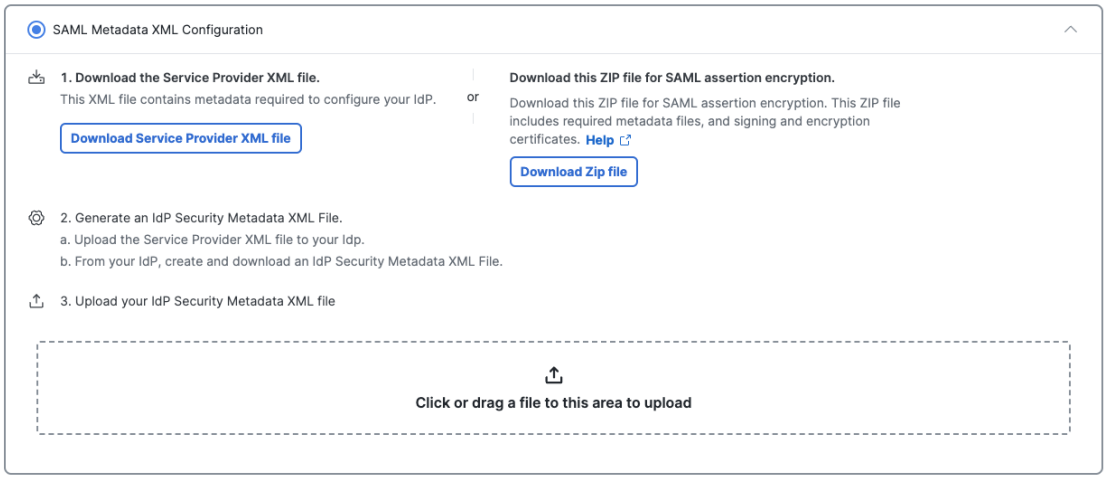
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

1. Check **SAML Metadata XML Configuration** or **Manual Configuration**.
2. Choose between unencrypted or encrypted SAML assertions.
   a) Click **Download Service Provider XML file** for the metadata XML file with the Secure Access root certificate that supports unencrypted SAML assertions.
   b) Click **Download Zip file** for the metadata XML file and signing and encryption certificate files required for encrypted SAML assertions.

      This metadata XML file includes the root certificate metadata for both the signing and the encryption certificates.



3. Open the **Cisco_SSE_SP_Metadata** XML file.
4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save.
   Use the certificate file in the next step when you create the app integration in the SAML IdP.

Step 3b – Add the Secure Access Service Provider Metadata to AD FS

Provides instructions for completing the Step 3b – Add the Secure Access Service Provider Metadata to AD FS workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Add the Secure Access service provider metadata to your instance of AD FS, then download the IdP metadata file to finish configuring Secure Access in the next step.

Contact Microsoft for assistance. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

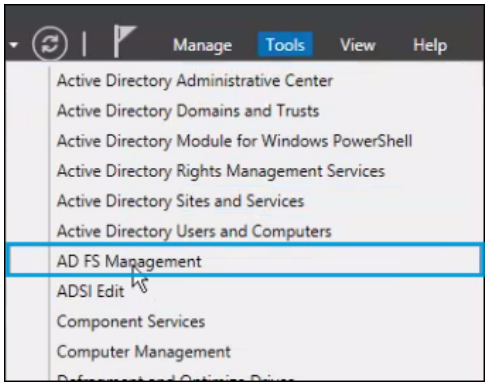
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.
- We recommend that you bypass web traffic to the **id.sse.cisco.com** domain on the Secure Access secure web gateway (SWG).

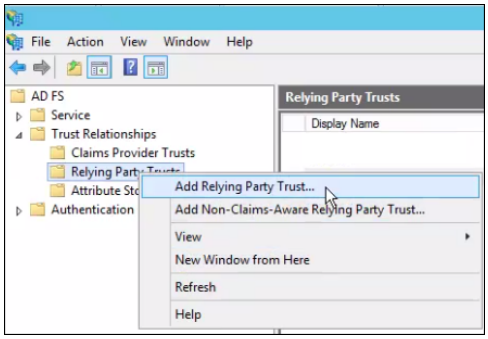
Procedure

---

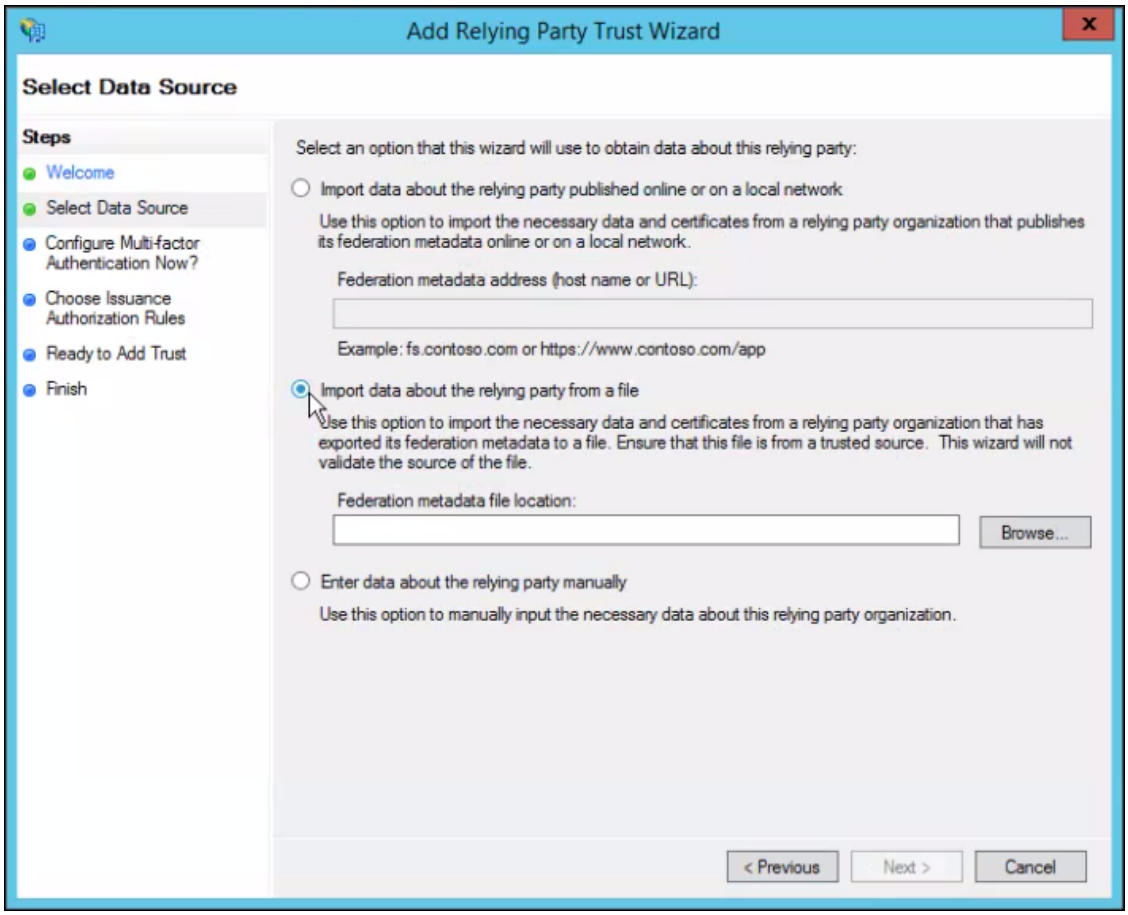
1. Log into AD FS and navigate to **Server Manager > Tools > AD FS Management**.



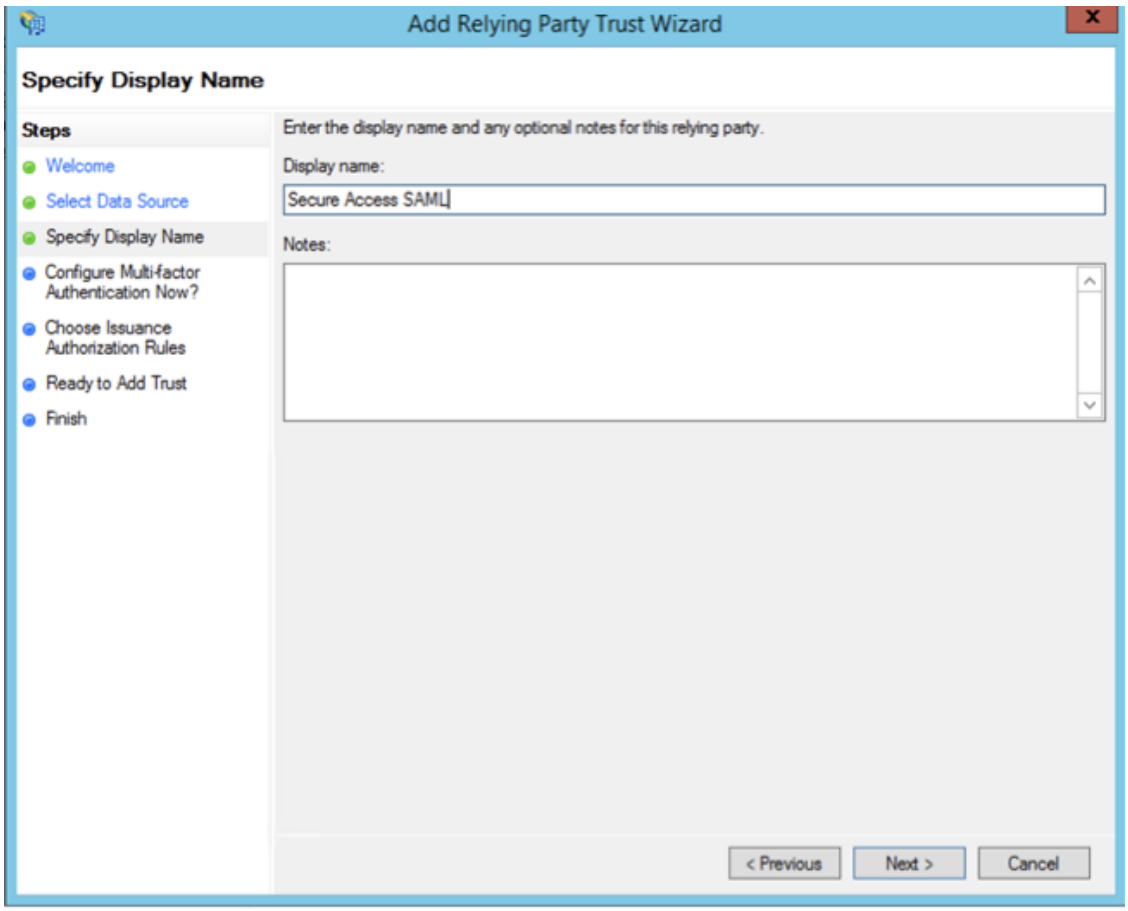
2. In the AD FS Manager, right-click on **Trust Relationships** and navigate to **Relying Party Trusts > Add Relying Party Trust** and select **Start**.



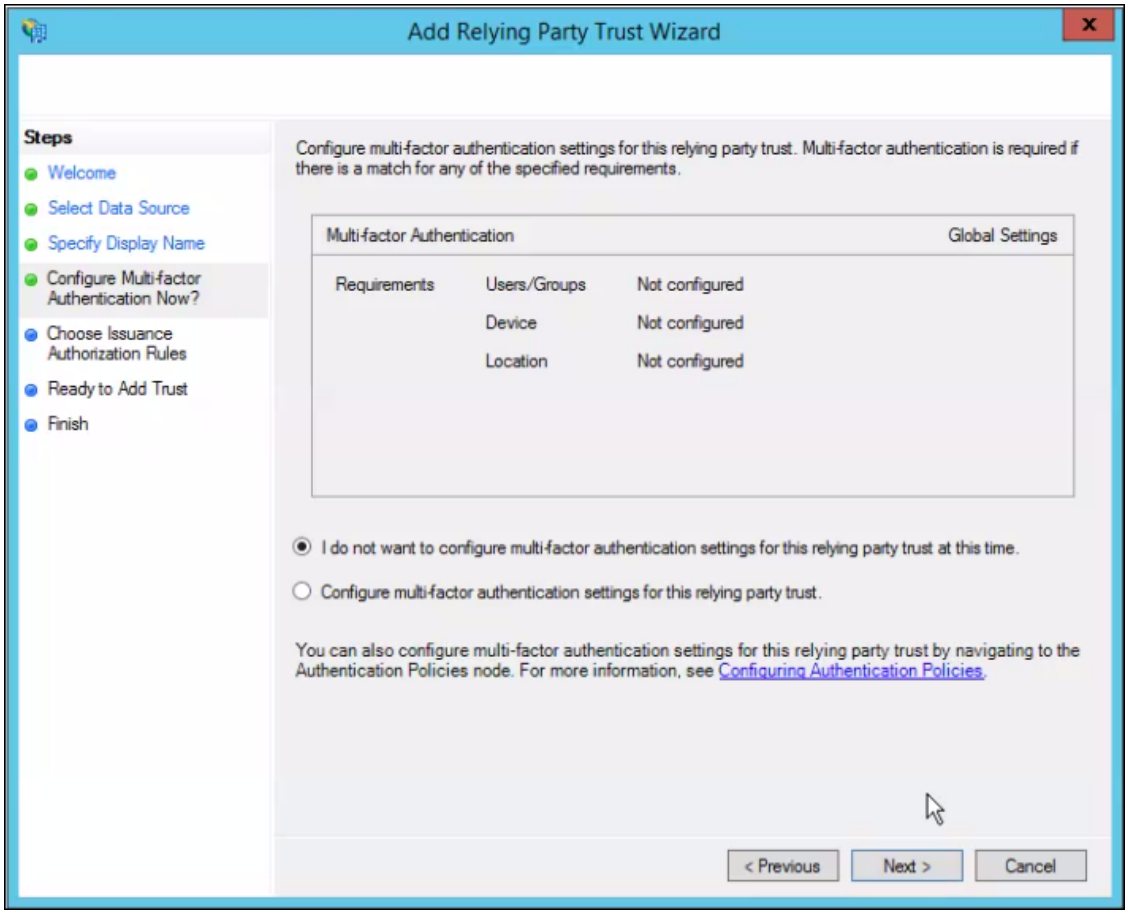
3. Choose **Import data about the relying party from a file** and browse for the **metadata.xml** file downloaded from Secure Access.



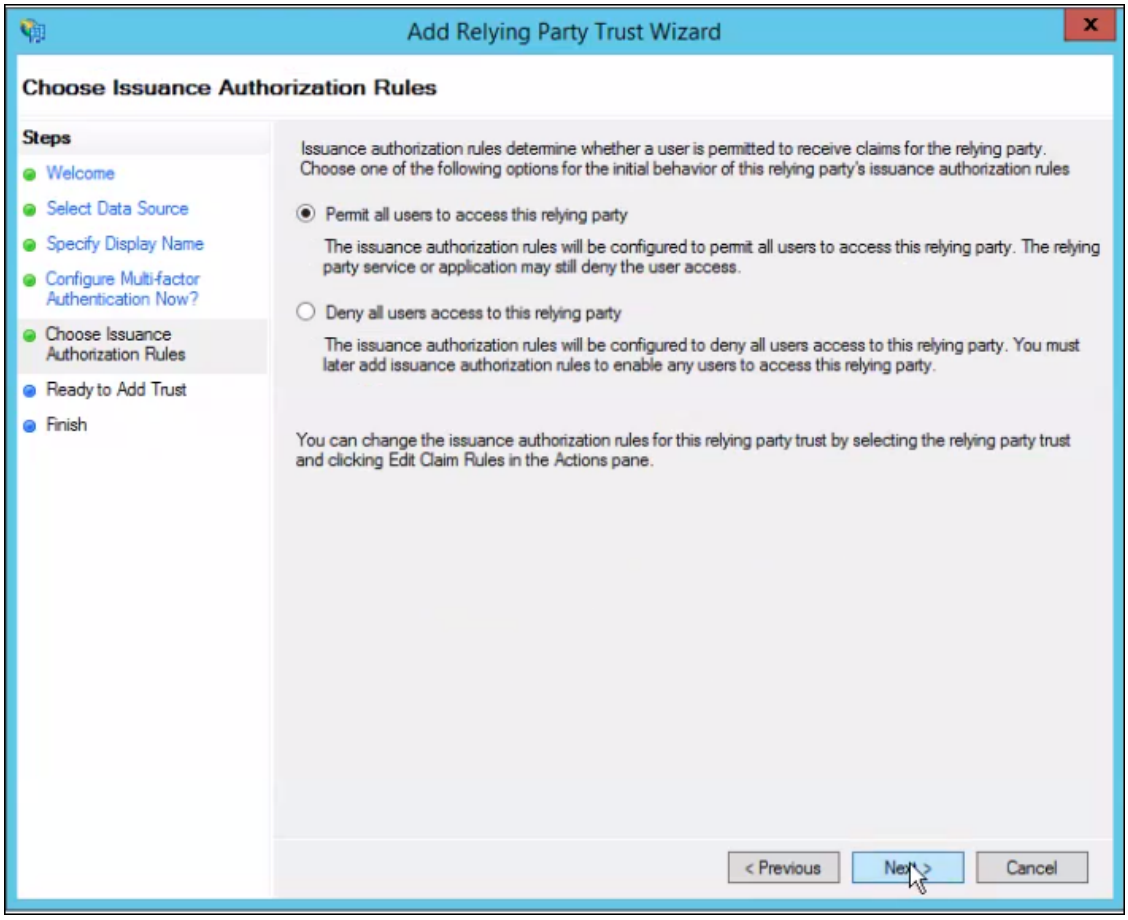
4. For **Display name**, provide a meaningful name for the trust connection, and then click **Next**.



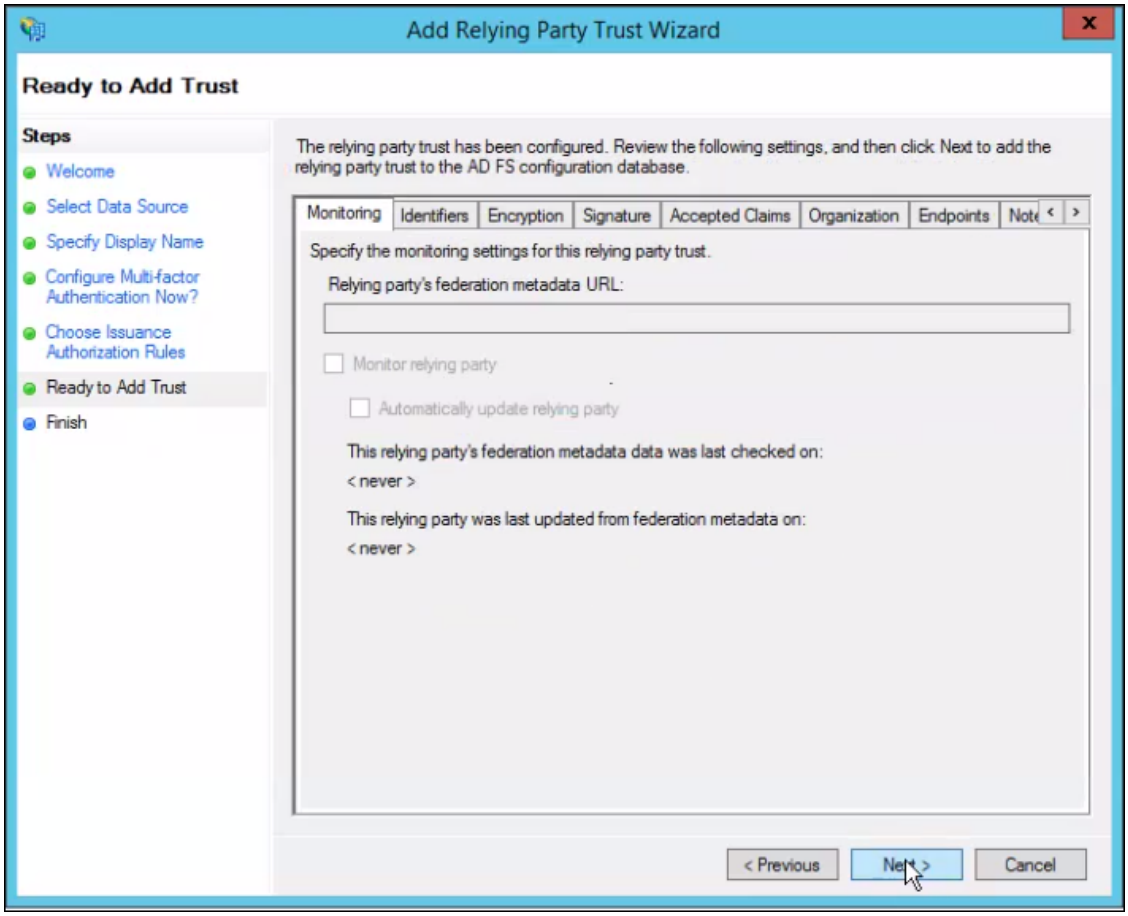
5. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.



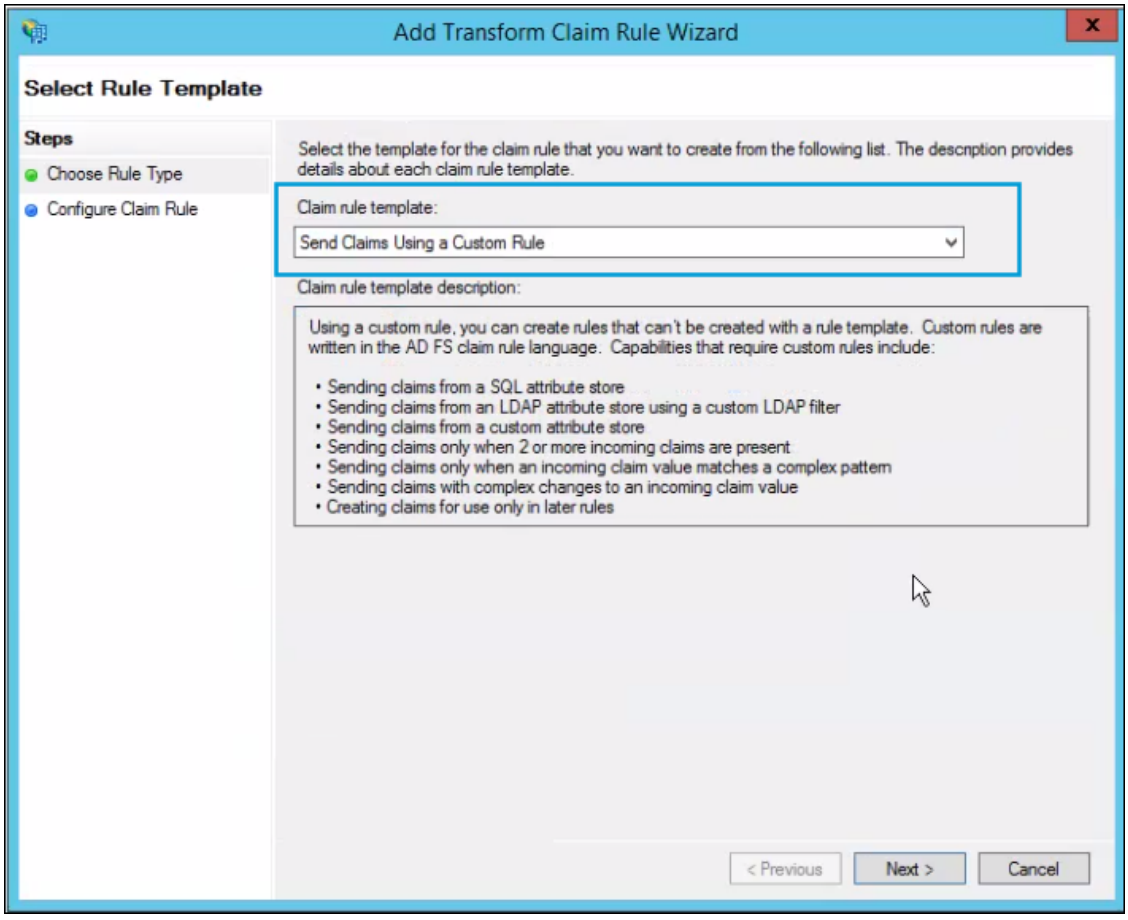
6. Select **Permit all users to access relying party** and click **Next**.



7. Verify settings and click **Next**.



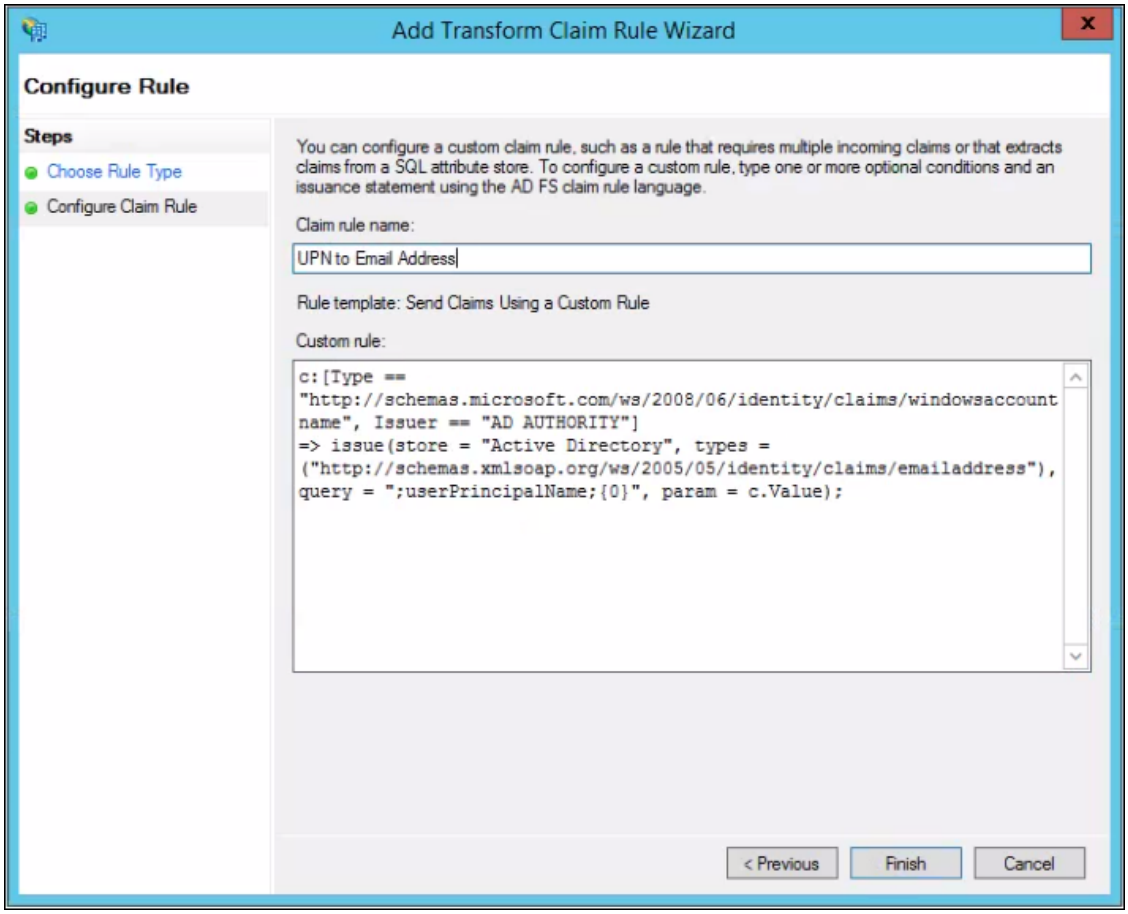
8. Right-click on the recently created relaying party and select **Edit Claim Rules**.



9. Under **Issuance Transform Rules**, click **Add Rule**, then choose **Send Claims Using a Custom Rule**.

```
c:\[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
 Issuer == "AD AUTHORITY"\]

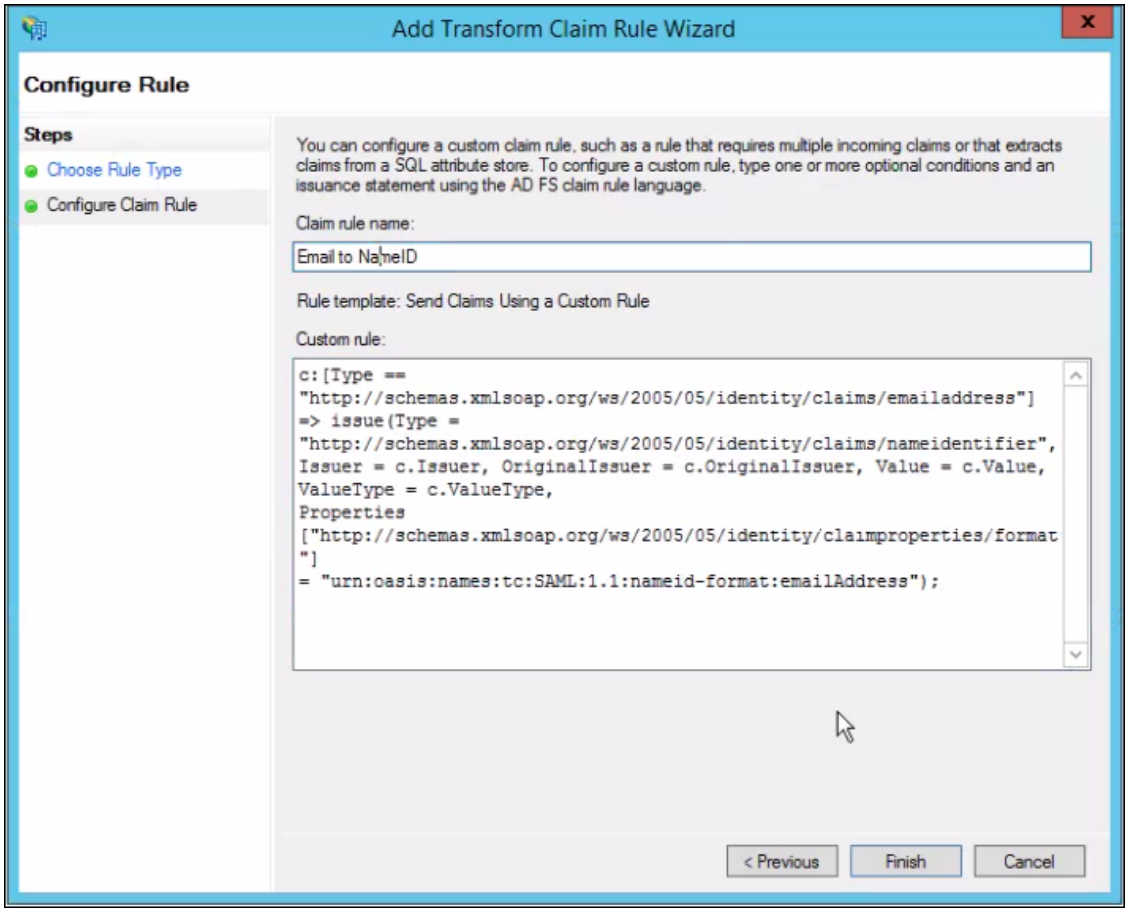
=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"), query
 = ";userPrincipalName;{0}", param = c.Value);
```



10. Repeat the previous step with the following configuration.

```
c:\[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"\]

=> issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
 = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties\["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"\]
 = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

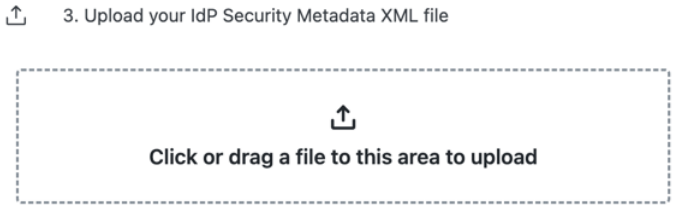


Step 3c – Add the SAML IdP Metadata to Secure Access

Provides instructions for completing the Step 3c – Add the SAML IdP Metadata to Secure Access workflow in Cisco Secure Access. If you selected SAML Metadata XML Configuration in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click Done.

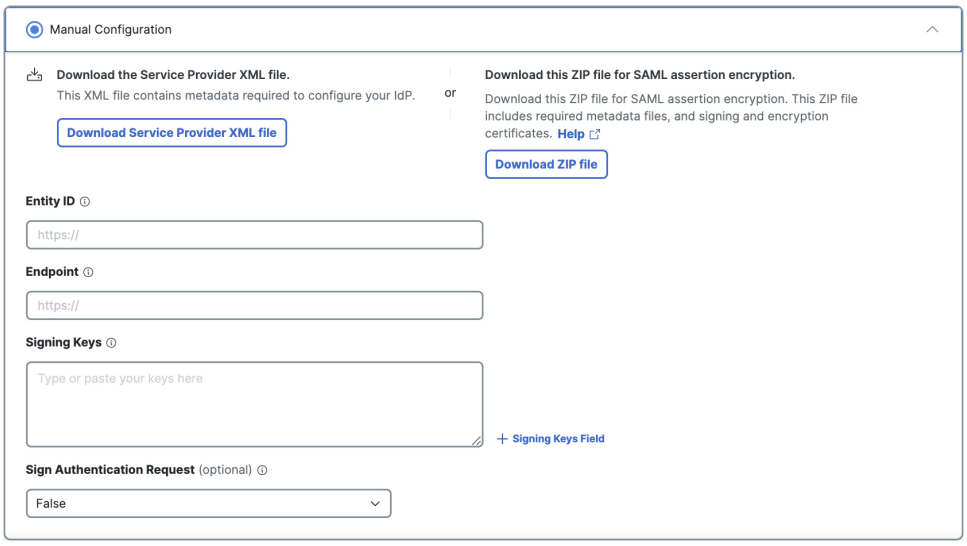
Procedure

1. If you selected **SAML Metadata XML Configuration** in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click **Done**.



2. If you selected **Manual Configuration** in Step 3a, enter your SAML IdP metadata for the Secure Access settings, then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.

- **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



Configure Duo Security for SAML

Describes Configure Duo Security for SAML in Cisco Secure Access and outlines Prerequisites and Procedure. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Access (ZTA) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Duo Security SAML IdP with Secure Access by uploading the Duo Security XML metadata file to Secure Access, or alternatively add the Duo Security metadata in Secure Access manually.

Prerequisites

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

- Step 1 – Add an Authentication Profile in Secure Access
- Step 2 – Add Duo SAML Identity Provider in Secure Access
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 – Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

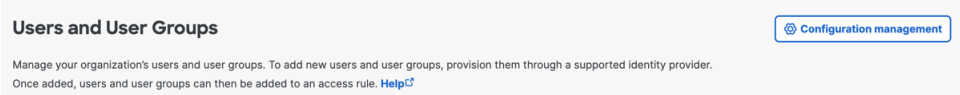
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

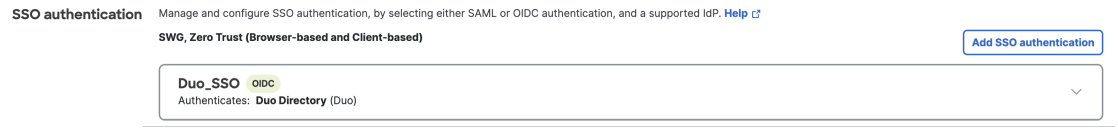
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

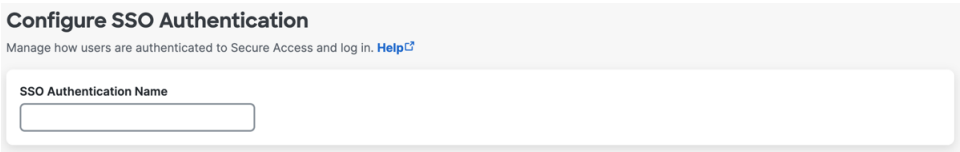
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



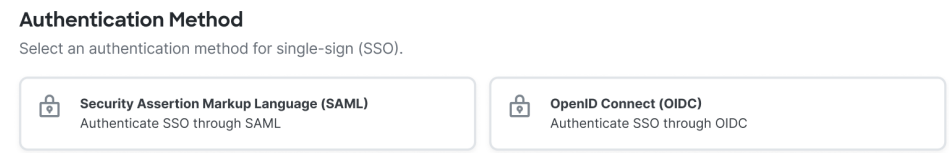
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



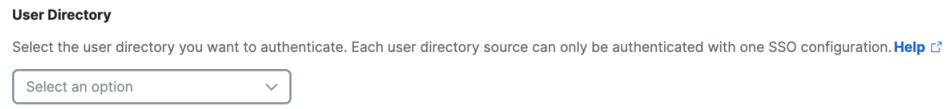
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

Step 2 – Add Duo Identity Provider in Secure Access

Provides instructions for completing the Step 2 - Add Duo Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

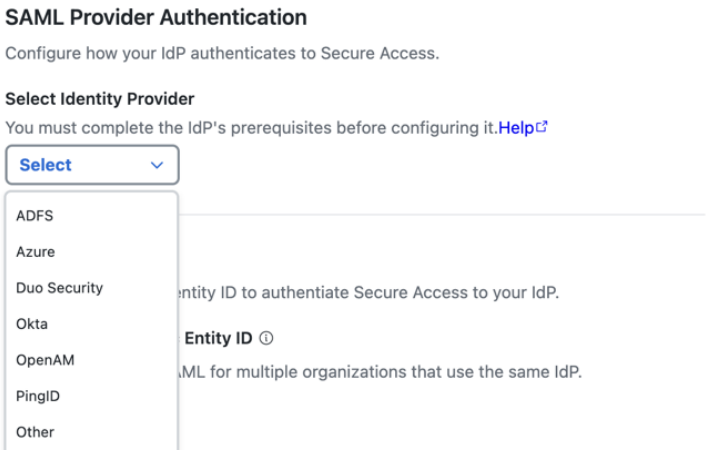
In the SSO authentication profile, select the SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. Select an **Identity Provider**.



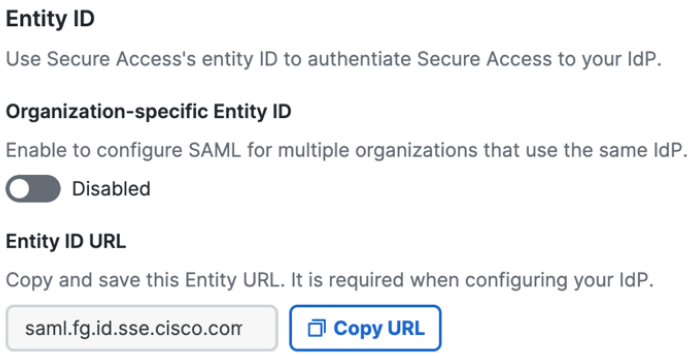
3. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.

4. For **Entity ID URL**, click **Copy URL**.

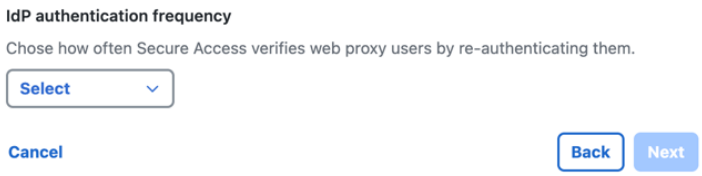
   Save the Secure Access metadata URL in your local environment.

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**.

   > **Note**
   >
   > Use the Secure Access SP metadata URL to configure the SAML IdP app integration.



5. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.



6. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes Step 3 - Add the Identity Provider's SAML Metadata to Secure Access. Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Duo Security.

Download the Secure Access Metadata XML file and use the service provider file to configure your instance of Duo Security.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

- Step 3a - Download the Secure Access Service Provider files
- Step 3b - Add the Secure Access Service Provider Metadata to Duo Security
- Step 3c - Add the Duo Security SAML Metadata to Secure Access

Step 3a – Download the Secure Access Service Provider files

Provides instructions for completing the Step 3a - Download the Secure Access Service Provider files workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

> **Note**
>
> Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

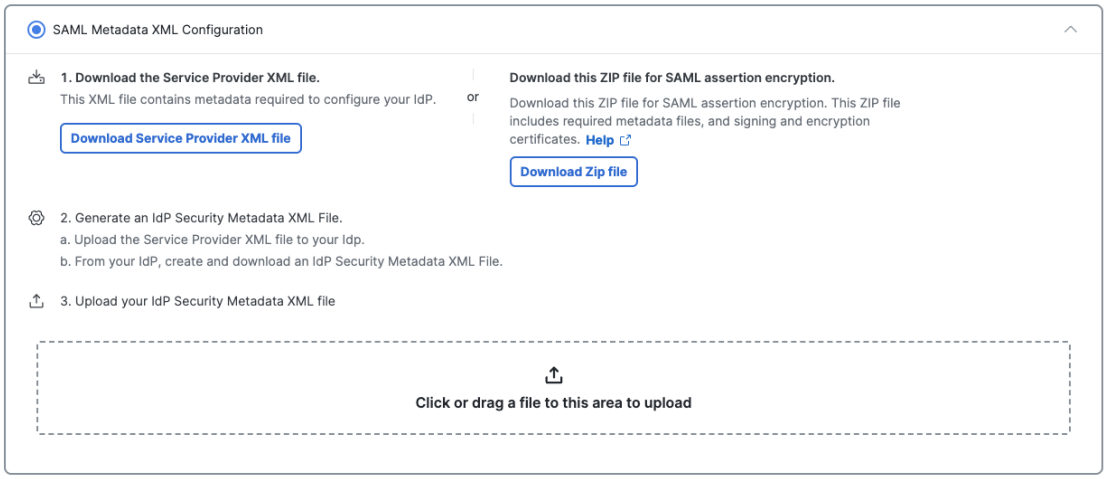
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

1. Check **SAML Metadata XML Configuration** or **Manual Configuration**.
2. Choose between unencrypted or encrypted SAML assertions.
   a) Click **Download Service Provider XML file** for the metadata XML file with the Secure Access root certificate that supports unencrypted SAML assertions.
   b) Click **Download Zip file** for the metadata XML file and signing and encryption certificate files required for encrypted SAML assertions.

      This metadata XML file includes the root certificate metadata for both the signing and the encryption certificates.



3. Open the **Cisco_SSE_SP_Metadata** XML file.
4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save.

   Use the certificate file in the next step when you create the app integration in the SAML IdP.

Step 3b – Add Secure Access Service Provider Metadata to Duo Security

Provides instructions for completing the Step 3b - Add Secure Access Service Provider Metadata to Duo Security workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Configure Secure Access with a Duo Single Sign-On for Cisco Secure Access. Add the Secure Access service provider metadata to Duo, then download the IdP metadata file from Duo to finish configuring Secure Access.

Contact Duo Security for assistance. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to the Duo Security documentation.

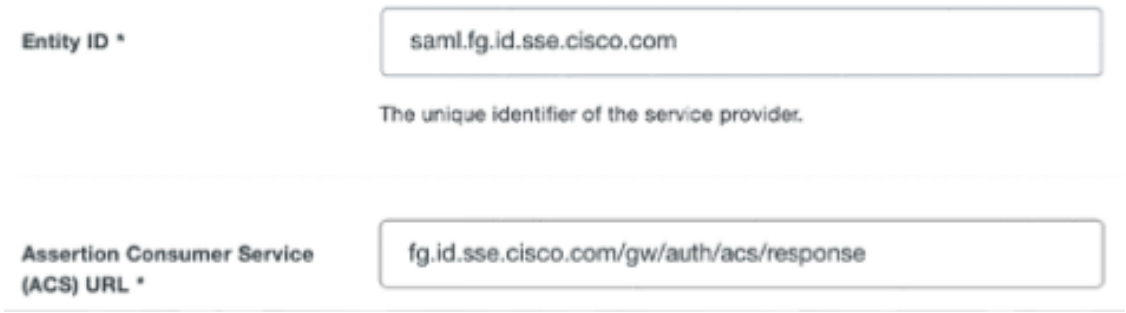
- To automatically configure the Cisco Secure Access SAML Duo Single Sign-On application, use the **Metadata Discovery** option in Update Your Cloud Application in Duo. Upload the Secure Access service provider metadata file **Cisco_SSE_SP_Metadata** to the Duo Single Sign-On app.
- To manually configure the Cisco Secure Access SAML Duo Single Sign-On application, extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata and add these to the applicable fields in Duo Security.

Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

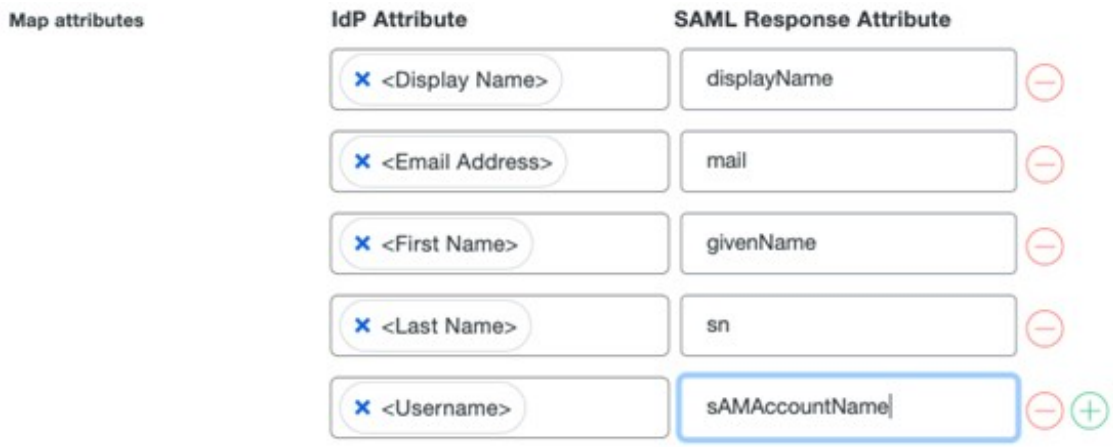
1. Sign in to the Duo admin portal and navigate to **Applications > Protect an Application**.
2. Search for **Cisco Secure Access Service Provider** and select **2FA with SSO hosted by Duo**.
3. For **Entity ID**, enter **saml.fg.id.sse.cisco.com** and for **Assertion Consumer Service (ACS) URL**, enter **fg.id.sse.cisco.com/gw/auth/acs/response**.



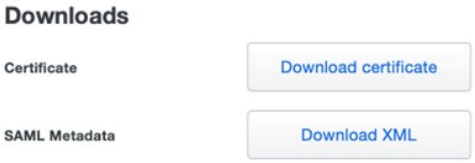
4. Enter an email address in the **NameID attribute** field.



5. For **Map attributes**, configure the IdP attributes.
   - **Display name**–Enter the name you want to display.
   - **Email Address**–Enter an email address.
   - **First Name**–Enter the first name.
   - **Last Name**–Enter the last name.
   - **Username**–Enter the user name.



6. Click **Save**.
7. Click **Download certificate** to download the certificate, and then click **Download XML** to download the SAML Metadata file.



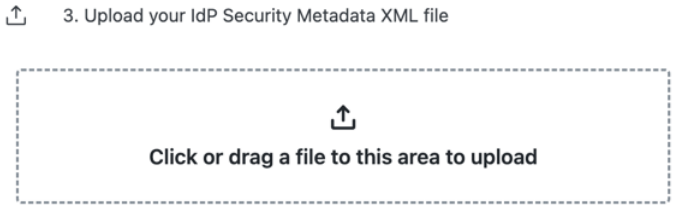
Step 3c – Add the Duo Security SAML Metadata to Secure Access

Provides instructions for completing the Step 3c - Add the Duo Security SAML Metadata to Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

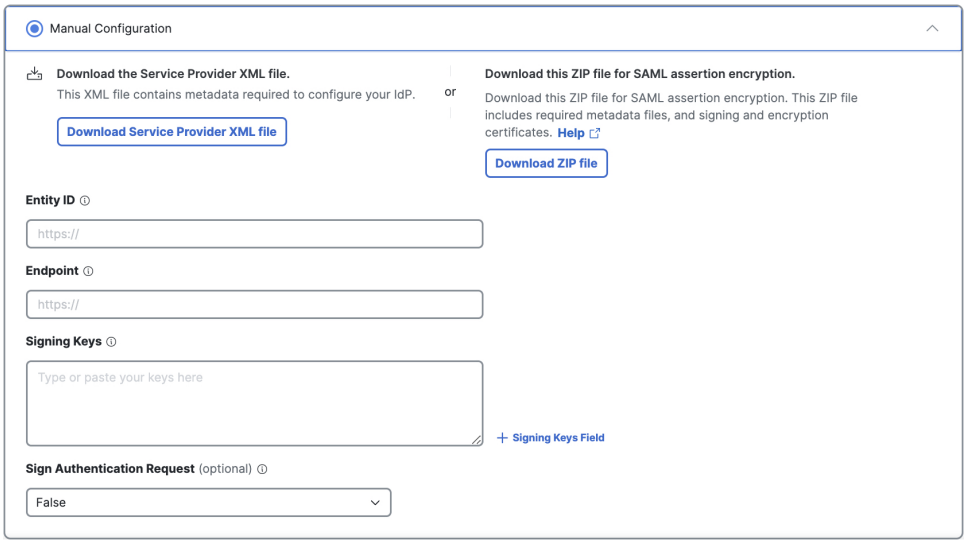
Procedure

---

1. If you selected **SAML Metadata XML Configuration** in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click **Done**.



2. If you selected **Manual Configuration** in Step 3a, enter your SAML IdP metadata for the Secure Access settings, then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



Configure Ping Identity for SAML

Describes Configure Ping Identity for SAML in Cisco Secure Access and outlines Prerequisites and Procedure. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Access (ZTA) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the Ping Identity SAML IdP with Secure Access by uploading the Ping Identity XML metadata file to Secure Access, or alternatively add the Ping Identity metadata in Secure Access manually.

Prerequisites

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

- Step 1 - Add an Authentication Profile in Secure Access
- Step 2 - Add Ping SAML Identity Provider in Secure Access
- Step 3 - Add the Identity Provider's SAML Metadata to Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 - Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

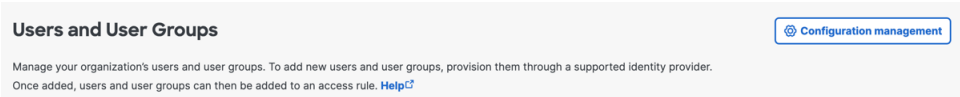
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

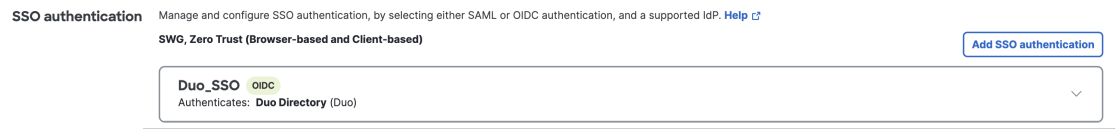
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

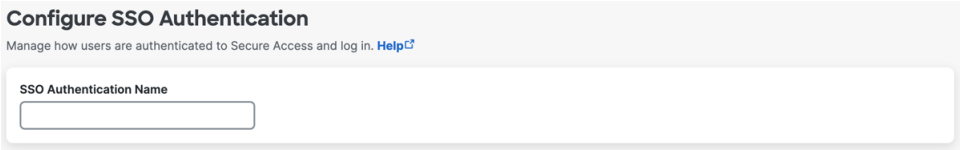
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



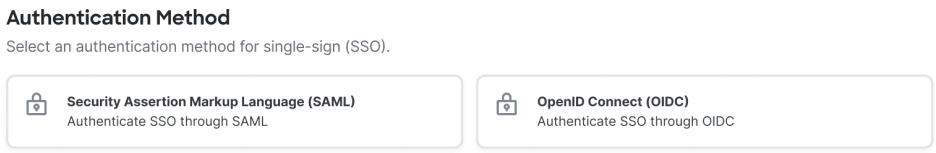
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



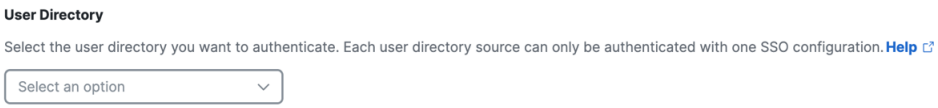
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.

7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.
9. Click **Done**.

Step 2 – Add Ping Identity Provider in Secure Access

Provides instructions for completing the Step 2 - Add Ping Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

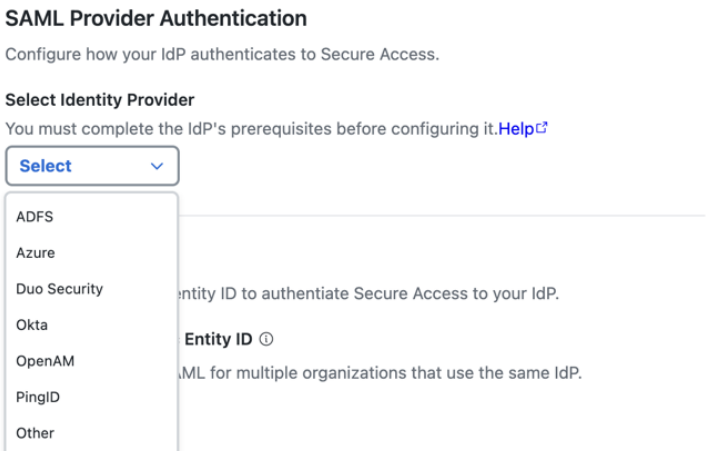
In the SSO authentication profile, select the SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. Select an **Identity Provider**.



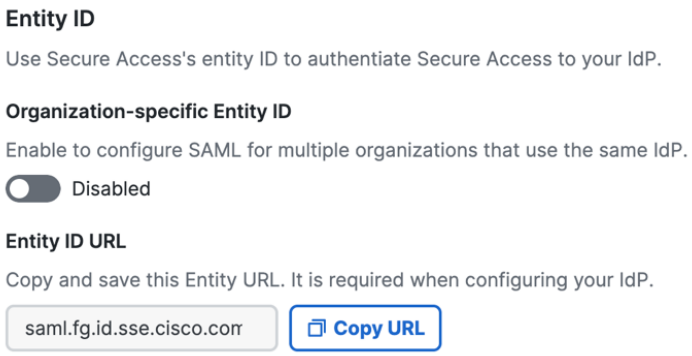
3. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.

4. For **Entity ID URL**, click **Copy URL**.

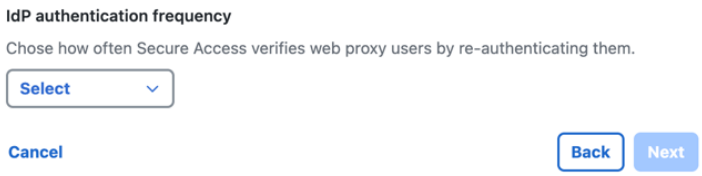
   Save the Secure Access metadata URL in your local environment.

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**.

   > **Note**
   >
   > Use the Secure Access SP metadata URL to configure the SAML IdP app integration.



5. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.



6. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes Step 3 - Add the Identity Provider's SAML Metadata to Secure Access. Download the Secure Access metadata files and use the service provider file to configure your instance of Ping Identity.

Download the Secure Access metadata files and use the service provider file to configure your instance of Ping Identity.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

- Step 3a - Download the Secure Access Service Provider files
- Step 3b - Add the Secure Access Service Provider Metadata to Ping Identity
- Step 3c - Add the Ping Identity SAML Metadata to Secure Access

Step 3a – Download the Secure Access Service Provider files

Provides instructions for completing the Step 3a - Download the Secure Access Service Provider files workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

> **Note**
>
> Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

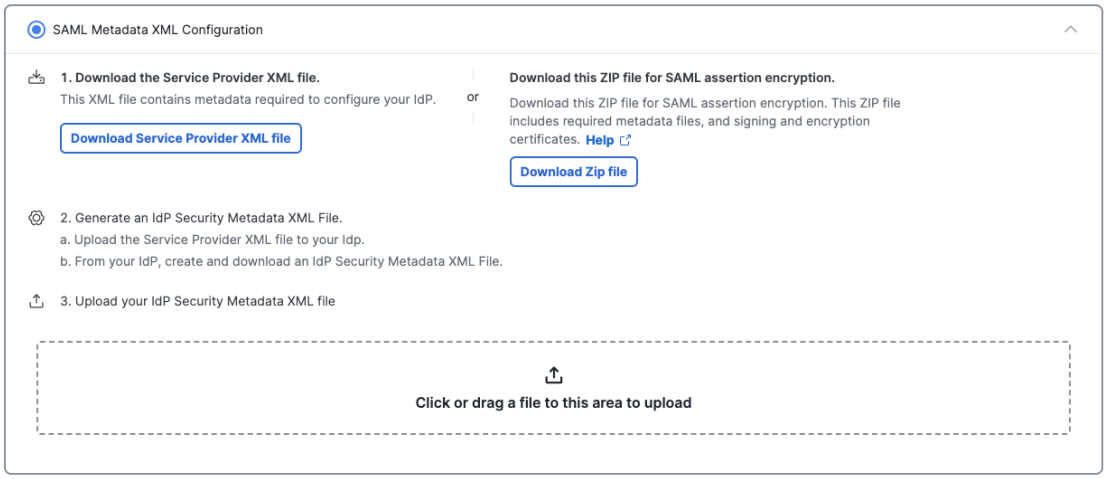
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

1. Check **SAML Metadata XML Configuration** or **Manual Configuration**.
2. Choose between unencrypted or encrypted SAML assertions.
   a) Click **Download Service Provider XML file** for the metadata XML file with the Secure Access root certificate that supports unencrypted SAML assertions.
   b) Click **Download Zip file** for the metadata XML file and signing and encryption certificate files required for encrypted SAML assertions.

      This metadata XML file includes the root certificate metadata for both the signing and the encryption certificates.



3. Open the **Cisco_SSE_SP_Metadata** XML file.
4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save.

   Use the certificate file in the next step when you create the app integration in the SAML IdP.

Step 3b – Add the Secure Access Service Provider Metadata to Ping Identity

Describes Step 3b - Add the Secure Access Service Provider Metadata to Ping Identity. Add the Secure Access service provider metadata to your instance of Ping Identity.

Add the Secure Access service provider metadata to your instance of Ping Identity.

You must configure Secure Access as a generic SAML 2.0 application within Ping Identity. Ping Identity does not provide a method to upload Secure Access metadata for automatic configuration. Extract the **EntityID** and **AssertionConsumerService** URLs from the Secure Access metadata and add these to the applicable fields in Ping Identity.

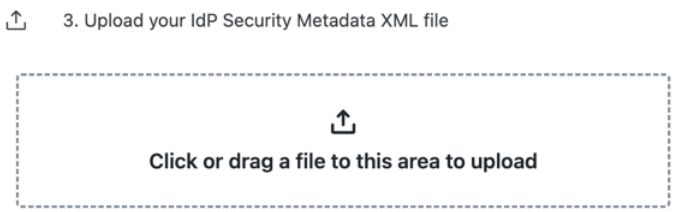
Contact Ping Identity for assistance. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

Step 3c – Add the Ping Identity SAML Metadata to Secure Access

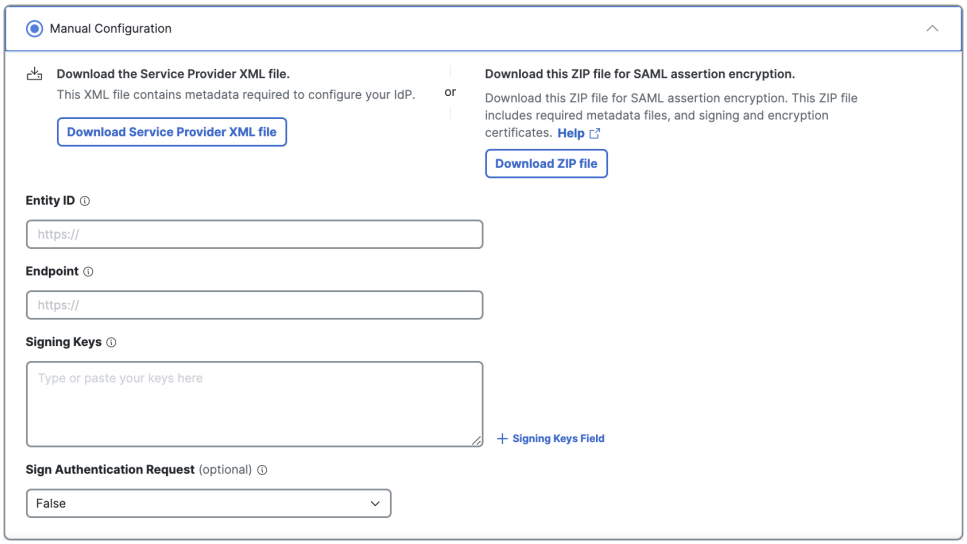
Provides instructions for completing the Step 3c - Add the Ping Identity SAML Metadata to Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. If you selected **SAML Metadata XML Configuration** in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click **Done**.



2. If you selected **Manual Configuration** in Step 3a, enter your SAML IdP metadata for the Secure Access settings, then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



Configure OpenAM for SAML

Describes Configure OpenAM for SAML in Cisco Secure Access. Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Access (ZTA) enabled.

Cisco Secure Access uses Security Assertion Markup Language (SAML) to authenticate and authorize web requests from user devices on networks and network tunnels with Web security enabled, and requests to private resources from user devices with Zero Trust Access (ZTA) enabled. To support SAML authentication and authorization, you must configure the integration of an SAML identity provider (IdP) in Secure Access.

Configure the OpenAM SAML IdP with Secure Access by uploading the OpenAM XML metadata file to Secure Access, or alternatively add the OpenAM metadata in Secure Access manually.

Prerequisites

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

- Step 1 – Add an Authentication Profile in Secure Access
- Step 2 – Add SAML Identity Provider in Secure Access
- Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Step 1 – Add SSO Authentication Profile in Secure Access

Provides instructions for completing the Step 1 – Add SSO Authentication Profile in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This guide describes how to add SSO authentication profiles for the integration of user authentication IdPs in Secure Access.

After you provision users and groups in Cisco Secure Access with a provisioning identity provider (IdP), you can configure the integration of a single sign-on (SSO) authentication identity provider (IdP). Secure Access supports Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to authenticate users.

When you add an SSO authentication profile in Secure Access, you must assign one of the user directories (integrated cloud provisioning IdPs) with the profile. You can associate a user directory that is not already assigned to an SSO authentication profile. For more information, see Manage User Directories.

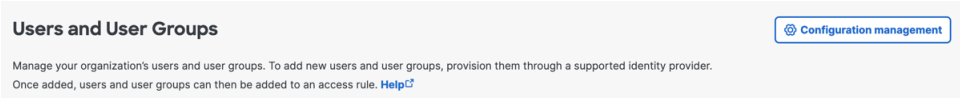
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add the Cisco User Management Connector integration app. For more information see Add the Cisco User Management Connector App in Okta on page 663.

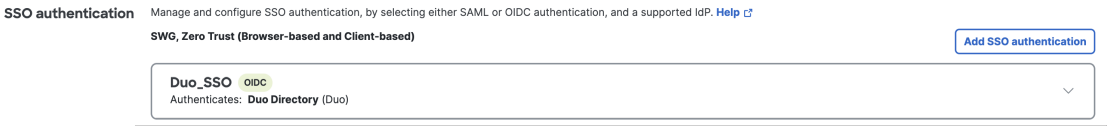
> **Note**
>
> When you add the Cisco User Management Connector application to your IdP, the connector app only supports SAML. You cannot use OIDC to authenticate with the connector.

Procedure

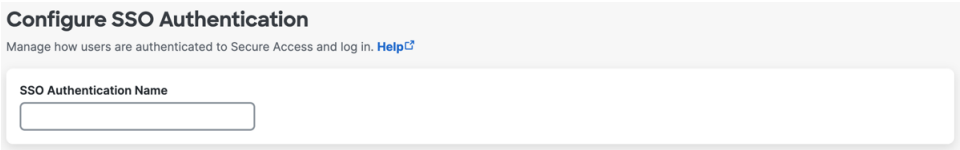
1. Navigate to **Connect** > **Users and User Groups**, and then click **Configuration management**.



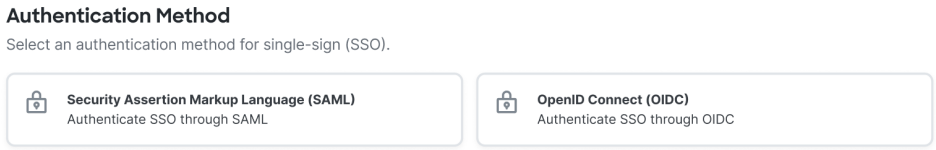
2. Navigate to **SSO authentication**, and then click **Add SSO authentication**.



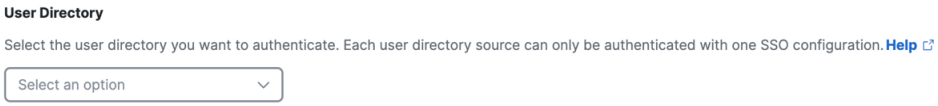
3. For **SSO Authentication Name**, enter a unique name for the SSO authentication profile.



4. For **Authentication Method**, click **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)**.



5. For **User Directory**, choose the directory for the cloud IdP that provisions the users and groups.



6. Click **Next**.
7. For **IdP Authentication**, follow the steps in the OIDC or SAML configuration guides to complete the integration of the SSO authentication IdP.
   - For more information, see Configure Integrations with OIDC Identity Providers. Note that the Cisco User Management Connector does not support OIDC as an authentication method.
   - For more information, see Configure Integrations with SAML Identity Providers.
8. We **strongly** recommend deploying a test configuration to ensure users can authenticate with the assigned IdP. For more information see Test SAML Identity Provider Integration on page 832.

9. Click **Done**.

Step 2 – Add OpenAM Identity Provider in Secure Access

Provides instructions for completing the Step 2 – Add OpenAM Identity Provider in Secure Access workflow in Cisco Secure Access. For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

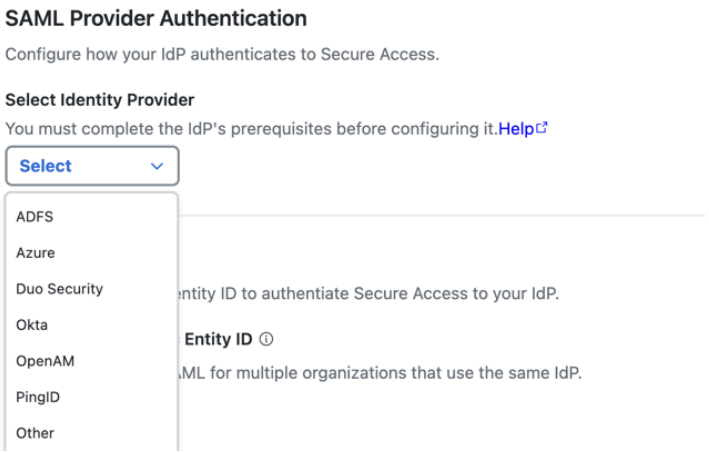
In the SSO authentication profile, select the SAML IdP, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.

Before you begin

For information on the prerequisites to integrate an SAML IdP with Secure Access, see Prerequisites for SAML Authentication.

Procedure

1. In the IdP Authentication section, step 2 of the wizard, copy the metadata URL for the Secure Access service provider, and choose the time interval when end users will authenticate with Secure Access.
2. Select an **Identity Provider**.



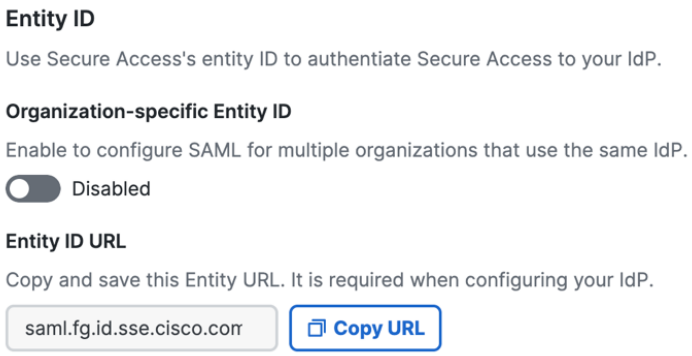
3. (Optional) Enable an organization-specific entity ID.
   - **Organization-specific Entity ID**–Choose this option when you have multiple Secure Access organizations and need to configure SAML authentication for Secure Access Internet Security and Zero Trust Network Access (ZTNA) for these organizations against the same IdP. The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**. Secure Access allows you to override the default Secure Access SAML EntityID for each organization.

4. For **Entity ID URL**, click **Copy URL**.

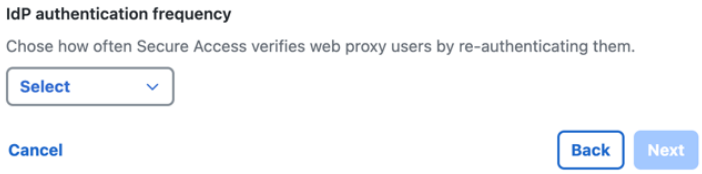
   Save the Secure Access metadata URL in your local environment.

   The Secure Access SAML default common `EntityID` is **saml.fg.id.sse.cisco.com**.

> **Note**
>
> Use the Secure Access SP metadata URL to configure the SAML IdP app integration.



5. Choose a time interval when a user must authenticate with Secure Access, or select **Never**. The time intervals are: **Daily**, **Weekly**, or **Monthly**.



6. Click **Next**.

Step 3 – Add the Identity Provider's SAML Metadata to Secure Access

Describes Step 3 - Add the Identity Provider's SAML Metadata to Secure Access. Download the Secure Access metadata files and use the service provider file to configure your instance of OpenAM.

Download the Secure Access metadata files and use the service provider file to configure your instance of OpenAM.

The Secure Access service provider metadata includes the service provider Issuer ID, the assertion consumer endpoint URL, and the SAML request signing certificate from Secure Access. The Secure Access metadata is required when configuring your IdP.

Your IdP must send the Cisco Secure Access **User principal name** in the **NameID** attribute in the SAML assertion.

- Step 3a - Download the Secure Access Service Provider files
- Step 3b - Add the Secure Access Service Provider Metadata to OpenAM
- Step 3c - Add the SAML IdP Metadata to Secure Access

Step 3a – Download the Secure Access Service Provider files

Provides instructions for completing the Step 3a - Download the Secure Access Service Provider files workflow in Cisco Secure Access. For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Note

Encrypted SAML assertions are a compliance standard in many industries and mitigate the risk of intercepted SAML assertions.

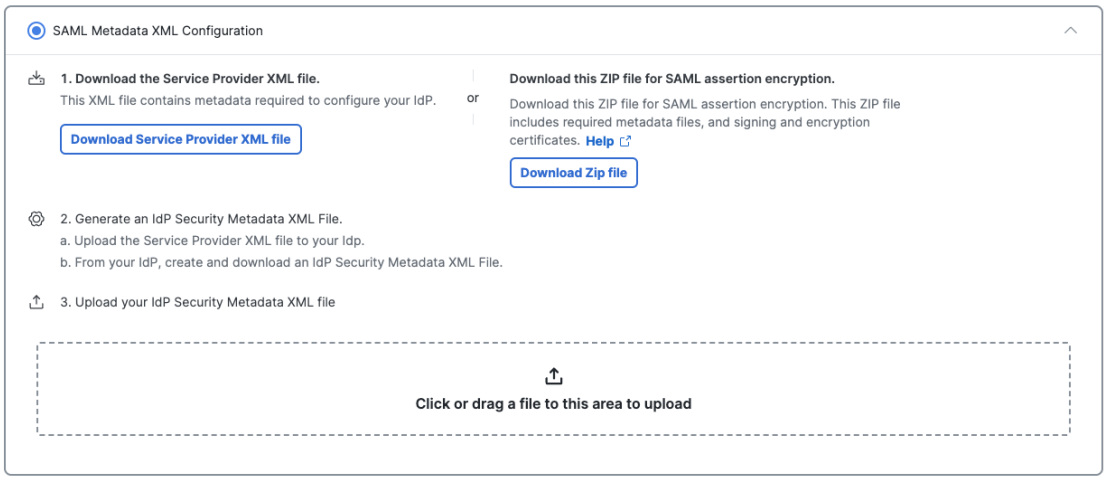
Before you begin

- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Procedure

1. Check **SAML Metadata XML Configuration** or **Manual Configuration**.
2. Choose between unencrypted or encrypted SAML assertions.
   a) Click **Download Service Provider XML file** for the metadata XML file with the Secure Access root certificate that supports unencrypted SAML assertions.
   b) Click **Download Zip file** for the metadata XML file and signing and encryption certificate files required for encrypted SAML assertions.

      This metadata XML file includes the root certificate metadata for both the signing and the encryption certificates.



3. Open the **Cisco_SSE_SP_Metadata** XML file.
4. Copy the certificates from the **Cisco_SSE_SP_Metadata** XML file to a new file and save.
   Use the certificate file in the next step when you create the app integration in the SAML IdP.

Step 3b – Add Secure Access Service Provider Metadata to OpenAM

Describes Step 3b – Add Secure Access Service Provider Metadata to OpenAM. Add the Secure Access service provider metadata to your instance of OpenAM, then download the IdP metadata file to finish configuring Secure Access in the next step.

Add the Secure Access service provider metadata to your instance of OpenAM, then download the IdP metadata file to finish configuring Secure Access in the next step.

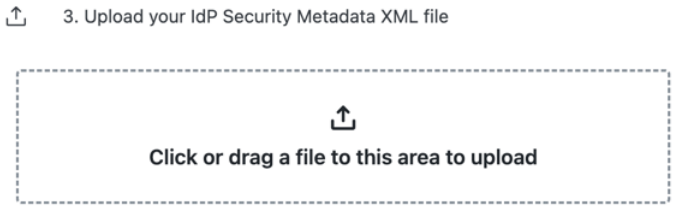
Contact OpenAM for assistance. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP's signing certificate, refer to your vendor's documentation.

Step 3c – Add the OpenAM Metadata to Secure Access

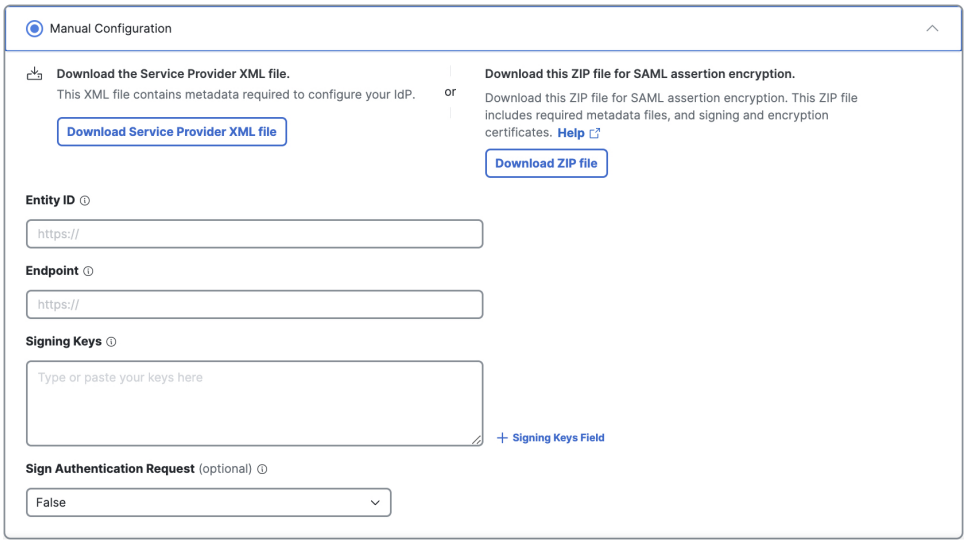
Provides instructions for completing the Step 3c – Add the OpenAM Metadata to Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. If you selected **SAML Metadata XML Configuration** in Step 3a, upload your configured SAML IdP Metadata XML file to Secure Access, then click **Done**.



2. If you selected **Manual Configuration** in Step 3a, enter your SAML IdP metadata for the Secure Access settings, then click **Done**.
   - **Entity ID**–A globally unique name for an identity provider.
   - **Endpoint**–The URL used to communicate with your identity provider.
   - **Signing Keys**–Your identity provider's x.509 certificate that is used to sign the authentication request.
   - **Signed Authentication Request (optional)**–Choose whether to sign the authentication request for the IdP.



SAML Certificate Renewal Options

Describes SAML Certificate Renewal Options in Cisco Secure Access. A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate.

A SAML identity provider (IdP) may require the verification of a service provider's request signing certificate. When you integrate a SAML IdP with Secure Access, you may have to import the Secure Access certificate information in to your IdP platform.

> **Note**
>
> Many IdPs do not validate SAML request signatures and therefore these steps are not required. We recommend that you contact your IdP for confirmation.

There are two options for importing the certificate information into your IdP: Automatic Configuration and Manual Import.

Known Limitations

If you have multiple Secure Access organizations and use the Secure Access multiple-Org SAML EntityID, then you must not use the URL-based metadata update mechanism. The Multiple-Org SAML Entity ID only applies if you have multiple Secure Access organizations linked to the same IdP. In this scenario you should manually add the Secure Access request signing certificate to each IdP configuration.

Automatic Configuration Through the Fixed Metadata URL

This option is the preferred configuration method for IdPs that support automatic updates of metadata through an URL. This includes popular IdPs such as AD FS and Ping Identity. The benefit is that the IdP automatically imports a new Secure Access certificate each year without manual intervention.

Prerequisites:

- An IdP that supports automatic updates of a service provider's metadata from a URL, for example: AD FS and Ping Identity.
- Configure your IdP platform to read one of the Secure Access metadata URLs for encrypted or unencrypted SAML assertions:

  Encrypted:

  ```
  https://api.sse.cisco.com/admin/v2/samlsp/certificates/Cisco_SSE_SP_Metadata_with_Encryption.xml
  ```

  Unencrypted:

  ```
  https://api.sse.cisco.com/admin/v2/samlsp/certificates/Cisco_SSE_SP_Metadata.xml
  ```

- Your IdP platform can read the associated Certificate Authority URLs:

  ```
  http://r3.o.lencr.org
  ```

  ```
  http://r3.i.lencr.org
  ```

- Your IdP platform must support TLS 1.2 in order to connect to the Secure Access metadata URL securely. If the IdP application utilizes .NET framework 4.6.1 or earlier this may require some further configuration. See Microsoft's documentation.
- For information on prerequisites that apply to all SAML IdPs, see Prerequisites for SAML Authentication.

Manual Import of the Secure Access SAML Certificate

Renew Identity Provider Certificates

Navigate to **Connect > Users, Groups, and Endpoint Devices > Configuration Management > SSO authentication >** select your **IdP > Edit > SAML Configuration >** click **Please upload the XML Configuration file from here**. For more information, see Edit an SSO Authentication Profile.

Renew Service Provider Certificates

Navigate to **Secure > Certificates > SAML integration > Service Provider certificates** > click **Download** next to any expiring or expired service provider certificate and add it to your IdP to activate.

Test SAML Identity Provider Integration

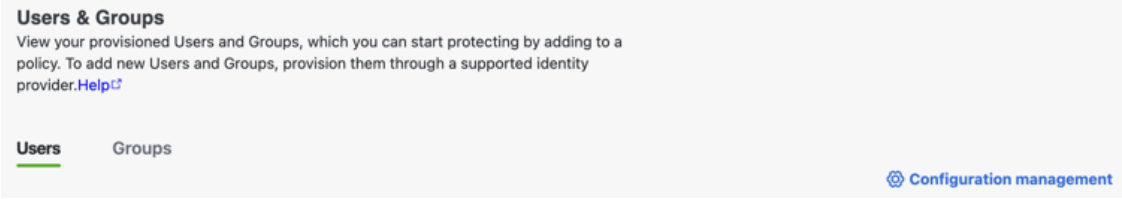
Provides instructions for completing the Test SAML Identity Provider Integration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

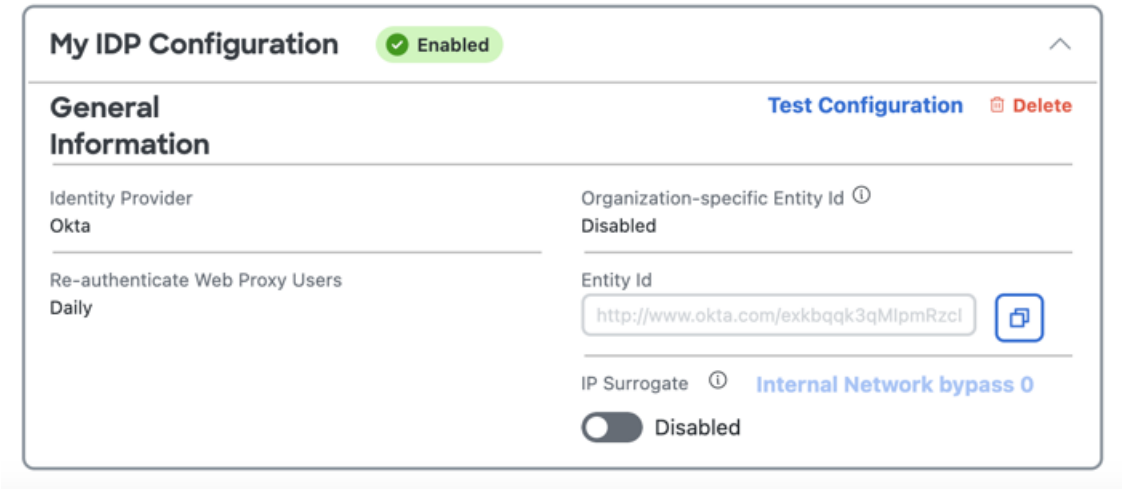
Procedure

1. Navigate to **Connect > Users and Groups** and click **Configuration management**.



2. Navigate to **SSO authentication**.
3. Click **Test Configuration** to confirm that a user in Secure Access can authenticate with the integrated IdP.

   Secure Access redirects you to sign in to your identity provider.



26 Access Policies

Topics:

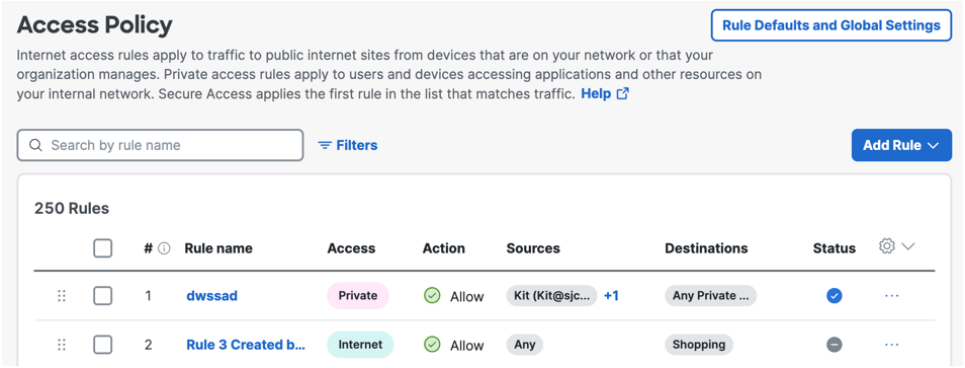
- Manage the Access Policy
- Manage Global Settings for Access Rules
- Rule Defaults: Default Settings for Access Rules
- Edit Rule Defaults and Global Settings
- Using Wildcard Masks on Access Rules
- View Related Activity for an Access Policy Rule
- View Related Events for an Access Policy Rule

Provides an overview of Access Policies in Cisco Secure Access, including Manage the Access Policy, Manage Global Settings for Access Rules, and Rule Defaults: Default Settings for Access Rules. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage the Access Policy

Describes Manage the Access Policy in Cisco Secure Access. Secure Access has a single Access policy, which consists of policy rules and settings.

Secure Access has a single Access policy, which consists of policy rules and settings. Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization. Before you start adding rules to your policy, we recommend that you read through the topics in this section in full.



Private and internet access rules

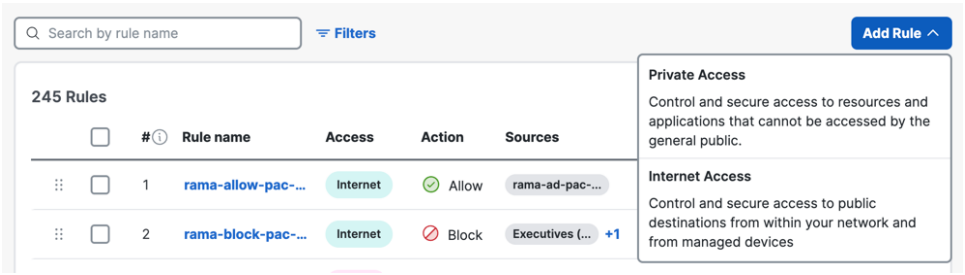
There are two types of access rules:

- **Private access rules**–Controls access to applications hosted from your data center and private clouds.

  To create and work with these rules, refer to Get Started With Private Access Rules.

- **Internet access rules**–Controls access to resources on the internet from managed devices.

  To create and work with these rules, refer to Get Started with Internet Access Rules.



Rule defaults and global settings

- Global settings apply to all rules (internet or private access or both) and cannot be changed for individual rules. For more information, see Global Settings for Access Rules.
- Rule defaults are settings that apply by default to new rules. You can change the settings for each rule. For more information, refer to Rule Defaults: Default Settings for Access Rules.

Default access rules

If your traffic does not match any of the rules in your policy, Secure Access applies the settings on the Default Access rules. For more information, refer to Default Access Rules in Your Policy.

About the Access Policy

Describes About the Access Policy in Cisco Secure Access. The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings.

The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings. The policy displays your configured rule data and allows you to choose how to prioritize the rules in your policy. Once you add a rule, you can edit various components on the rule. You decide how to view and manage your rules that best meets your organization's access controls to resources.

Best Practices

When working with access rules, keep the following in mind:

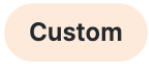
- You can change the rule defaults and global settings. For more information, see Rule Defaults: Default Settings for Access Rules, Global Settings for Access Rules, and Edit Rule Defaults and Global Settings.
- At the top of each rule is a summary section. After you add your rule, the summary displays the configured rule components.
- If you edit an access rule after saving it, you cannot change the rule action. Instead, create a new rule.
- For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. To understand how to optimize the location of a domain controller, see this documentation.

> **Warning**
>
> If you attach an empty private resource group to a policy, the entire rule containing the empty private resource is dropped.

- In each rule, features where you can configure a default option show one of the following indicators:
  - **Rule Defaults**–If you see this icon beside a control, it means the selected option or value is the selection configured on the rule default page.

  - **Custom**–If you see this icon beside a control, it means the selected option or value is different from the selection configured on the rule default page.

Control Options on an Access Rule

Provides instructions for completing the Control Options on an Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Secure Access, the Access policy contains the organization's configured access rules and the details about the Default Access Rules. From each access rule in the rules table, you can show the menu of rule controls and choose how to manage an access rule.

Before you begin

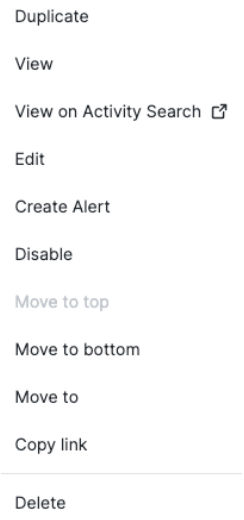
- Full Admin user rule. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy** and then navigate to an access rule in the rules table.



2. At the end of the row, click the **...** (ellipsis) to open the menu.
3. In the drop-down menu, choose one of the controls to manage the access rule or monitor the traffic enforced by the access rule.



- **Duplicate**–Make a copy of the access rule and add the new rule in the Access policy.
- **View**–View the details for the access rule.
- **View on Activity Search**–View the events in the Activity Search report for the traffic where Secure Access enforced the access rule.
- **Edit**–Edit the access rule.
- **Create Alert**–Configure an alert rule for monitoring the changes to the access rule.
- **Disable**–Disable the access rule in the Access policy.
- **Move to top**–Move the access rule before the first rule in the Access policy.
- **Move to bottom**–Move the access rule after the last rule in the Access policy.
- **Copy link**–Copy the link to the access rule.
- **Delete**–Duplicate the access rule.

Rule Data

Describes Rule Data in Cisco Secure Access. The Secure Access policy displays various columns of data on your configured internet and private access rules.

The Secure Access policy displays various columns of data on your configured internet and private access rules. For information about choosing additional data on your rules, see Show Additional Data on Your Access Rules.

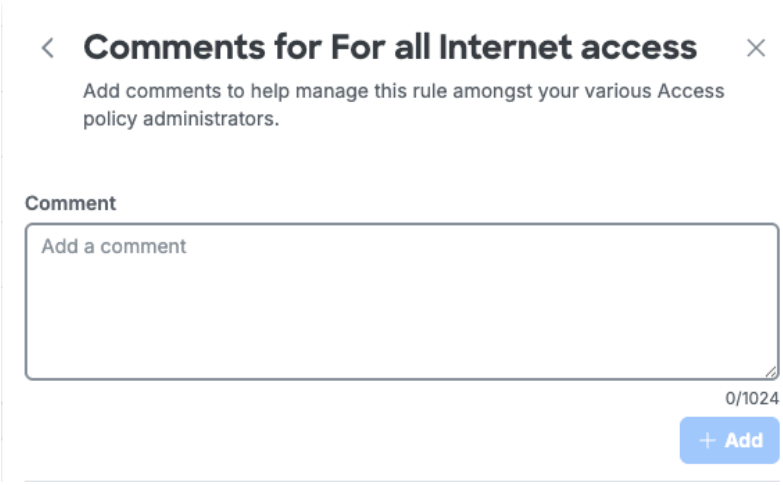


- **#**–The pound sign (hash symbol) indicates the priority of the rule.
- **Rule name**–The unique name that you assigned to the rule. A rule name may contain a sequence of 2-50 alphanumeric, hyphen, underscore, and space characters.
- **Access**–The type of access rule either **Internet** or **Private**.
- **Action**–The type of action on the rule.
  - For internet access rules: **Allow**, **Block**, **Isolate**, or **Warn**.
  - For private access rules: **Allow** or **Block**.
- **Sources**–The sources that can connect to the destinations.
- **Destinations**–The resources that are available on the organization and from the internet.
- **Security**–The security controls applied to the rule.

  Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Security profiles, and Tenant profiles. Hover over the security icon to display the profile information for the rule.
  - **IPS Profile**. For more information, see Manage IPS Profiles.
  - **Security Profile**. For more information, see Manage Security Profiles.
  - **Tenant Profile**. For more information, see Manage Tenant Control Profiles.
- **Hits**–The number of times in the last seven days that Secure Access applied the access rule to the traffic defined by the sources and destinations.
- **Status**–The state of the rule. Indicates whether the rule is enabled or disabled.

Status of Rule	Status Icon
Enabled	
Disabled	

- **Comments**: The notes added to a rule. Click the **...** icon to view or add comments. You can add comments to access policy rules to provide context, track changes, or share notes with other administrators.



Note

The Comments column is hidden. To view, click the settings gear icon and check the Comments column. This column also displays the selected rule's comment count.

Note

Comments are limited to 1024 characters and are sorted in reverse chronological order (most recent comment on top).

Each comment displays its author's name and time stamp.

- Add a comment:
  - Rules page: Locate the rule and click the comment icon to add a note.
  - Edit rule: Click the edit icon for a rule and add a comment in the rule details page.
  - Rule details: Click the rule name to open the rule details page, scroll to the comments section, and add your note.
- View a comment:
  - Click the table settings icon.
  - Select the Comments column and click Apply.
  - Click the comment icon in the row to view the comments page for that rule.
- Edit or delete a comment: Navigate to the rule details page or the comments page, locate your comment, and select the appropriate action. An edited comment has a label "Edited".

> **Note**
>
> Only the author of a comment can edit or delete it. When a rule is deleted, all comments associated with that rule are permanently removed.

Audit logs

All actions related to comments, including adding, editing, and deleting, are captured in the admin audit logs. You can view these events in the audit log to track administrative changes to your organization policy. For more information, refer to Admin Audit Log Report.

Show Additional Data on Your Access Rules

Provides instructions for completing the Show Additional Data on Your Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Cisco Secure Access policy table lists the configured properties, security controls, logging, and status information for your internet and private access rules. The table shows a default set of columns on the table. You can customize your view of the policy table. For more information about the default rule data, see Rule Data.

To customize the policy table, you can change the height of the table rows, add more columns of rule data, and remove the **Security** and **Hits** columns.

Customize the row height on the policy table, select additional data to display about your access rules, and remove data columns on your policy table view.



Before you begin

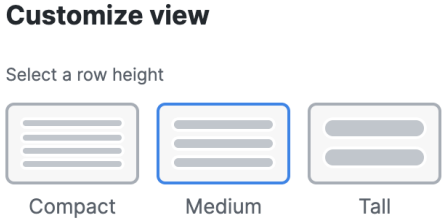
- Full Admin user role. For more information, see Manage Accounts.
- Your policy has at least one configured access rule.

Procedure

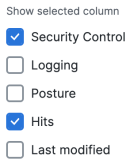
1. Navigate to **Secure** > **Access Policy**, and then click **Customize view**.

2. (Optional) For **Select a row height**, choose the height of the rows in the policy table.
   Select either **Compact**, **Medium**, or **Tall**. The default table row height is **Medium**.

3. For **Show selected columns**, add the names of the data columns to display on your policy table and remove the **Security Control** or **Hits** columns.



- **Security**–The security controls applied to the rule.



Security controls are the globally-configured profiles that are enabled on the rule: Intrusion Prevention (IPS), Security profiles, and Tenant profiles. Hover over the security icon to display the profile information for the rule.

  - **IPS Profile**. For more information, see Manage IPS Profiles.
  - **Security Profile**. For more information, see Manage Security Profiles.
  - **Tenant Profile**. For more information, see Manage Tenant Control Profiles.

- **Logging**–Indicates whether logging is enabled for the organization.
- **Posture**–The name of the endpoint posture profile that is defined on the rule.
- **Hits**–The number of times in the last seven days that Secure Access applied the access rule to the traffic defined by the sources and destinations. For more information, see Edit the Order of the Rules in Your Access Policy.
- **Last Modified**–The date of the modification of the access rule by the user account.

> **Note**
>
> Hover over the date to display the ID of the user account that last modified the rule.



4. Click **Reset defaults** to show the policy table with the default rule data view or click anywhere on the page outside of the **Customize View** component to enable your selections and close the window.



Edit the Order of the Rules in Your Access Policy

Describes Edit the Order of the Rules in Your Access Policy in Cisco Secure Access. The order of the rules listed on the Policy page is critical to traffic handling.

The order of the rules listed on the Policy page is critical to traffic handling.

Traffic is handled by the first rule in the list that matches the traffic. Rules lower in the list have no effect on traffic that matches a rule higher in the list.

Order your rules so that more specific rules are above more general rules that might also apply to the traffic.

Put essential rules at the top, such as rules blocking access for all users to sites that you absolutely do not want any users to visit.

If no rule in the list matches the traffic, Secure Access applies the applicable default access rule for the type of traffic (internet access or private access.) Default access rules (one for each type) appear at the bottom of the Policy page.

Important

For rule matching of encrypted internet traffic, see Ensure Rule Matching for Encrypted Internet Traffic.

An error in configuration may result in unintended results:

Resources may be unprotected from threats or users may access destinations you want blocked. Plan and design your rules before you build them.

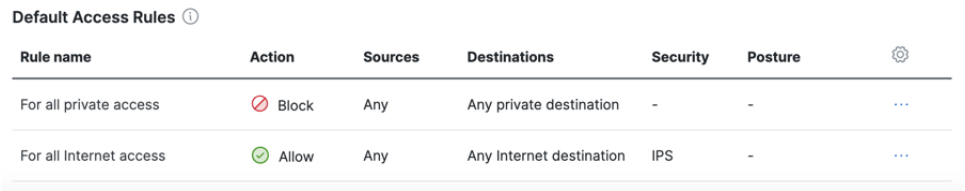
Ways to reorder rules:

- On the Access Policy page, right-click a rule and choose one of the following options:
  - **Move to top** of the list
  - **Move to bottom** of the list
  - **Move to** and then choose an order
- While editing a rule, click the **Rule Order** field and click the rule you want to be immediately before the rule you are moving.

Default Access Rules in Your Policy

Describes Default Access Rules in Your Policy in Cisco Secure Access. If your traffic does not match any of the rules in your policy, Secure Access applies the settings in the Default Access rules.

If your traffic does not match any of the rules in your policy, Secure Access applies the settings in the Default Access rules. For more information, see View or Edit Default Access Rules.



Default Internet Access Rule

- Secure Access applies this rule to traffic to internet destinations that does not match any other internet access rule in the policy.
- The default internet access rule **allows** traffic that hits it. You cannot change the rule action.
- You can edit the logging settings.
- You can edit the security control settings.
- Posture is not applicable for internet access rules.

Default Private Access Rule

- Secure Access applies this rule to traffic to private destinations that does not match any other private access rule in the policy.
- The default private access rule **blocks** traffic that hits it. You cannot change the rule action.
- You cannot edit the logging settings.
- Because the action for this rule is Block, the security control settings are not needed or offered.
- Posture is not applicable for the default access rule. Secure Access blocks the traffic whether or not the posture requirements are met.

View or Edit Default Access Rules

Provides instructions for completing the View or Edit Default Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access has a default internet access rule and a default private access rule. The default access rules apply to traffic that does not match any other rule in the Access policy.

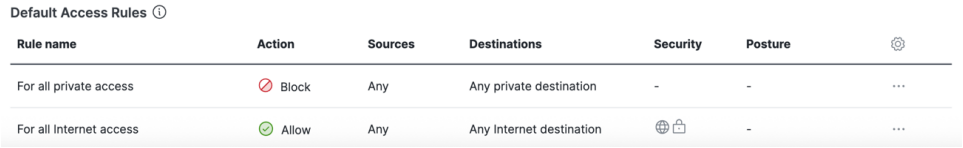
You can view the settings for a default private access rule. You can view and edit the settings on a default internet access rule.

Before you begin

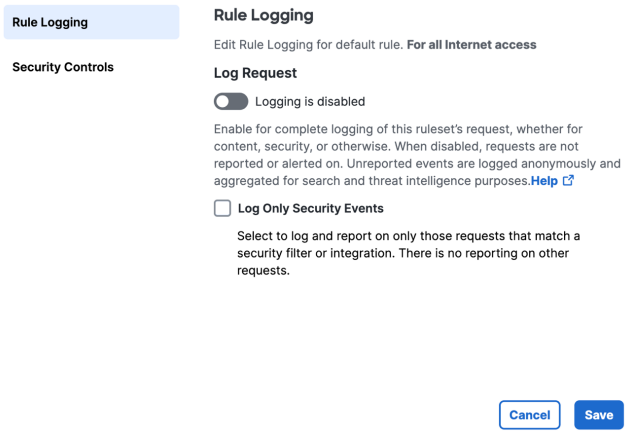
- Full Admin user rule. For more information, see Manage Accounts.

Procedure

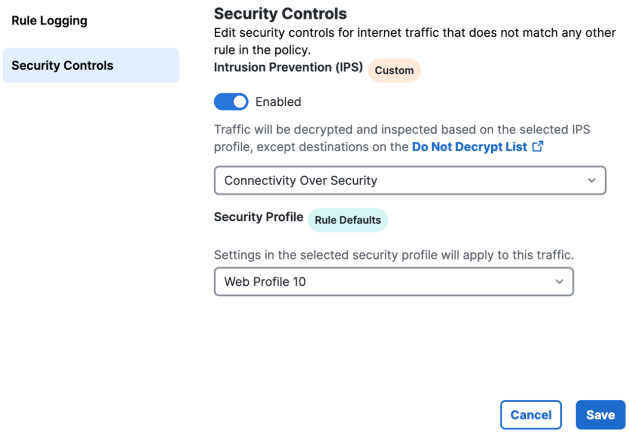
1. Navigate to **Secure** > **Access Policy**.
2. Navigate **Default Access Rules** located at the bottom of the Access policy page.



3. Navigate to **For all private access** and click the ellipsis (**...**) at the end of the row to open the menu.
   a) Choose **View** to display the logging and security controls on the default private access rule.
4. Navigate to **For all internet access** and click the ellipsis (**...**) at the end of the row to open the menu.
   a) Choose **View** to display the logging and security controls on the internet access rule.
   b) Choose **Edit** to modify the logging and security controls on the default internet access rule.
   c) For **Rule Logging**, enable or disable the settings and then click **Save**.



d) For **Security Controls**, enable or disable the security control settings, select an IPS profile, select a Security profile, and then click **Save**.



Manage Global Settings for Access Rules

Describes Manage Global Settings for Access Rules in Cisco Secure Access. Not all of the features described here are available to all Secure Access packages.

> **Note**
>
> **Secure Access Packages and Feature Availability**
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the **Admin > Licensing** page. For more information, see Determine Your Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. See also, Cisco Secure Access Packages

The Global Settings configuration in the Access policy affects all rules of the applicable type: internet access rules or private access rules.

Some global settings are intended only for troubleshooting purposes. Change these settings only if you have good reason to do so. For more information, Edit Rule Defaults and Global Settings.

You can edit these Global Settings in your Access policy:

- Display User Input Field on Warn Pages
- Microsoft 365 Compatibility
- Decryption
- Disable Decryption for Specific sources
- Client Resolved Domain Destination List
- Disable Decryption for Specific Sources
- Decryption Logging
- Certificate Pinning

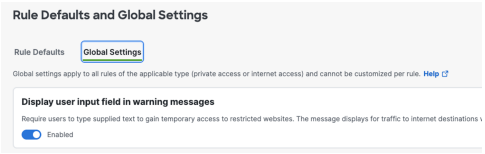
To configure the global settings for the Access policy, navigate to **Secure** > **Access Policy** > **Rule Defaults and Global Settings** in Secure Access.

Display User Input Field on Warn Pages

Describes Display User Input Field on Warn Pages in Cisco Secure Access. This setting applies only for destinations on internet access rules in the Access policy that have enabled the Warn action.

This setting applies only for destinations on internet access rules in the Access policy that have enabled the **Warn** action.

- Click to enable the display of the user input field on all Warn pages for internet access rules.



Once enabled, all Warn pages that are displayed by Secure Access have the user input field instead of the link to continue to the warning message.

> **Note**
>
> The **Display user input field in warning messages** option does not affect the use of the organization's custom Warn pages.

About the Warn Page User Input Field

When Secure Access displays a **Warn** page with the user input field, the end-user must enter the word **Continue** to reach the destination. If the user's language is not supported, then use **Continue**.

The value of the user input field is a case-insensitive string.

Once the user enters **Continue**, Secure Access enables the **Continue** button on the Warn page. The user then clicks the **Continue** button to reach the destination. For more information, see Manage Notification Pages.

Microsoft 365 Compatibility

Describes Microsoft 365 Compatibility in Cisco Secure Access. This setting applies only to web security features, not to Intrusion Prevention System (IPS).

This setting applies only to web security features, not to Intrusion Prevention System (IPS).

The Microsoft 365 Compatibility feature exempts Microsoft 365-related domains, marked as **Optimize** and **Allow** in Microsoft's endpoint categories,to bypass inspection and policy enforcement by web security features, allowing traffic to those domains to pass through unaltered. The domains are excluded from HTTPS decryption and content filtering. The Microsoft 365 traffic appears in the Secure Access reports, however, since HTTPS inspection is disabled, traffic is logged only at the host/domain level and does not show the full URL.

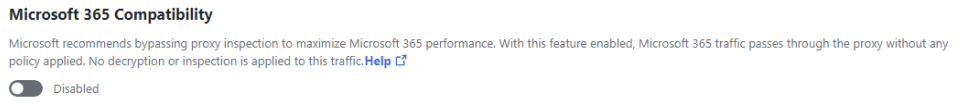
Tenant Controls

If you use tenant controls for Microsoft 365, see additional information at Use Tenant Controls in Access Rules.

Limitations

- Microsoft 365 traffic is still sent to Secure Access's web proxy service in all deployment methods (Tunnel, AnyConnect, PAC). To stop this traffic from hitting Secure Access entirely, add manual 'External Domain' entries or route the traffic direct to the internet from your connecting devices.
- File Inspection will no longer apply to this traffic.
- This will not prevent the Microsoft 365 traffic egressing from a Secure Access IP address.
- This does not apply to all Microsoft/Microsoft 365 domains. Only those categorized as important for performance by Microsoft.
- This setting allows a number of important Microsoft 365 domains so web security and filtering do not apply to them, and prevents these domains from triggering Secure Access SAML authentication.

> **Note**
>
> MS Intune sync requires "manage.microsoft.com" to be added to the Do Not Decrypt List(s) used in the relevant rules even when Microsoft365 Compatibility is enabled. For more information, see the official Microsoft documentation.



Decryption

Describes Decryption in Cisco Secure Access. Secure Access recommends the decryption of traffic for effective security control, but you can temporarily disable decryption for troubleshooting purposes.

Secure Access recommends the decryption of traffic for effective security control, but you can temporarily disable decryption for troubleshooting purposes.

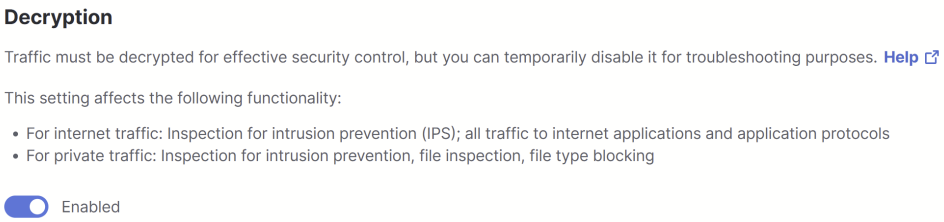
The **Decryption** Global Setting in the Access policy applies to internet destinations and private resources.

The **Decryption** setting is used to disable or enable the firewall-based Secure Access Intrusion Prevention System (IPS) and does not affect the Secure Access Secure Web Gateway (SWG) and the inspection of the body of the web messages.

For internet destinations, enable the **Decryption** setting to inspect the initial phase of the message handshake for all traffic to internet applications and application-layer protocols.

For private destinations, enable the **Decryption** setting to inspect the initial phase of the message handshake for all traffic to private resources, and perform file inspection and file type blocking.

Disabling decryption does not disable the affected features, but decreases their effectiveness for encrypted traffic. Traffic that is not encrypted is not affected.



For information about other decryption settings, see Manage Traffic Decryption.

Configure Decryption for Specific Sources

Use this procedure to add source IP addresses or Classless Inter-Domain Routing (CIDR) blocks in Cisco Secure Access and exclude their internet traffic from decryption.

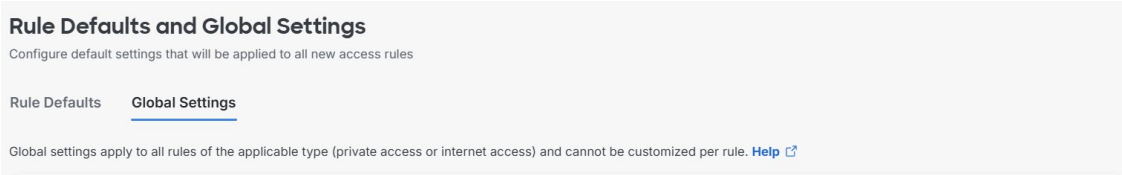
To exclude specific internet traffic from decryption, add source IP addresses or Classless Inter-Domain Routing (CIDR) blocks. This setting applies to internet access rules.

Before you begin

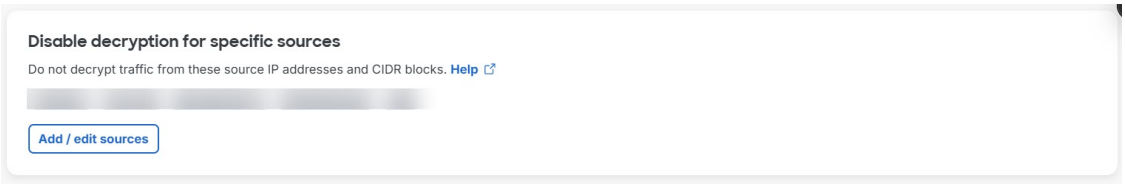
You must have Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Click **Rule Defaults and Global Settings**, and then select the **Global Settings** tab .



2. Under **Disable decryption for specific sources**, click **Add/edit sources**.



3. In the **Disable decryption for specific sources** panel, enter the source IP addresses or CIDR blocks in the **Add sources** field.



4. Click **+ Add**.

   The source count updates and the added sources appear in the list.



5. (Optional) In the **Search sources** field, enter an IP address or CIDR block to filter the list.
6. (Optional) To modify an existing entry, click the **Edit** (pencil) icon next to the source.



7. (Optional) To remove a source, click the **Delete** (trash can) icon next to the source.

Client Resolved Domain Destination List

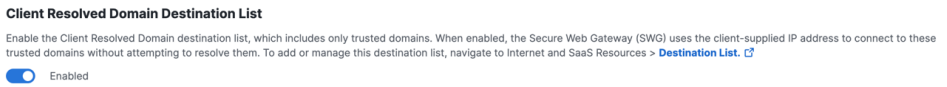
In Secure Access, enable the Client Resolved Domain Destination List global setting in the Access policy.

The Client Resolved Domain Destination List global setting provides the Client Resolved Domain destination list in the organization. Administrators can add trusted domains in the Client Resolved Domain destination list, which affects how Secure Access manages the connections to internet destinations on the trusted domains. For more information, see About Client Resolved Domain Destination List.

The Client Resolved Domain Destination List global setting ensures that the Secure Web Gateway (SWG) does not perform DNS lookups to resolve IP addresses on trusted domains. When end users in the organization send a web request over TCP/80 or TCP/443 for a domain in the Client Resolved Domain destination list, the SWG uses the IP address for the domain resolved by the client to connect to the destination.

Enable the Client Resolved Domain Destination List

In Global Settings on the Access policy, enable the **Client Resolved Domain Destination List** setting.



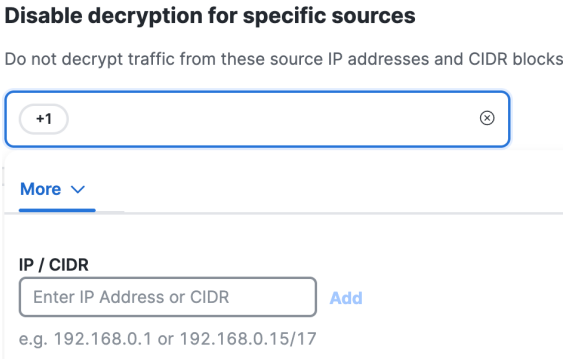
Disable Decryption for Specific Sources

Describes Disable Decryption for Specific Sources in Cisco Secure Access. The Disable Decryption for Specific Sources Global Setting in the Access policy disables the decryption of internet traffic for the configured sources.

The **Disable Decryption for Specific Sources** Global Setting in the Access policy disables the decryption of internet traffic for the configured sources. This setting applies to sources on internet access rules only. The sources may be endpoints or other devices where you cannot install certificates, such as Internet of Things (IOT) devices.

The organization can use the **Disable Decryption for Specific Sources** setting to disable or enable the firewall-based Secure Access Intrusion Prevention System (IPS) for specific sources. This setting does not affect the Secure Access Secure Web Gateway (SWG) and the inspection of the body of the web messages.

To disable decryption on internet traffic from the sources, add IP addresses or CIDR blocks as sources in the **Disable Decryption for Specific Sources** setting. For information about other decryption settings, see Manage Traffic Decryption.



Decryption Logging

Describes Decryption Logging in Cisco Secure Access. You can enable or disable decryption logging globally in Global Settings, for traffic to private resources or internet destinations or both.

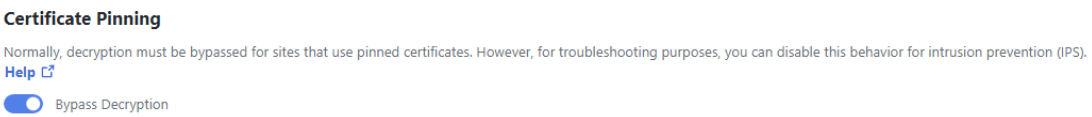
You can enable or disable decryption logging globally in Global Settings, for traffic to private resources or internet destinations or both.

Certificate Pinning

Describes Certificate Pinning in Cisco Secure Access. Certificate pinning is an Internet security mechanism which allows applications to resist impersonation against HTTPS servers using mis-issued or otherwise fraudulent digital certificates.

Certificate pinning is an Internet security mechanism which allows applications to resist impersonation against HTTPS servers using mis-issued or otherwise fraudulent digital certificates. However, if this security feature causes problems when users attempt to access destinations that are both essential and trusted, you may bypass this security feature for destinations that use certificate pinning.

> **Note**
>
> Normally, decryption must be bypassed for sites that use pinned certificates. However, for troubleshooting purposes, you can disable this behavior for intrusion prevention (IPS).



Rule Defaults: Default Settings for Access Rules

Describes Rule Defaults: Default Settings for Access Rules in Cisco Secure Access. When you create a new access rule, Secure Access configures the rule with the default rule settings unless you select other options in the rule.

When you create a new access rule, Secure Access configures the rule with the default rule settings unless you select other options in the rule. The rule defaults are a collection of controls for endpoint security posture and security profiles, and the zero trust authentication interval property.

You can modify the default rule settings. For more information, see Edit Rule Defaults and Global Settings.

> **Note**
>
> **Important Information About Changing Rule Defaults**
>
> If you modify a rule default, all existing rules that are configured to use a particular rule default will change to use the new default.
>
> For example, if you change the default IPS Profile from **Balanced Security and Connectivity** to **Maximum Security**, the IPS profile in all existing rules that are configured to use the default IPS Profile will now use the **Maximum Security** settings for IPS.
>
> Existing rules that are configured to use custom settings are not affected by changing the rule default. To determine whether a rule uses default or custom settings, see About the Access Policy.

Zero Trust Access: Endpoint Posture Profiles

Describes Zero Trust Access: Endpoint Posture Profiles in Cisco Secure Access. Client-based and browser-based Zero Trust Access (ZTA) profiles specify end-user device requirements when connecting to private and internet resources using ZTA.

Client-based and browser-based Zero Trust Access (ZTA) profiles specify end-user device requirements when connecting to private and internet resources using ZTA.

Choose from these types of Private Access posture profiles:

- **Client-based**–Select as the default profile for devices where the Cisco Secure Client is installed.
- **Browser-based**–Select as the default profile for devices where the Cisco Secure Client **is not** installed.

For Internet Access, which designates the default requirements for client-based ZTA connections to internet destinations, select a client-based posture profile from the drop-down menu.

> **Note**
>
> Internet Access posture profiles are applied at the global level, not at the rule level.

For more information about Zero Trust posture profiles, see Manage Zero Trust Access Posture Profiles.

Zero Trust Access: User Authentication Interval

Describes Zero Trust Access: User Authentication Interval in Cisco Secure Access. The Zero Trust Access User Authentication Interval is sometimes known as step-up authentication.

The Zero Trust Access User Authentication Interval is sometimes known as step-up authentication.

For the ZTA user authentication interval, specify the default frequency with which end users must verify their identity, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network.

Note: iOS clients do not support the User Authentication Interval option. The User Authentication Interval must be disabled in access rules that apply to iOS devices.

User Authentication Default Interval Settings

Describes User Authentication Default Interval Settings in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- The default interval is 3 days.
- The minimum value is 1 minute.

For more information, see Network Authentication for Zero Trust Access.

Configure Access Rule Editing Sessions

Use this procedure to specify the duration that an administrator can lock and edit an access rule. You can also allow a single session extension of up to 40 minutes.

Use the editing-session settings to control how long an administrator can lock and edit an access rule, and to determine whether they can extend the active session.

Before you begin

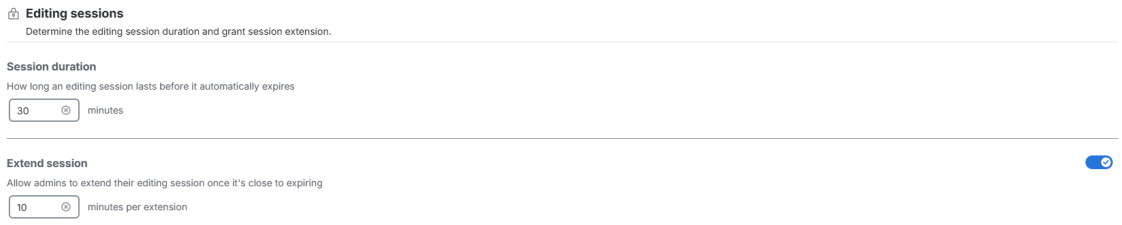
You must have the Full Admin user role to configure rule defaults and global settings. For more information, see Manage Accounts.

Procedure

1. In the global settings panel, locate the **Editing sessions**.
2. In the **Session duration** section, enter the number of minutes that an access rule remains locked for an editing session before it expires.
3. To allow administrators to extend a session, enable the **Extend session** toggle button, and then enter the number of minutes to add under **minutes added per extension**.

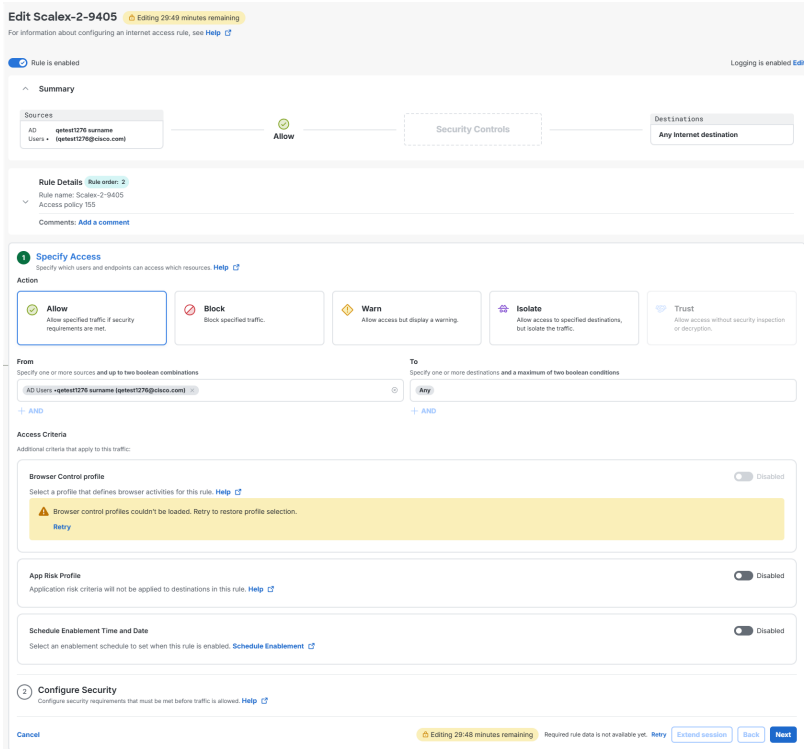
> **Note**
>
> You can extend an editing session only once. The maximum extension duration is 40 minutes.

4. Click **Save**.

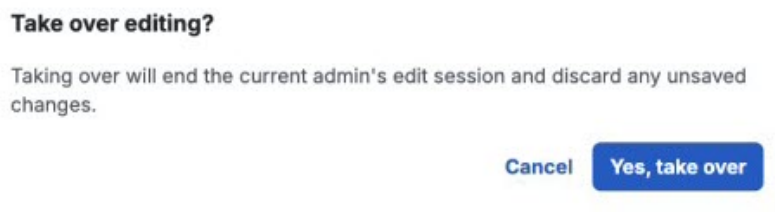


5. While editing a rule, the **Internet Access Rule** and **Private Access Rule** page both shows the remaining time at the top and bottom. Click **Extend session** before the time expires to extend the session. If another admin opens

the rule during an active session, Secure Access displays a dashboard notification and opens the rule in preview mode.



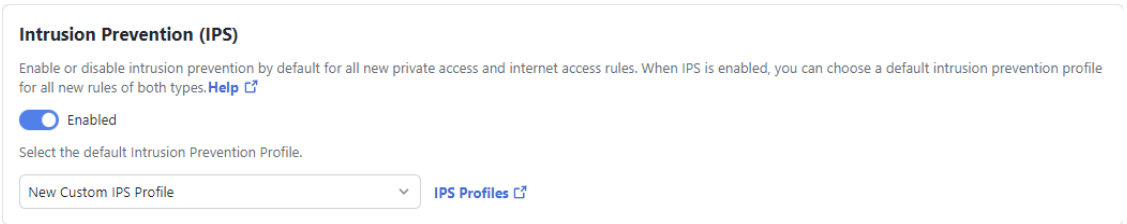
6. To take over editing, click **Take Over Editing**, and then click **Yes, take over**. This action ends the current administrator's session and discards any unsaved changes.



Intrusion Prevention (IPS)

Describes Intrusion Prevention (IPS) in Cisco Secure Access. Enable or disable intrusion prevention by default for all new private access and internet access rules.

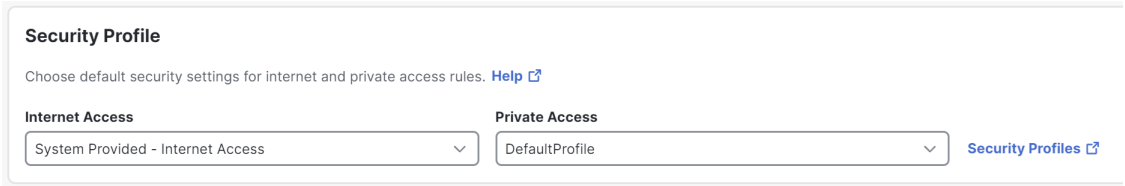
Enable or disable intrusion prevention by default for all new private access and internet access rules. When IPS is enabled, you can choose a default intrusion prevention profile for all new rules of both types. For more information about IPS profiles, see Manage IPS Profiles.



Security Profile

Describes Security Profile in Cisco Secure Access. A security profile lets you configure settings that you can use in a rule as a set.

A security profile lets you configure settings that you can use in a rule as a set. Choose a profile to apply to all new access rules of each type (internet and private access). For more information about Security profiles, see Manage Security Profiles.



Isolation Profile

Describes Isolation Profile in Cisco Secure Access. Isolation profiles allow you to define granular security controls for web traffic that is redirected to an isolated browser.

Isolation profiles allow you to define granular security controls for web traffic that is redirected to an isolated browser. This setting applies only to internet access rules. For more information about Isolation Profiles, see Manage Remote Browser Isolation Profiles.

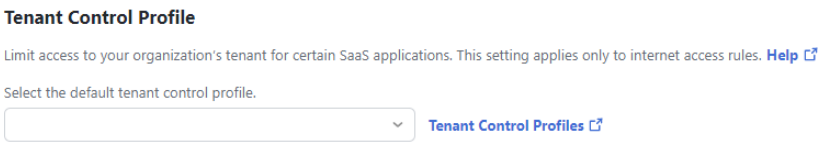


Select the default isolation profile from the drop-down list.

Tenant Control Profile

Describes Tenant Control Profile in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Limit access to your organization's tenant for certain SaaS applications. This setting applies only to internet access rules. For more information about tenant control profiles, see Manage Tenant Control Profiles.



Edit Rule Defaults and Global Settings

Provides instructions for completing the Edit Rule Defaults and Global Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Important

Before you change the default rule settings on the Cisco Secure Access policy, see Important Information About Changing Rule Defaults.

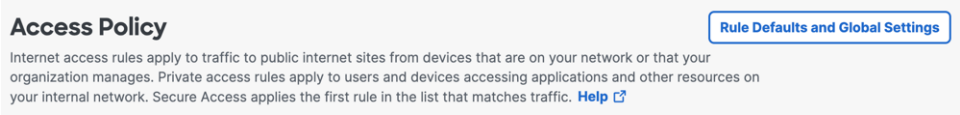
Secure Access is pre-configured with default and global settings for access rules. We recommend that you change the default rule settings. You may need to change the global policy settings.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure > Access Policy**.
2. Click **Rule Defaults and Global Settings**.



3. Click the tab to edit **Rule Defaults** or **Global Settings**.
   For details about each setting, see:
   - Rule Defaults: Default Settings for Access Rules
   - Manage Global Settings for Access Rules
4. Scroll to the bottom of the page, and then click **Save**.

Using Wildcard Masks on Access Rules

Describes Using Wildcard Masks on Access Rules in Cisco Secure Access. The Cisco Secure Access policy is the collection of an organization's internet and private access rules.

The Cisco Secure Access policy is the collection of an organization's internet and private access rules. You can define composite source and destination components on Access rules. A composite source or destination may include multiple network address components.

For composite sources, add IPv4 addresses or CIDR blocks. You can also add a wildcard mask with an IPv4 address.

- For information about sources and internet access rules, see Sources.
- For information about sources and private access rules, see About Configuring Sources in Private Access Rules.

For composite destinations, add IP addresses, CIDR blocks, ports and port ranges, and transport protocols. You can also add a wildcard mask with an IP address.

- For information about destinations and internet access rules, see About Configuring Destinations in Internet Access Rules.
- For information about destinations and private access rules, see About Configuring Destinations in Private Access Rules.

Wildcard Masks in Composite Sources or Destinations

Describes Wildcard Masks in Composite Sources or Destinations in Cisco Secure Access. You can add a wildcard mask with an IPv4 address for a composite source or destination on an Access rule.

You can add a wildcard mask with an IPv4 address for a composite source or destination on an Access rule.

A wildcard mask represents the bits of an IP address and determines if certain parts of the network address are ignored or allowed. Secure Access applies the wildcard mask to the IP address to configure network addresses for the sources or destinations.

When a user device connects from a source or requests a destination, Secure Access verifies that the traffic on the network address connection or resource is supported by the composite component.

Guidelines

Describes Guidelines in Cisco Secure Access. You can add a 32-bit IPv4 address with a wildcard mask on an Access rule, for example: 192.168.0.1/0.0.255.0.

- You can add a 32-bit IPv4 address with a wildcard mask on an Access rule, for example: **192.168.0.1/0.0.255.0**.
- Secure Access accepts valid wildcard masks only.
- If the bit value on the position in the wildcard mask is zero (0), then the bit value on the position in the IP address must match.
- If the bit value on the position in the wildcard mask is one (1), then the bit value on the position in the IP address is ignored.
- Secure Access does not support a comma-separated list of wildcard masks in composite sources or destinations.
- Secure Access does not support composite sources or destinations that include a subnet mask with an IPv4 address.

Examples of Wildcard Masks

Describes Examples of Wildcard Masks in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Wildcard Mask	Bits in IPv4 Address	Description
0.0.0.63	00000000 00000000 00000000 00111111	Matches the first three octets. Matches the two leftmost bits of the last octet. Ignores the last six bits.
0.0.0.254	00000000 00000000 00000000 11111110	Matches the first three octets. Matches the rightmost bit of the last octet. Ignores the first seven bits.
0.0.0.255	00000000 00000000 00000000 11111111	Matches the first three octets. Ignores the last octet.

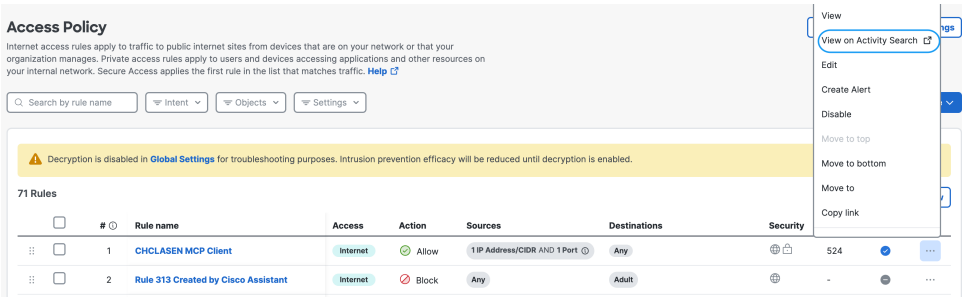
View Related Activity for an Access Policy Rule

Use this task to quickly access and review activities associated with a specific access policy rule for troubleshooting and validation

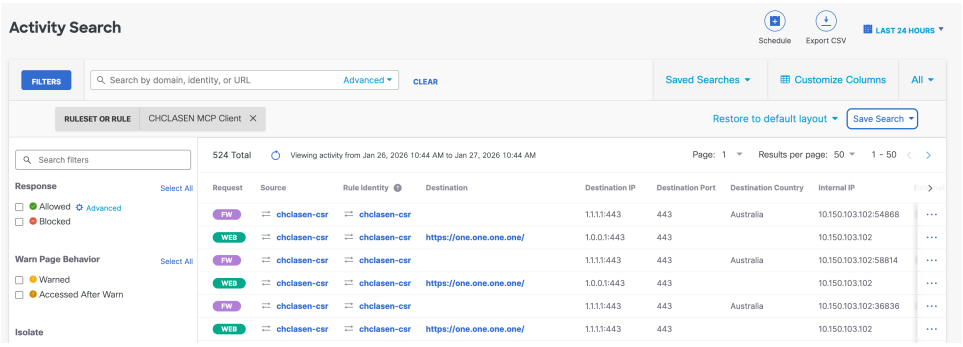
You can view all activities associated with a specific access policy rule directly from the Access Policy page. This feature enables efficient validation, troubleshooting, and analysis by letting you launch an Activity Search that is automatically filtered for the selected rule.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. From the list of access policy rules, click **More options** (three-dot) menu for the rule you want to investigate, and click **View on Activity Search**.



This opens the **Activity Search** page in a new browser tab, automatically filtered to display only activities related to the selected rule.



Alternatively, click the rule name to open the details panel, then select the **View on Activity Search** link to view the related activity.

3. In the **Activity Search** page, review the activity records associated with the rule and use additional search filters as needed to refine your results.

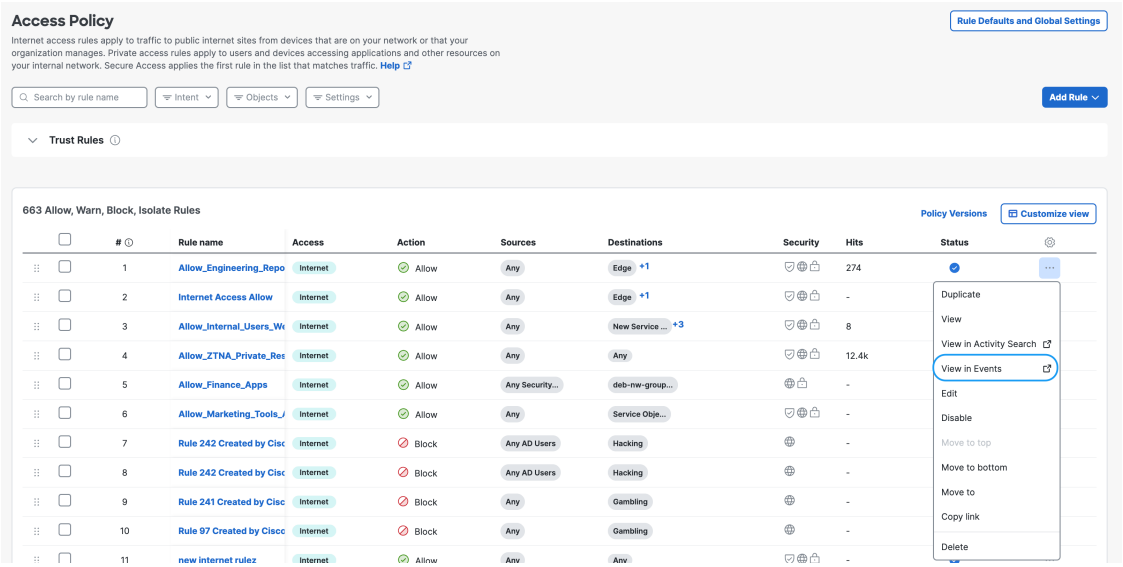
View Related Events for an Access Policy Rule

Use this task to quickly access and review events associated with a specific access policy rule for troubleshooting and validation

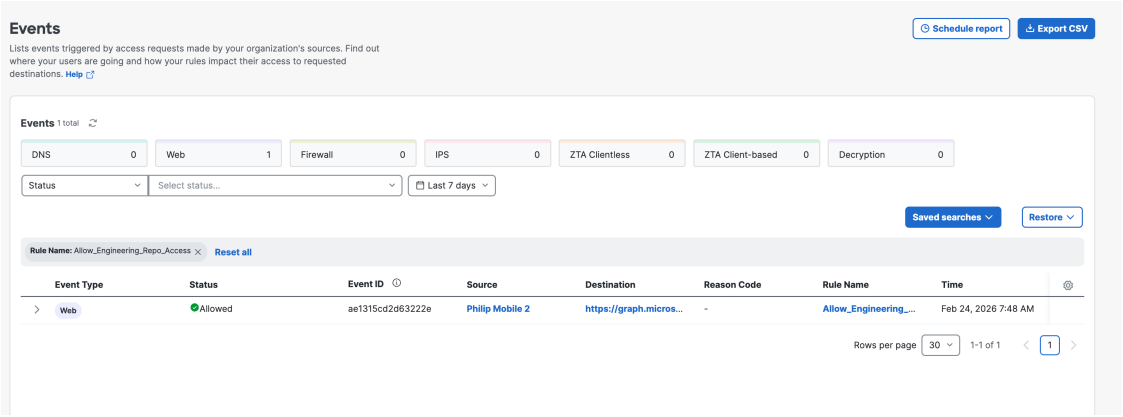
You can view all events associated with a specific access policy rule directly from the Access Policy page. This feature enables efficient validation, troubleshooting, and analysis by letting you launch an Events page that is automatically filtered for the selected rule.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. From the list of access policy rules, click **More options** (three-dot) menu for the rule you want to investigate, and click **View in Events**.



This opens the **Events** page in a new browser tab, automatically filtered to display only events related to the selected rule. When you navigate from the **Access Policy** page to the **Events** page, the default filter is set to the last 7 days.



Alternatively, click the rule name to open the details panel, then select the **View in Events** link to view the related events.

3. In the **Events** page, review the activity records associated with the rule and use additional search filters as needed to refine your results.

27 Internet Access Rules

Topics:

- Internet Access Rules
- Add an Internet Access Rule
- Geolocation Sources and Internet Access Rules
- Edit an Internet Access Rule
- About Isolated Destinations
- Troubleshoot Internet Access Rules

Provides an overview of Internet Access Rules in Cisco Secure Access, including Get Started With Internet Access Rules, Add an Internet Access Rule, and Geolocation Sources and Internet Rules. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Internet Access Rules

Describes Internet Access Rules in Cisco Secure Access. Internet access rules specify how traffic to internet destinations should be secured and handled.

Internet access rules specify how traffic to internet destinations should be secured and handled.

Traffic to internet destinations is allowed by default. You must create rules to block access to internet destinations either for acceptable use or security reasons, to warn users before you allow access, or to isolate specified internet traffic.

1. **Plan your internet access rules**

   Plan your rule set so you get the results you expect. Read the documentation and familiarize yourself with the various components that make up rules.

2. **Create rule components**

   Assemble rules largely from pre-configured source and destination components, and security control components. For more information, see Components for Internet Access Rules.

3. **Specify rule defaults**

   New rules will use the default security controls and other settings that you specify on the Rule Defaults page. For more information, see Default Settings for Internet Access Rules.

4. **Edit the default internet access rule**

   Traffic to internet destinations that does not match any other internet access rule in the policy will be handled. For more information, see View or Edit the Default Access Rules.

5. **Add internet access rules**

   For more information, see Add an Internet Access Rule.

6. **Review the global settings**

   Normally you will not change these settings for internet access rules, but you should be familiar with their impact. For more information, see Global Settings for Internet Access Rules.

7. **Ensure that rules match encrypted traffic**

   For more information, see Ensure Rule Matching for Encrypted Internet Traffic.

8. **Review the rule order**

   Make sure the order of the rules on the Access Policy will have the results you expect. For more information, see Edit the Order of the Rules on the Policy Page.

9. **Test your internet access rules**

Default Settings for Internet Access Rules

Describes Default Settings for Internet Access Rules in Cisco Secure Access. You can choose default settings that will automatically populate newly created internet access rules by default.

You can choose default settings that will automatically populate newly created internet access rules by default.

In Secure Access, navigate to the **Secure > Access Policy**, click **Global Settings and Rule Defaults** to configure the **Default Settings**.

For more information, see Rule Defaults and Edit Rule Defaults and Global Settings.

Important

Choose rule defaults carefully. Changing the Default Settings later may impact existing rules. For more information, see Important Information About Changing Rule Defaults.

Default Settings that apply to internet access rules:

- **Intrusion Prevention (IPS) Profile**–Specify the traffic-inspection behavior to use by default in new access rules. This setting applies to both private access rules and internet access rules. For more information about IPS profiles, see Manage IPS Profiles.
- **Security Profile**–Specify a default set of settings that control security and other interactions for end users accessing the internet. For more information about security profiles, see Manage Security Profiles.
- **Tenant Controls**–If your company uses Microsoft 365, Google G-Suite, Slack, or Dropbox, you must configure tenant controls. For more information about tenant controls, see Manage Tenant Control Profiles.

Global Settings for Internet Access Rules

Describes Global Settings for Internet Access Rules in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Global settings generally apply to all rules. However, some settings apply only to private access rules, not to internet access rules.

Do not change global settings unless you have a specific reason to do so.

If your company uses either of the following, verify that the applicable global settings are correct for your company:

- Microsoft 365 applications
- Applications that use pinned certificates

Decryption-related settings:

- **Decryption**–For troubleshooting purposes, you can temporarily disable decryption for the specified features, for all private and internet access rules.
- **Disable decryption for specific sources**–Use this setting to disable decryption from sources on which certificates cannot be installed, such as IOT "internet of things" devices, that need to connect to the internet.
- **Decryption Logging**–Choose whether to enable or disable logging of decryption events for internet access rules.

For more information about these settings, see Global Settings for Access Rules.

To change default rule settings, see Edit Rule Defaults and Global Settings.

Components for Internet Access Rules

Describes Components for Internet Access Rules in Cisco Secure Access. Cisco Secure Access supports configuring security controls for sources and destinations (resources) on internet access rules in the organization's Access policy.

Cisco Secure Access supports configuring security controls for sources and destinations (resources) on internet access rules in the organization's Access policy. You can create access rules by adding components that you or others have previously created or entering network information directly on a rule for sources and destinations. Pre-configured components described in this topic are reusable. You can use the same pre-configured components in multiple access rules.

Before you can add resources in Secure Access, deploy the resources in the organization's environments. Also configure resources for destinations in Secure Access: content categories, destination lists, and application lists. Once you register the resources in Secure Access, you can select these components on the internet access rules.

For example, you can define a set of users as a source, then use the same source in an internet access rule and in a private access rule for the same set of users. Some components are profiles, or groups of settings bundled together that you choose as a unit when configuring a rule.

Sources

Describes Sources in Cisco Secure Access and outlines About Selecting Sources on an Access Rule and Number of Sources Supported in a Rule. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Sources on internet rules are either pre-configured or composite components. Pre-configured source components such as Registered Networks and Network Tunnel Groups acquire and manage the web traffic in your organization. For information about pre-configured source components, see Reusable Sources in Internet Access Rules.

Composite sources may include IP addresses, CIDR blocks, and wildcard masks, and ports and port ranges. For information about composite source components, see Composite Sources in Internet Access Rules.

About Selecting Sources on an Access Rule

If you select Network Tunnel Groups, Secure Access secures and controls the traffic access from the IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and look at the group configuration.

If you select a Network Tunnel Group, the destination also includes IP addresses configured in the network tunnel group for routing, in addition to all associated Internal Networks. IP addresses include routes advertised using Border Gateway Protocol, if that option is selected in the network tunnel group configuration.

If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future.

Number of Sources Supported in a Rule

You can add up to 250 sources in an internet access rule. The total number of sources accepted in an access rule includes both pre-configured sources (resources) and sources that you enter directly on an access rule (composite sources).

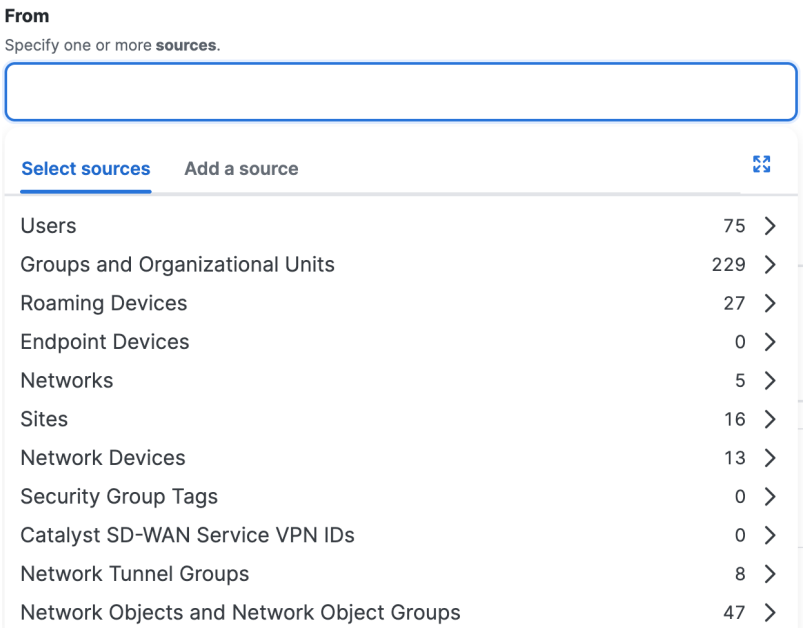
You can add at most 10 composite sources in an internet access rule.

Reusable Sources in Internet Access Rules

Describes Reusable Sources in Internet Access Rules in Cisco Secure Access. You can configure internet access rules for specific source-destination pairs.

You can configure internet access rules for specific source-destination pairs. Sources are the users, groups of users, or other entities that comprise the **From** end of traffic where Secure Access applies an access rule.

In a rule, you can also specify sources by typing in IP addresses and subnets, but these are not reusable source components. For more information, see Composite Sources in Internet Access Rules on page 865



You can use these reusable sources in your internet access rules:

- Users

  You can apply rules to the traffic for the users in the organization.

- Groups and Organizational Units

  You can apply rules to the traffic for users in AD Groups and Google Workspace Organizational Units.

- Roaming Devices

  You can apply rules to traffic originating from managed devices that have the Cisco Secure Client installed, but that may not currently be on the corporate network.

- Network Objects

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Objects.

- Network Object Groups

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Objects in Network Object Groups.

- Endpoint Devices

  You can apply internet access rule security controls to AD devices in Secure Access. Once provisioned, AD devices are available as sources on internet access rules. You can select all AD devices or individual AD devices identified by device name. For more information about AD device provisioning, see Manage Users, Groups, and Endpoints Devices.

- Registered Networks

  You can apply rules to traffic originating from IP addresses in network segments defined by Registered Networks.

  - When on a Registered Network, users devices can send traffic to the Secure Access DNS resolvers and the Secure Web Gateway (SWG) directly. In this scenario, user devices are not required to deploy the Cisco Secure Client with the Internet Security and VPN modules or deploy IPsec tunnels (RAVPN).
  - If the user device has the Cisco Secure Client deployed with the Internet Security and VPN modules, then traffic is sent over IPsec tunnels to Secure Access.

- Sites

You can apply rules to traffic originating from IP addresses in network segments defined by Secure Access Sites.

- Network Devices

  You can apply rules to traffic originating from network devices.

- Security Group Tags

  You can apply rules to traffic originating from IP addresses in network segments that include Security Group Tags.

- Catalyst SD-WAN Service VPN IDs

  You can apply rules to traffic originating from IP addresses in network segments that include VPN IDs. Be aware that if the same VPN ID (*VPN 88* for example) is assigned across different branches, then traffic coming into Secure Access from these branches is subject to the same policy. A Secure Access policy rule cannot differentiate traffic between branches using the same VPN ID.

- Network Tunnel Groups

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Tunnel Groups.

Combining Reusable Sources in a Rule with Boolean Logic

Describes Combining Reusable Sources in a Rule with Boolean Logic in Cisco Secure Access. If an internet access rule includes multiple reusable sources, Secure Access applies the sources together using boolean logic.

If an internet access rule includes multiple reusable sources, Secure Access applies the sources together using boolean logic.

Secure Access combines all types of reusable sources and all sources within a type using the boolean **OR** operator. Traffic to each source that you specify in the access rule matches the rule.

For example, if you specify a user group and a network tunnel group as sources, traffic from any member of either group matches the rule.

Using the AND Operator With Sources

Secure Access supports adding pre-configured sources on internet access rules combined with the logical **AND** operator. For information about adding sources with the **AND** operator, see Add an Internet Access Rule.

Secure Access enforces the access rule only if all sources added on the access rule match the organization's network traffic. For example, if you add a **Google Workspace User** source and add the **AND** operator with a **Registered Network** source, traffic for both sources must match for Secure Access to apply the access rule.

Supported Combinations of Reusable Sources with Composite Sources

You can select pre-configured sources and enter composite sources on the internet access rules in your Access policy. Secure Access uses the logical OR operator to combine the pre-configured sources with the composite sources.

You can enter these composite sources on an internet access rule:

- IP/CIDR Blocks/Wildcard Mask
- Ports and port ranges

For more information about composite sources, see Composite Sources in Internet Access Rules.

Supported Combinations of Reusable Sources With the AND Operator

Reusable Sources	AND with Other Reusable Sources
AD Users	Registered Networks Internal Networks Network Tunnel Groups
AD Groups	Registered Networks Internal Networks Network Tunnel Groups
Google Workspace Users	Registered Networks Network Tunnel Groups
Google Workspace Organizational Units (OUs)	Registered Networks Network Tunnel Groups
Chromebooks	Registered Networks Network Tunnel Groups
Mobile Devices	Registered Networks
Roaming Devices	Registered Networks
Network Tunnel Groups	Users Groups and Organizational Units
Registered Networks	AD Users AD Groups Google Workspace Users Google Workspace OUs Chromebooks Mobile Devices Roaming Computers Internal Networks Sites
Sites	AD Users AD Groups Google Workspace Users Google Workspace OUs Chromebooks Mobile Devices Roaming Computers Internal Networks Registered Networks

Reusable Sources	AND with Other Reusable Sources
Internal Networks	AD Users
	AD Groups
	Google Workspace Users
	Google Workspace OUs
	Sites

Composite Sources in Internet Access Rules

Describes Composite Sources in Internet Access Rules in Cisco Secure Access. Organizations can add network address information directly in the source component of an internet access rule.

Organizations can add network address information directly in the source component of an internet access rule. The source component supports IP addresses (IPv4 and IPv6), CIDR blocks, and wildcard masks, and ports and port ranges. For more information, see Add an Internet Access Rule.

Note

Internet access rules that include composite sources support the **Allow** and **Block** actions only.

Guidelines for Adding Composite Sources in a Rule

- Composite sources are valid public IPv4 or IPv6 addresses, private non-routable IPs (RFC-1918 compliant), CIDR blocks, wildcard masks, and ports and port ranges. For information about wildcard masks, see Using Wildcard Masks on Access Rules.
- IP addresses do not require a deployed IPsec tunnel.
- Secure Access does not support a comma-separated list of wildcard masks.
- If the IP addresses added as composite sources are not associated with the organization's Registered Networks, Secure Access does not manage traffic on these IP addresses.

Combining Source Addresses and Ports

Combining IPs, CIDRs, or Wildcard Masks on a Source

When you add the IP addresses and CIDR blocks for a source on an internet access rule, Secure Access creates a single source entry. Secure Access uses the OR operator to combine the IP addresses, CIDR blocks, and wildcard masks that you entered on the rule.

Combining Ports and Port Ranges on a Source

When you add the ports and port ranges for a source on an internet access rule, Secure Access creates a single source entry. Secure Access uses the OR operator to combine the ports and port ranges that you entered on the rule.

Combining IP Addresses and CIDR Blocks With Ports on a Source

Secure Access uses the AND operator to combine the IP addresses and CIDR blocks with the ports and port ranges entered on the source component of the internet access rule.

Boolean logic for addresses and port



Destinations

Describes Destinations in Cisco Secure Access and outlines Number of Destinations Supported in a Rule and How to Add Destinations on Internet Access Rules. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Destinations on internet rules are either pre-configured or composite components. For information about pre-configured destination components, see Reusable Destinations in Internet Access Rules.

Composite destinations may include IP addresses, CIDR blocks, wildcard masks, fully-qualified domain names (FQDNs), ports and port ranges, and transport protocols. For information about composite destination components, see Composite Destinations in Internet Access Rules.

Number of Destinations Supported in a Rule

You can add up to 5000 destinations in an internet access rule. The total number of destinations accepted on an access rule includes both pre-configured destinations (resources) and destinations that you enter directly on an access rule (composite destinations).

You can add at most 10 composite destinations in an internet access rule.

For optimal performance, include no more than 100 destinations in a rule.

How to Add Destinations on Internet Access Rules

For more information, see Add an Internet Access Rule.

- We recommend that you pre-configure destinations in Secure Access.
- You can also specify web sites by their content categories, individual web application, or web application categories without creating content category lists or application lists. On an internet rule, choose **Content Categories** or **Application Categories**.
- Depending on the destinations you select (for example certain applications, application lists, or application categories) other options may appear in the rule.
- If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future.
- When you select a list or group, entities that are added to the list or group in the future are automatically included. For example, if you select a Destination List, any destinations that you add to that destination list later are automatically included.
- If this rule involves tenant controls, you must include the relevant application as a destination in the rule, as well as configuring the applicable tenant control profile and specifying that profile in the Security Controls section of the rule. For more information, see Manage Tenant Control Profiles.

- When specifying applications, it is not possible to search for an application with fewer than three letters in its name—for example, **QQ** or **YY**. You must pick the applications manually from the tree under their respective categories or use a wildcard in search—for example, **QQ***. This behavior is by design.

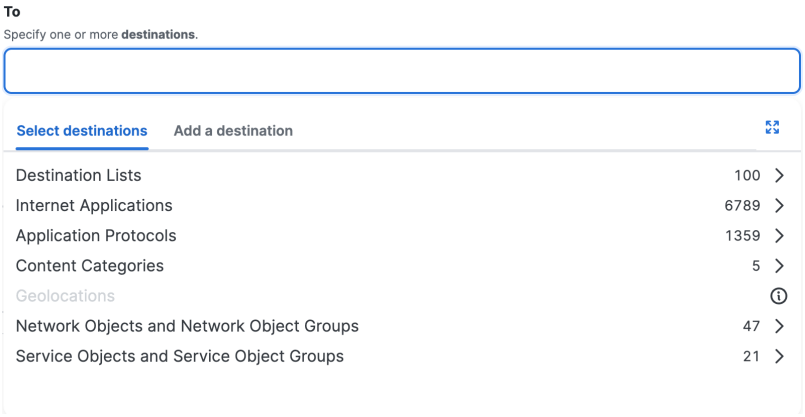
Reusable Destinations in Internet Access Rules

Describes Reusable Destinations in Internet Access Rules in Cisco Secure Access. You can configure internet access rules in the Access policy for specific source-destination pairs.

You can configure internet access rules in the Access policy for specific source-destination pairs. Destinations are the web applications, web sites in particular categories, or other internet destinations that comprise the "To" end of traffic where Secure Access applies an access rule.

In an access rule, you can also enter destination IP addresses and subnets, and ports and protocols directly on the rule. For more information, see Composite Destinations in Internet Access Rules.

You can use these reusable destinations in your internet access rules:



- Destination Lists—Lists that group domains, URLs, IP addresses, and CIDR blocks where you want to apply the same security controls. You can create custom lists of destinations based on any criteria you choose.
- Application Lists—Lists of web-based applications where you want to apply the same policy.

  For example, if you want to apply a single policy to all social media applications, you can create an application list that includes all applications in the Social Networking category.

  For some web-based applications, you can allow access to the application, but block uploads, downloads, and posting or sharing information. You will see these options in each rule when you configure applicable destinations in the rule. For details, see Advanced Application Controls.
- Application Protocols—Select the application protocols for the network destinations where Secure Access applies the rule.
- Content Category Lists—Lists of web sites based on the content or type of the site, so you can control access to a variety of sites as a group. For example, you might create a content category list that includes all sites belonging to the Adult, Child abuse, and Pornography categories.
- Network Objects—Network Objects represent IPv4 and IPv6 addresses, CIDR blocks, ranges of IPv4 addresses, wildcard masks, or fully-qualified domain names (FQDNs). Select the Network Objects on the access rules to apply security controls to the traffic on the networks.
- Network Object Groups—Select the Network Object Groups on the access rules to apply security controls to the traffic on the networks in groups.
- Service Objects—Service Objects represent a port, range of ports, protocol, or traffic on any protocols. Select the Service Objects on the access rules to apply security controls to the services.

- Service Object Groups–Select the Service Object Groups on the access rules to apply security controls to the traffic on the services in groups.

Additional Configuration Options

- Specify web sites by content category, or specify web applications or categories of web application, without creating content category lists or application lists.
- Apply an app risk profile to modify the list of destinations the rule targets. An app risk profile defines a list of risk characteristics. When you add an app risk profile to an access rule, the rule takes the characteristics from the profile into account when determining whether to flag an internet application.

  The app risk profile characteristics can include:

  - The label status from the App Discovery Report.
  - The application risk score calculated by Secure Access. For more information see, Procedure on page 2480 or Change App Details on page 2483.
  - Business risk factors.
  - Various security-related attributes such as security standard compliance, or resistance to various known vulnerabilities. For more information, see Add an App Risk Profile.

Rule Enforcement with Destination Lists and Fully Qualified Domain Names

You can add destination lists that include fully qualified domain names (FQDNs) on internet access rules.

Important

To enforce internet access rules that include destination lists with fully qualified domain names (FQDNs), Secure Access requires that DNS lookups for these FQDNs route through Secure Access. For more information, see Manage End-User Connectivity and Manage DNS Servers.

For information about decryption, see Security Profiles for Internet Access and Manage Traffic Decryption.

Composite Destinations in Internet Access Rules

Describes Composite Destinations in Internet Access Rules in Cisco Secure Access. You can define a destination from multiple network address components.

You can define a destination from multiple network address components. A composite destination accepts IP addresses, CIDR blocks, wildcard masks, ports 80 and 443 for web traffic or all ports on non-web traffic, and the TCP, UDP, and ICMP transport protocols. You can choose **ANY** to select all available protocols on a destination. For more information, see Add an Internet Access Rule.

This option is useful if you need to quickly address a specific issue that arises, for example to immediately allow access to a necessary destination that is being blocked by another rule, or to immediately block access to a problem destination.

Limitations of Composite Destinations

- Internet rules with composite destinations only support the **Allow** and **Block** actions.
- Composite destinations do not accept private non-routable IP addresses.

IP Addresses, CIDR Blocks, and Wildcard Masks

- Destinations accept valid public IP addresses, CIDR blocks, or wildcard masks.

For information about wildcard masks, see Using Wildcard Masks on Access Rules.

Ports

- Destinations accept ports 80 and 443 only for web traffic and all ports or port ranges for non-web traffic.

Protocols

- Destinations accept the TCP transport protocol. If you select **TCP**, the rule applies to web traffic and is protected by the secure web gateway.
- Destinations accept the UDP or ICMP protocols. If you select **UDP** or **ICMP**, the rule applies to non-web traffic and is protected by the IPS.
- For the protocol on the destination, you can choose **ANY**. If you select **ANY**, the rule applies to traffic on the TCP, UDP, and ICMP protocols. The traffic is protected by the secure web gateway.

Combining Composite Destinations on an Internet Access Rule

When you add individual network address components on a destination, Secure Access combines the field values to create a single destination entry. You can add multiple composite destinations on a rule.

- The ports added to the destination are OR'ed together. The rule applies to traffic on ports 80 or 443.
- The protocols added to the destination are OR'ed together. The rule applies to traffic on the selected protocols.
- The individual network component field values that you enter for **Ports**, **Protocols**, and **IPs**, **CIDRs**, or **Wildcard Masks** are AND'ed together to create a single destination. The rule applies to the traffic on the composite destination.

> **Note**
>
> You are not required to choose an IP, protocols, or ports to add a composite destination. Instead, you can choose the **ANY** protocol to define a destination that matches traffic on any IP or CIDR, with any port, on the available destination protocols.

Combining Multiple Destinations in a Rule (Boolean Logic)

Describes Combining Multiple Destinations in a Rule (Boolean Logic) in Cisco Secure Access and outlines Combine Internet Destinations with Objects and Groups. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

If an internet access rule includes multiple destinations, the following boolean logic applies:

- All types of destinations, and all destinations within a type, are treated as using the boolean OR operator. Traffic to each destination that you specify in a rule matches the rule.
  - For example, if you specify a content category and an application list as destinations in a single rule, traffic to any destination that is a member of either group will match the rule.
- If you specify **ANY** for the protocol, then all traffic on the protocols (**TCP**, **UDP**, **ICMP**) supported by internet rules matches the rule, regardless of any other destinations that you specify.
- If you enter in values of different types (IP address, port, protocol), traffic matches if any of the specified values match the rule.
  - For example, if you specify an IP address and a port, traffic to any IP address on the specified port matches the rule, as does traffic to the specified address on any port.

Combine Internet Destinations with Objects and Groups

You can use the logical AND operator to combine reusable destinations with objects and groups on the internet access rules in the Access policy. Combine the Network Objects or Network Object Groups or Service Objects or Service Object Groups with these destinations.

- Application lists, internet applications, internet application categories
- Application protocols
- Content categories

	Network Objects	Network Object Groups	Service Objects	Service Object Groups
Application Lists, Internet Applications Application Categories	AND	AND	AND	AND
Application Protocols	AND	AND	AND	AND
Content Categories	AND	AND	AND	AND
Destination Lists	AND	AND	AND	AND

Security Controls

Describes Security Controls in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Security controls make use of profiles and other pre-configured settings.

These security controls apply to internet traffic:

- Intrusion Prevention (IPS)
- Security Profile
- Tenant Controls

Intrusion Prevention (IPS)

Describes Intrusion Prevention (IPS) in Cisco Secure Access. Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics.

Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics.

You will specify a single intrusion prevention profile in each access rule.

Set Up Certificates for Decrypting Internet Traffic

Internet traffic must be decrypted in order to allow it to be inspected by the intrusion prevention and for web security features, for example those defined in a Security Profile. In order to decrypt this traffic, certificates are required. You may have already set up these certificates to decrypt traffic for web security features.

See Certificates for Internet Decryption.

Configure Intrusion Prevention (IPS) Profiles

Intrusion Prevention (IPS) detects a large number of known threats. Sets of settings are grouped together in profiles, which you can specify in access rules. Secure Access provides several pre-configured profiles that address common

needs, such as Balanced Security and Connectivity or Maximum Security. Or you can create a custom profile using Snort signatures. You can also choose to block or just monitor traffic that matches a profile.

You can choose a different IPS profile for each access rule based on the balance of convenience vs. risk appropriate for the particular traffic.

For details, see Manage IPS Profiles.

Configure the Do Not Decrypt List for IPS

Secure Access must decrypt traffic in order to allow the Intrusion Prevention feature to inspect the traffic for threats.

However, decrypting traffic to certain sites, such as health-related or financial sites, may be restricted by privacy laws in some geographic regions.

Use the default Do Not Decrypt List to specify destinations that should not be decrypted by intrusion prevention processes (IPS.)

Web security features, for example those configured in a Security Profile, also require decryption in order to be effective; you can use this list for web security decryption, or you can create and use a different list or lists for web security.

For details, see Important Information About Do Not Decrypt Lists.

> **Note**
>
> IPS in Cisco Secure Access does not support traffic from the Secure Client roaming module.

Security Profile

Describes Security Profile in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You can specify a single Security Profile in an internet access rule. Each security profile includes multiple components that you should pre-configure.

Sets of security security settings grouped into profiles control aspects of security for internet traffic.

Enable these options in a security profile and then choose the security profile in an access rule. For more information, see Add a Security Profile for Internet Access.

- For **Decryption** (including Do Not Decrypt lists), see Set Up Certificates for Decrypting Internet Traffic and Configure Do Not Decrypt Lists.
- **SSO Authentication**. For more information, see Security Profiles for Internet Access.

  SSO authentication is required for some web security features.
- **Threat Categories**. For more information, see Threat Categories.

  Choose the types of web-borne threats to block. Blocking some threat categories may affect legitimate traffic.
- For **File inspection**, see Manage File Inspection and File Analysis.

  File inspection detects threats using Cisco Advanced Malware Protection and Cisco Secure Malware Analytics.
- For **File type blocking**, see Manage File Type Control.

  Block files based on their type. For example, you can prevent users from downloading executable files from the web.
- For **SafeSearch**, see SafeSearch.

  SafeSearch filters out offensive, explicit, unsafe, and harmful results from searches in Google, YouTube, Yahoo, and Bing.

- For **AI Supply Chain Blocking**, see AI Supply Chain Report.

  AI Supply Chain Blocking controls end user access to files that can pose AI supply chain risk to security and compliance.

- For **End-user notifications**, see Manage Notification Pages.

  If you do not want to use the default Secure Access-branded notifications, configure the notifications that are:

  - presented to end users who attempt to access internet destinations that are blocked
  - present when users attempt to access destinations that match a rule configured with the Warn action

  End-user notifications require decryption.

  Web pages shown to users who attempt to access blocked destinations or destinations allowed with a warning.

Set Up Certificates for Decrypting Internet Traffic

Describes Set Up Certificates for Decrypting Internet Traffic in Cisco Secure Access. If you have already set up certificates for this purpose for the intrusion prevention feature, you may not need to do anything more.

If you have already set up certificates for this purpose for the intrusion prevention feature, you may not need to do anything more.

Internet traffic must be decrypted in order to allow it to be inspected by the intrusion prevention and web security features, to apply acceptable use controls, for rules in which the rule action is Isolate or Warn, and to display end-user notifications when destinations are blocked.

In order to decrypt this traffic, certificates are required.

See Certificates for Internet Decryption.

Configure Do Not Decrypt Lists

Describes Configure Do Not Decrypt Lists in Cisco Secure Access. Secure Access must decrypt internet traffic in order to allow Web Security features to protect your network effectively.

Secure Access must decrypt internet traffic in order to allow Web Security features to protect your network effectively.

However, decrypting traffic to certain sites, such as health-related or financial sites, may be restricted by confidentiality law in certain geographic regions.

Use a Do Not Decrypt List to specify destinations that should not be decrypted by web security processes. You can create different Do Not Decrypt Lists for different regions or purposes.

You can use the same Do Not Decrypt List that you use for IPS, or create one or more Do Not Decrypt lists to use only for security features included in the security profile.

For details, see Important Information About Do Not Decrypt Lists.

Tenant Controls

Describes Tenant Controls in Cisco Secure Access. If your company uses Microsoft 365, Slack, Google G-Suite, or Dropbox, see Manage Tenant Control Profiles.

If your company uses Microsoft 365, Slack, Google G-Suite, or Dropbox, see Manage Tenant Control Profiles.

Advanced Security Controls

Describes Advanced Security Controls in Cisco Secure Access. This section includes options to skip enforcement of certain security features, which you may want to do permanently for trusted destinations or temporarily to troubleshoot an issue.

This section includes options to skip enforcement of certain security features, which you may want to do permanently for trusted destinations or temporarily to troubleshoot an issue.

This section includes the ability to access files without decrypting them (sometimes known as "protected file bypass") and the ability to not enforce certain web security features for this rule.

In general, you should allow access to encrypted files only for trusted destinations, because encrypted files cannot be effectively assessed for threats. By default, access to encrypted files is not enabled.

Disable security features only when you have a specific reason to do so.

For more information, see Manage Advanced Security Controls .

Control Egress IP Address for Select SaaS Internet Destinations

Describes Control Egress IP Address for Select SaaS Internet Destinations in Cisco Secure Access. To ensure specific egress IP addresses for traffic to specific SaaS internet destinations outside your network, such as YourCompany.OtherCompany.com, see Zero Trust Access to Internet Destinations.

To ensure specific egress IP addresses for traffic to specific SaaS internet destinations outside your network, such as *YourCompany.OtherCompany.com*, see Zero Trust Access to Internet Destinations.

Ensure Rule Matching for Encrypted Internet Traffic

Describes Ensure Rule Matching for Encrypted Internet Traffic in Cisco Secure Access. In order to ensure that internet rules match encrypted traffic as expected, you must add an extra rule to decrypt the traffic.

Important

In order to ensure that internet rules match encrypted traffic as expected, you must add an extra rule to decrypt the traffic. Essentially, traffic cannot be inspected until after it is decrypted, and cannot match a rule until it can be inspected, and a single rule cannot both decrypt and inspect a transaction.

This situation is best explained using the following example scenario.

Scenario

A Network ("Network1") source makes a web request to URL https://www.mydomain.com/myurl.

Rule does not match the traffic:

Top rule: Source: Any. Destination: https://www.mydomain.com/myurl. Decryption is enabled.

2nd Rule: Source Any. Destination: Any. Decryption is disabled.

Result: The 2nd rule will apply.

Explanation: The top rule specifies a destination that can only be identified if decryption has occurred for the request. However, because the only place decryption is enabled is in that same rule, that rule will never be matched and therefore decryption will not occur.

Rule matches the traffic:

Top rule: Source: Any. Destination: https://www.mydomain.com/myurl. Decryption can be enabled or disabled.

2nd Rule: Source Any. Destination: Any. Decryption is enabled.

Result: The top rule will apply.

Explanation: The 2nd rule triggers decryption, giving Secure Access visibility to the URL being requested, but does not match the rule. The rules are then re-run, top down, with the URL information. This results in matching the top rule.

Block Internet Access to Geographic Locations

Describes Block Internet Access to Geographic Locations in Cisco Secure Access. To prevent users from accessing web sites hosted in certain countries, you can specify a geolocation destination on an internet access rule.

To prevent users from accessing web sites hosted in certain countries, you can specify a geolocation destination on an internet access rule. This option is available only when the rule action is Block and the rule includes no destinations other than geolocations. Secure Access logs all traffic that is blocked based on configured geolocation.

The location of a site is determined by its public IP address.

> **Note**
>
> **Blocked Internet Access**
>
> Traffic to a blocked destination may be allowed if a domain resolves to multiple IP addresses corresponding to different countries.

To block access by site location:

1. Create an internet access rule.
2. (Recommended) Position geolocation rules at the top of the rule list and place any exceptions above the general geolocation rules.
3. Choose **Block** as the rule action.
4. Choose **Geolocations** as the Destination.
5. Select continents and countries as applicable.
6. In the security controls section, choose a security profile in which decryption is enabled. You can also specify in this profile a notification page that will be displayed to end users who attempt to access destinations blocked by this rule.

Add an Internet Access Rule

Provides instructions for completing the Add an Internet Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Cisco Secure Access policy is a collection of an organization's internet and private access rules. To start protecting user devices that connect to the Internet, add internet access rules to the organization's Access policy.

This guide describes the steps to add an internet access rule and configure the security controls and profiles.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- At a minimum, to add an internet access rule, configure the source and destination components and rule settings.
  - For more information, see Components for Internet Access Rules.
  - For more information, see Default Settings for Internet Access Rules.
- For other factors involved in creating and enforcing internet access rules, see Get Started With Internet Access Rules.
- In general, decryption is required to properly process HTTPS traffic, including traffic that will be blocked. For more information, see Security Profile.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Click **Add Rule** > **Internet Access**.

   At the top of the rule is a summary section. The **Summary** describes the security controls that you configure on this rule.

3. Navigate to **Specify Access**, and then configure the access criteria for the rule.
   For more information, see Access Criteria
4. Click **Next**.

   > **Note**
   >
   > The **Next** button is not available until you give the rule a name and then click out of the **Rule name** field.

5. Navigate to **Configure Security**, and then configure the security control settings for the rule.
   For more information, see Security Control Options.
6. Click **Save**.
7. (Optional) Enable or disable the rule using the toggle at the top of the page.

What to do next

Return to Get Started with Internet Access Rules and review additional steps you should take after configuring a rule.

Important

Additional rules are required for most traffic. For more information, see Ensure Rule Matching for Encrypted Internet Traffic.

Access Criteria

Describes Access Criteria in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- Disable or enable the rule
- Logging settings

- Summary
- Rule name
- Rule order
- Rule action
- Enable a Schedule on an Internet Rule
- Pre-Configured Sources
- Composite Sources
- Pre-Configured Destinations
- Composite Destinations
- App Risk Profiles
- Advanced Application Controls

Enable the Rule and Edit Your Logging Settings

Provides instructions for completing the Enable the Rule and Edit Your Logging Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Enable the internet access rule in the Access policy and manage the logging settings on the access rule.

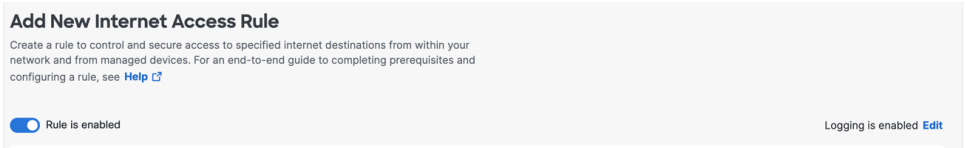
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

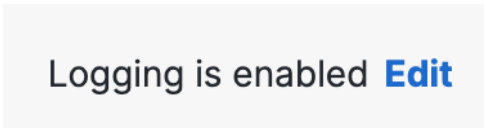
Procedure

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Click **Rule is enabled** to toggle on the rule.

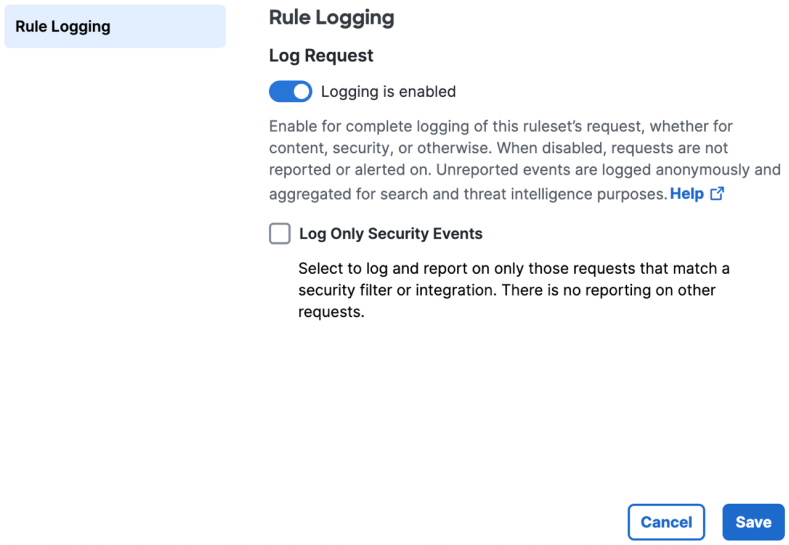
   After you configure and save the rule to your policy, the rule is enabled. You can toggle off the rule at any time to disable it.

3. Navigate to the **Logging** options on the top right corner of the page.

   a) Click **Edit** to manage your logging settings on the access rule.



b) For **Log Request**, toggle off or on to choose whether Secure Access logs the events for the traffic managed by the access rule.

c) For **Log Only Security Events**, select whether Secure Access logs the events that match thesecurity filters.

For more information, see Manage Logging.

d) Click **Save**.

Summary

Provides instructions for completing the Summary workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a rule to your policy, you can edit the rule and then view the rule summary.

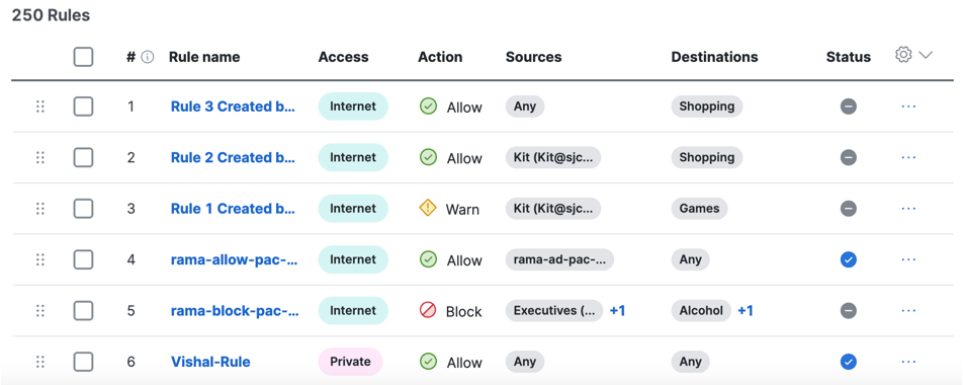
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Secure** > **Access Policy**.
2. Navigate to a rule, and then click on the horizontal ellipsis (**...**) to expand the rule menu.



3. Click **Edit** to open the rule and view the rule summary.



The summary contains the components that you configured on the access rule:

- **Sources**
- **Action**
- **Security Controls**
- **Destinations**

What to do next

If you see an **Upgrade** button, this means your organization has an opportunity to upgrade to a licensing package that offers additional functionality. For details, contact your Cisco representative.

Rule Name

Describes Rule Name in Cisco Secure Access and outlines Guidelines for Creating a Rule Name. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You must give your access rule a meaningful name. The **Rule name** is required. You must add a rule name before you can continue to configure the **Security Controls** on the access rule.

> **Note**
>
> The **Next** button on the access rule is not available until you enter a name for the rule.

Guidelines for Creating a Rule Name

Secure Access enforces the number and type of characters supported in a rule name. You can add a rule name with these constraints:

- A rule name is a sequence of 2–50 alphanumeric, hyphen, underscore, and space characters.
- A rule name must be unique across all access rules in the organization's Access policy.

Rule Order

Describes Rule Order in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Specify where you want this rule in the overall rule order.

Secure Access applies the first rule in the list on the Access Policy page that matches the traffic.

Order your rules so that more specific rules are above more general rules that might also apply to the traffic.

For important guidelines, see Edit the Order of Rules on the Access Policy Page.

Rule Action

Describes Rule Action in Cisco Secure Access. By default, access to internet destinations is allowed unless an access rule blocks or modifies access using the Warn or Isolate options.

By default, access to internet destinations is allowed unless an access rule blocks or modifies access using the Warn or Isolate options.

The action you choose determines which other options are available in the rule.

Specify the rule action before you specify other settings including source and destination, or those configurations will be reset when you change the action.

- **Allow** – When the action is Allow, traffic can still be blocked if it does not pass the security controls specified in the rule.
- **Block** – If you want to display a notification page to end users who attempt to access a blocked destination. For more information, see Manage Notification Pages.
- **Warn** – When the action is Warn:
  - End users must click a link in a warning notification to access the destination.
  - The destination can include applications and application categories as well as content categories and content category lists.
  - You can configure a custom warning notification that Secure Access will present to users who attempt to access a warned destination. You can also preview the notification page. See Manage Notification Pages.
  - Decryption must be enabled in order to present the notification.
  - For required certificates for displaying notifications, see Certificates for Internet Decryption.
- **Isolate** – If your license includes the Remote Browser Isolation feature, Secure Access creates a virtual browser that hosts applicable destination access requests. This action is available only for certain destinations.

  For information about the Isolate action, see Understand Isolated Destinations.

  If you see an **Upgrade** button, click it for information about enhanced functionality for this feature.

Enable a Schedule on an Internet Access Rule

Provides instructions for completing the Enable a Schedule on an Internet Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

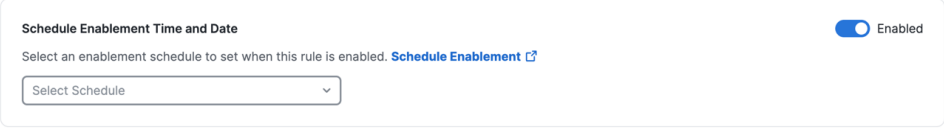
Configure the **Schedule Enablement Time and Date** setting and add a Schedule on the internet access rule. For information about configuring Schedules in Secure Access, see Manage Schedules.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. On an internet access rule in the Access policy, navigate to **Specify Access**, and then navigate to **Schedule Enablement Time and Date**.



2. Click **Enabled** to activate a Schedule on the internet access rule.
   a) (Optional) To disable a Schedule on the internet access rule, toggle off the **Schedule Enablement Time and Date** setting.
3. Click the **Select Schedule** drop-down menu and then choose a schedule to enable on the internet access rule.
4. Click **Save**.

Pre-Configured Sources

Provides instructions for completing the Pre-Configured Sources workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

We recommend that you create reusable components rather than adding source IP addresses, CIDR blocks, wildcard masks, and ports directly to a rule. For more information, see Components for Internet Access Rules.

On an internet access rule, you can select multiple pre-configured sources with the boolean **AND** operator. For information about combining sources on internet access rules with boolean logic, see Sources.

> **Note**
>
> The arrows out icon opens a window to configure the sources in your rule.

Before you begin

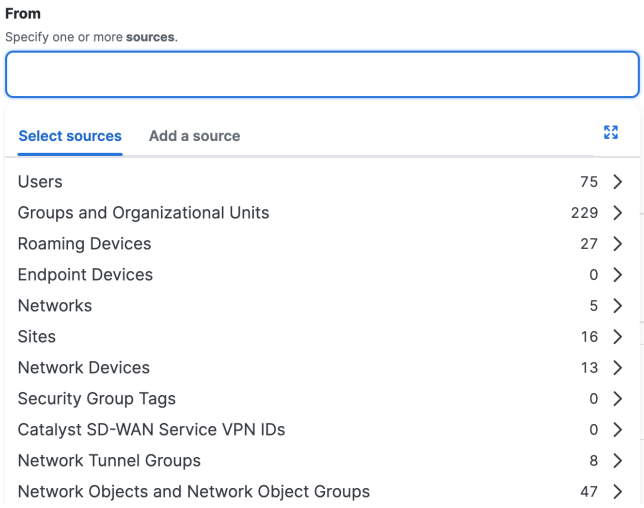
- Full Admin user role. For more information, see Manage Accounts.

Procedure

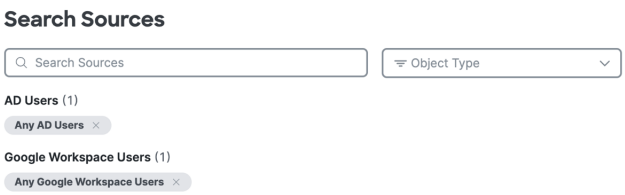
---

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access**, click on the search bar under **From**, and then navigate to **Select sources**.
3. Choose a source and all of its members or choose specific sources in your organization.

   For descriptions of the different types of sources, including links to how to create reusable sources, see Components for Internet Access Rules.

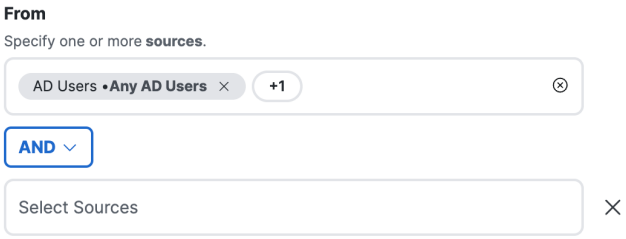


   a) (Optional) After you add a source, click **+More** to view the list of sources that you added to the access rule.

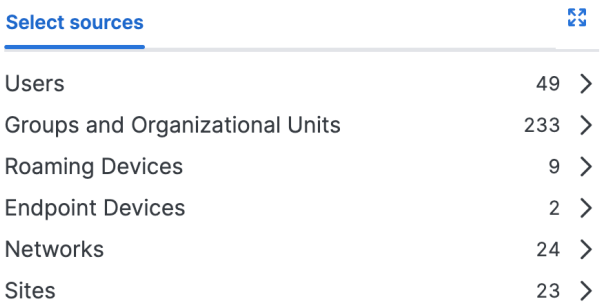


b) Click on the **X** to remove a previously-added source.
c) Click **Done** when you finish modifying the list of added sources.

4. (Optional) Click **AND**, and then click in the **Select Sources** text area.

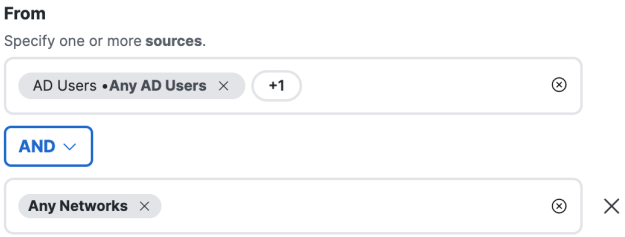


a) Choose a source and all of its members or choose specific sources in your organization.



b) (Optional) Click on the **X** outside of the second **Select Sources** text area.

Secure Access removes the selected **AND** operator with the sources.



Composite Sources

Provides instructions for completing the Composite Sources workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can add network information as composite sources directly on an internet rule. This option is useful if you need to quickly address a specific issue that arises, for example to immediately block a particular user's access to an internet destination. For information about configuring composite sources, see Composite Sources for Internet Access Rules.

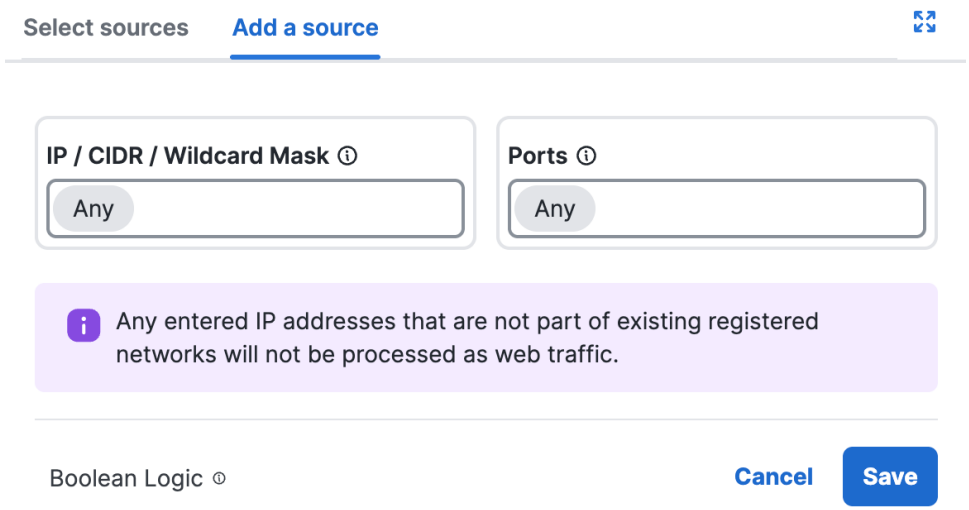
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **From**.
3. For **Add a source**, enter the network components that Secure Access combines on a source in the internet access rule.
   a) For **IP/CIDR/Wildcard Mask** , enter a single IPv4 or IPv6 address, CIDR block, IPv4 address with a wildcard mask, or a comma-separated list of IP addresses or CIDR blocks. You can also choose the **Any** option instead of entering IP addresses or CIDR blocks.



   For example:

   - IPv4 address–**1.2.3.4**
   - CIDR block–**1.2.3.4/24**
   - Wildcard mask–**1.2.3.4/255.255.255.255**

     For **Wildcard Mask**, use this format: `<IP address>/<Wildcard Mask>`. For information about wildcard masks, see Using Wildcard Masks on Internet Rules.

   b) For **Ports**, enter a port or range of ports separated by a hyphen (**-**), or a comma-separated list of ports and port ranges. You can also choose the **Any** option instead of entering the ports for the source.
4. Click **Save** to add the source.
   a) (Optional) After you add a composite source, click **+number** to view the list of sources that you added to the internet access rule.



b) Click on the **X** to remove a source entry.
c) Click **Done** to confirm the list of sources.

Pre-Configured Destinations

Provides instructions for completing the Pre-Configured Destinations workflow in Cisco Secure Access. We recommend that you create reusable components rather than adding destinations directly in a rule.

We recommend that you create reusable components rather than adding destinations directly in a rule. For more information, see Components for Internet Access Rules.

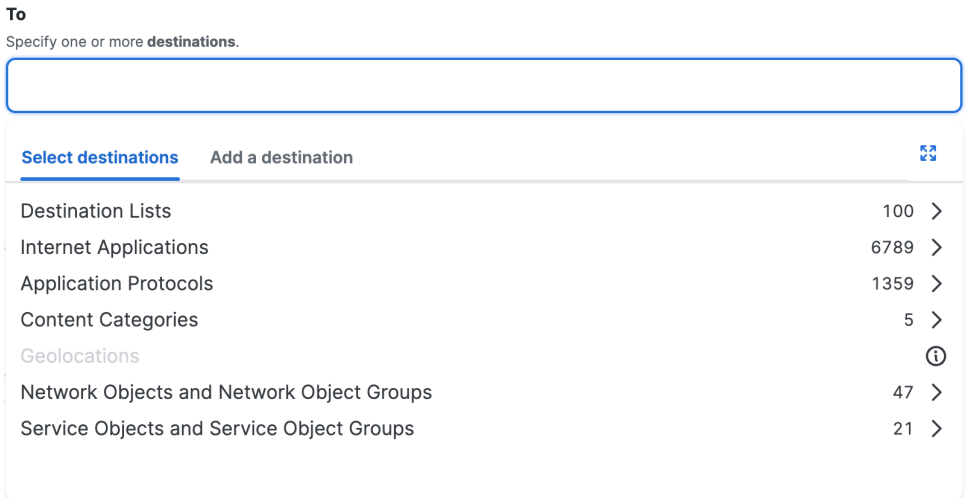
The rule action sets the the destination options that are available on the rule. Usually you will select destinations that you or others have previously configured.

> **Note**
>
> The arrows out icon opens a window to configure the destinations in your rule.

Procedure

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. Click **Select destinations**, click in the white space beside the default value (**Any**) and choose the configured destinations in your organization.

> **Note**
>
> If the rule action is **Block**, Secure Access displays the **Geolocations**.



4. (Optional) After you add a destination component, click **+More** to view the list of destinations that you added to the rule.
   a) Click on the **X** to remove a previously-added destination. Click **Done** when the list of destinations is complete.



Select Applications with Objects or Groups on Rules

Provides instructions for completing the Select Applications with Objects or Groups on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select reusable internet application lists, application categories, and internet applications for the destination component on internet access rules in the Access policy.

Once you add applications on an access rule, Secure Access enables the **+AND** button. Then, you can combine any Network Objects or Network Object Groups or Service Objects or Service Object Groups using the logical AND operator with the internet application lists, applications, and application categories.

> **Note**
>
> To determine if any internet access rules in the Access policy match the traffic on an application, Secure Access inspects 3-10 packets from an outbound client connection. The number of packets inspected depends on the application. Secure Access allows a few packets to reach the Internet regardless if you enabled the block action on the access rule.

Before you begin

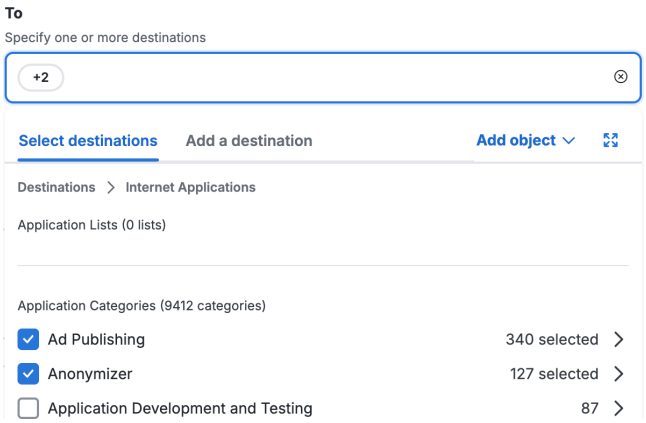
- Full Admin user role. For more information, see Manage Accounts.

Procedure

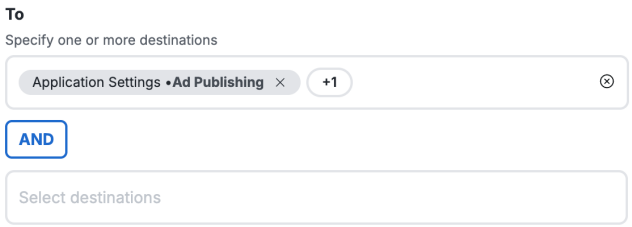
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



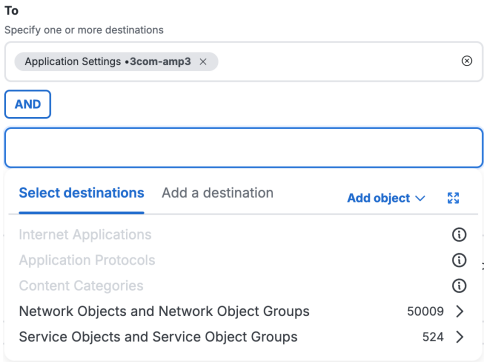
3. Click **Select destinations**, expand **Internet Applications**, and then select the internet applications and application categories to add to the internet rule.



4. (Optional) Click **+AND**.



5. Click in the **Select destinations** search bar.



a) Choose the Network Objects or Network Objects Groups to combine with the selected internet applications.
b) Choose the Service Objects or Service Objects Groups to combine with the selected internet applications.

Select Application Protocols with Objects or Groups on Rules

Provides instructions for completing the Select Application Protocols with Objects or Groups on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select application protocols for the destination component on internet access rules in the Access policy.

Once you add application protocols on an access rule, Secure Access enables the **+AND** button. You can combine any Network Objects or Network Object Groups or Service Objects or Service Object Groups using the logical AND operator with the selected internet application protocols.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

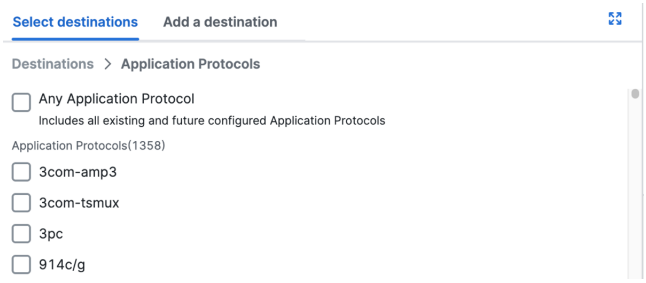
Procedure

---

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



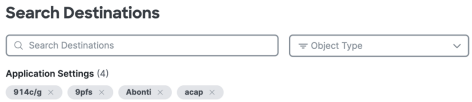
3. Click **Select destinations**, expand **Application Protocols**, and then select the application protocols to add to the internet rule.



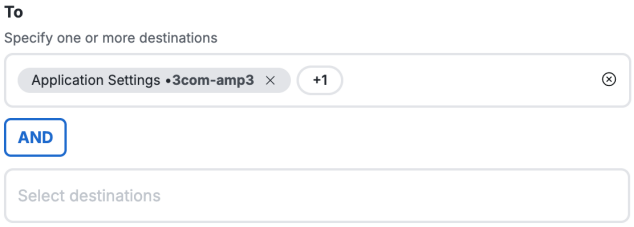
4. Click **+More** to view the added application protocols.



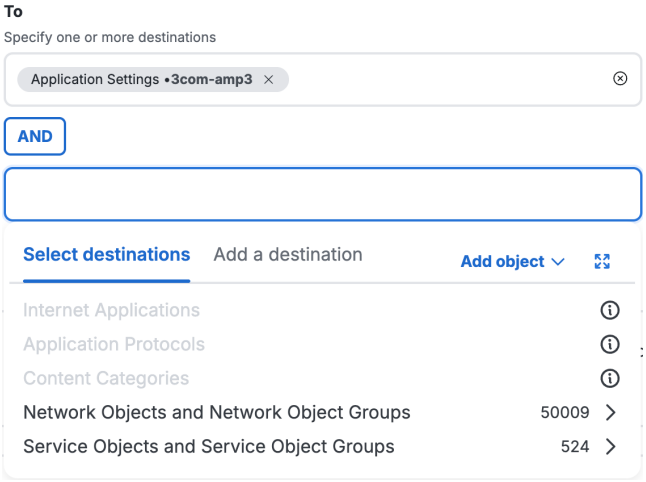
5. View or search for the added application protocols.



6. (Optional) Click **+AND**.



7. Click in the **Select destinations** search bar.



a) Choose the Network Objects or Network Objects Groups to combine with the selected internet applications.
b) Choose the Service Objects or Service Objects Groups to combine with the selected internet applications.

Select Content Categories with Objects or Groups on Rules

Provides instructions for completing the Select Content Categories with Objects or Groups on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

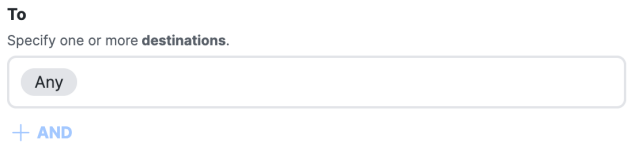
You can select content categories on an internet access rule in the Access policy. Once you add the content categories for the destination component on an access rule, Secure Access enables the **+AND** button. Then, you can combine any Network Objects or Network Object Groups or Service Objects or Service Object Groups using the logical AND operator with the selected content categories.

Before you begin

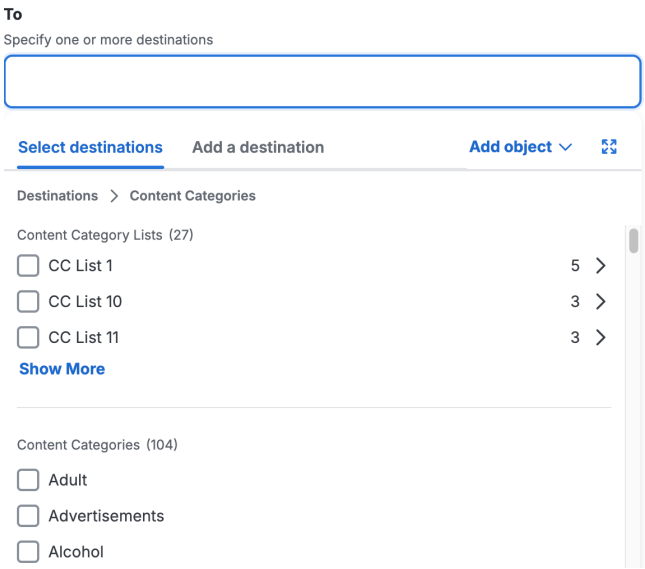
- Full Admin user role. For more information, see Manage Accounts.

Procedure

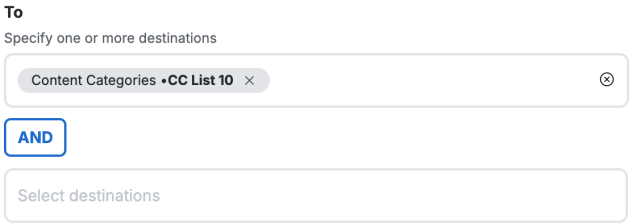
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



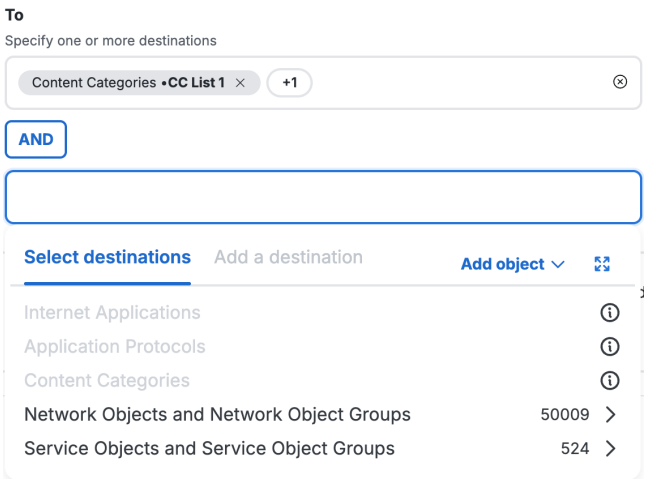
3. Click **Select destinations**, expand **Content Categories**, and then select the content categories to add to the internet rule.



4. (Optional) Click **+AND**.



5. Click in the **Select destinations** search bar.



a) Choose the Network Objects or Network Objects Groups to combine with the selected internet applications.
b) Choose the Service Objects or Service Objects Groups to combine with the selected internet applications.

Select Objects and Groups with Other Destinations on Rules

Provides instructions for completing the Select Objects and Groups with Other Destinations on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select Network Objects and Groups and Service Objects and Groups for the destination component on internet access rules in the Access policy. When you choose the objects and groups, you have the option to combine the objects and groups with the logical AND operator.

If you do not add the logical AND operator with the selected destinations, Secure Access combines the destinations with the logical OR operator. For more information, see Combining Multiple Destinations in a Rule (Boolean Logic).

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

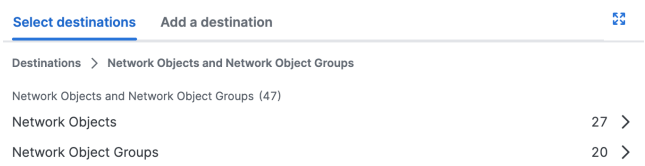
Procedure

---

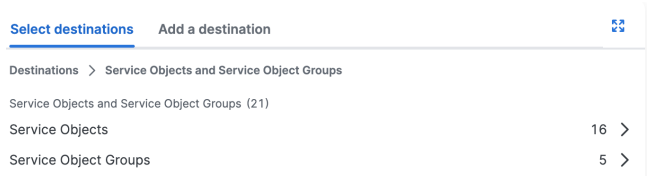
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



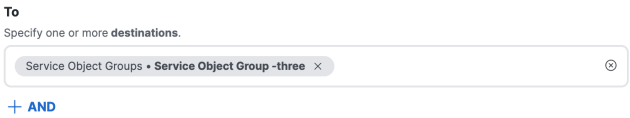
3. Select the Network Objects and Groups or Service Objects and Groups.
   a) Click **Select destinations**, and then choose the Network Objects and Groups to add to the internet rule.



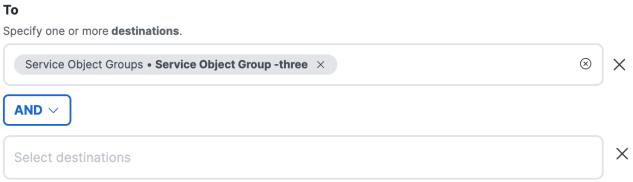
   b) Click **Select destinations**, and then choose the Service Objects and Groups to add to the internet rule.



4. (Optional) Click **+AND**.

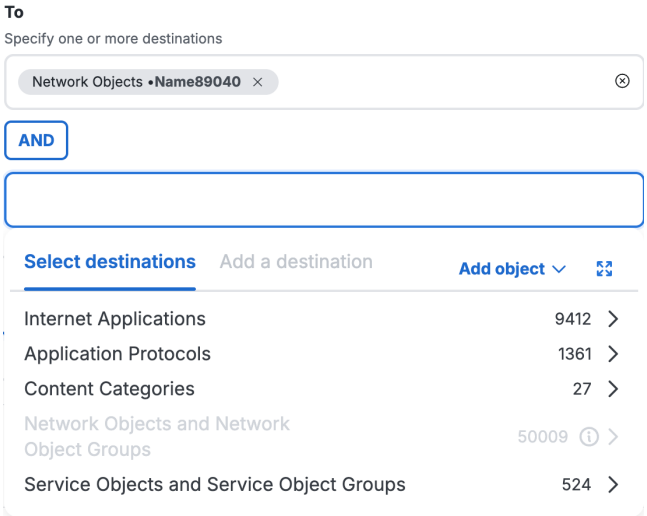


a) Click in the **Select destinations** search bar.



b) Choose a destination to combine with the other selected destinations using the logical AND operator.

For more information, see Combine Destinations With Boolean Logic.



After you select the objects and groups to use with the AND operator, you can remove the destinations and then add new destinations.

Add Reusable Network Objects on Rules

Provides instructions for completing the Add Reusable Network Objects on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can add a reusable Network Object resource for the destination component on the internet access rules in the Access policy. A Network Object represents a network resource–a single IPv4 address, IPv4 or IPv6 CIDR block, range of IPv4 addresses, wildcard mask, or fully-qualified domain name (FQDN).

Before you begin

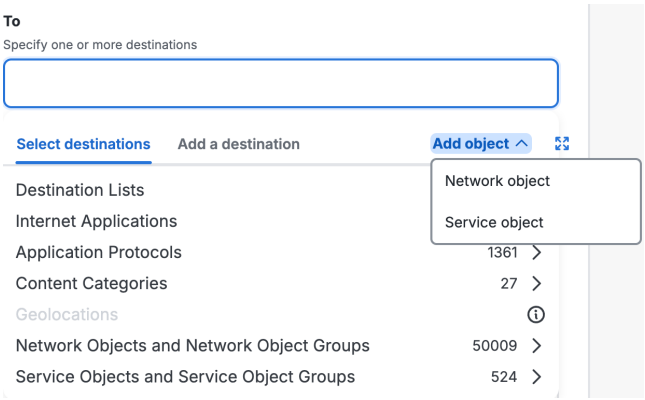
- Full Admin user role. For more information, see Manage Accounts.

Procedure

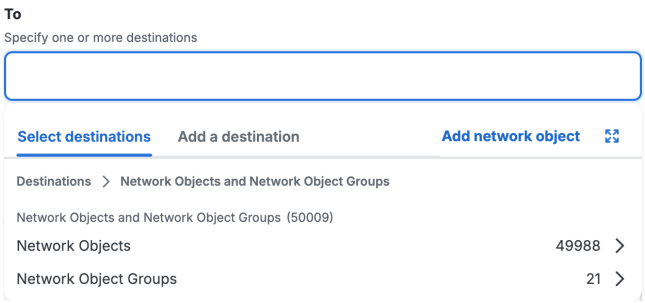
1. Navigate to **Secure** > **Access Policy**.
   a) To add a network object on a new access rule, click **Add Rule** > **Internet Access**.
   b) To add a network object on an existing access rule, click on the name of rule in the access rules table and then click **Edit**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



3. Navigate to **Select destinations**.
   a) Option 1: Click in the search bar for a network or service object, click **Add object**, and then choose **Network object**.



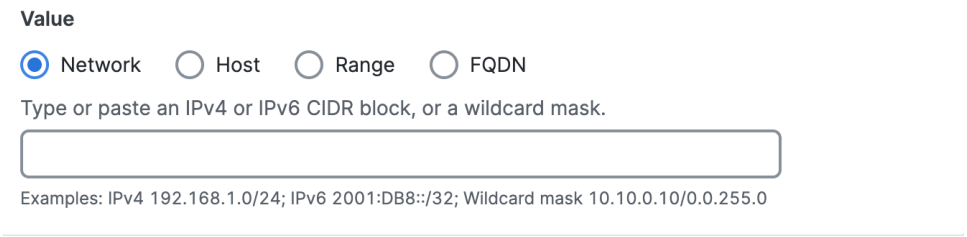
   b) Option 2: Navigate to **Network Objects and Network Object Groups** > **Network Objects**, and then click **Add network object**.



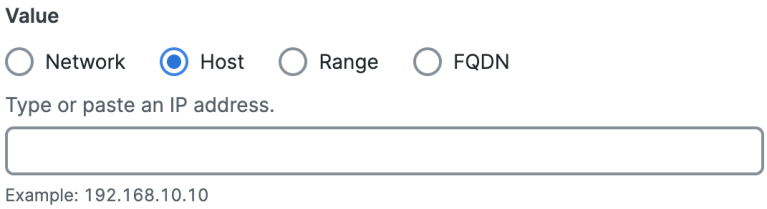
4. On **Add Network Object**, add a name and description for the network object.
   a) For **Network Object Name**, enter a unique name for the network object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters for the name of the network object.
   b) (Optional) For **Description**, enter text that describes the network object.
5. Navigate to **Object values**.
6. For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

   You must choose the type of the Network Object and enter the IP address information.

   a) Click **Network**, and then enter a IPv4 CIDR block, IPv6 address, or Wildcard mask.

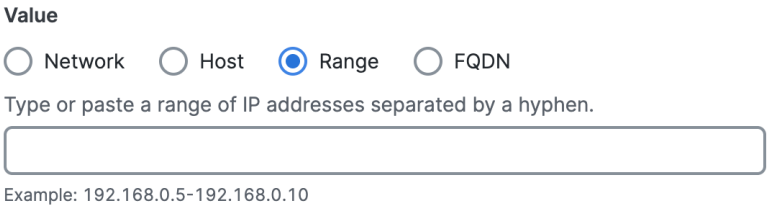


b) Click **Host**, and then enter an IPv4 address.

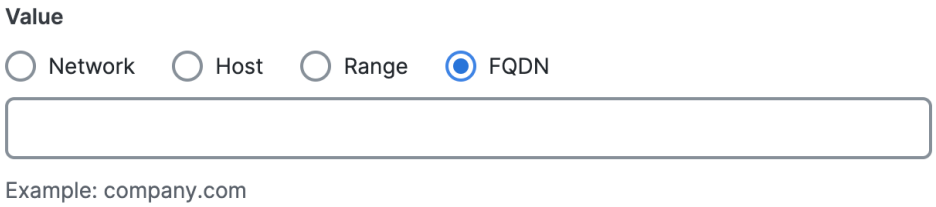


c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (-).

For example: **192.168.0.0-192.168.0.10**.

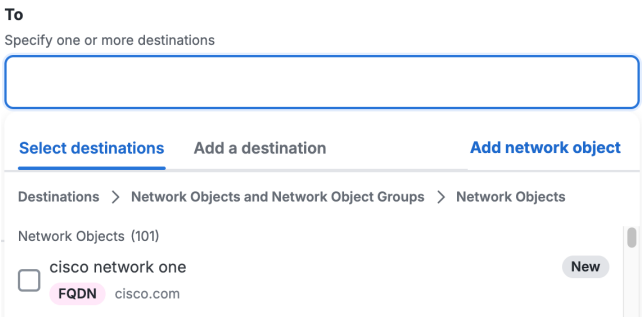


d) Click **FQDN**, and then enter a fully-qualified domain name (FQDN).



7. Click **Add network object**.

Secure Access displays the object with the **New** label in the list of Network Objects.



Edit Network Objects on Rules

Provides instructions for completing the Edit Network Objects on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit the properties of a reusable network object directly on internet rules in the Access policy.

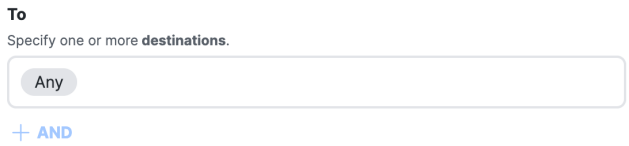
> **Note**
>
> If an VPN profile references a network object, you cannot edit the network object.

Before you begin

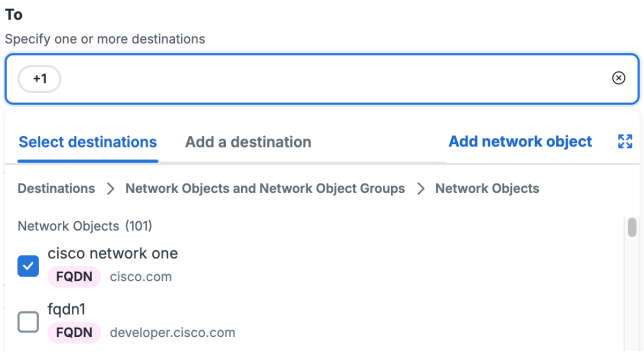
- Full Admin user role. For more information, see Manage Accounts.

Procedure

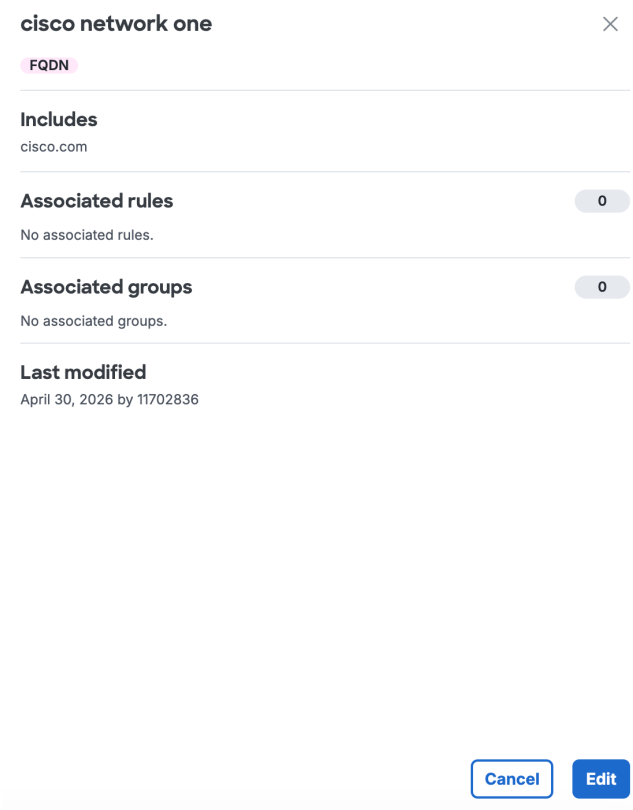
1. Navigate to **Secure** > **Access Policy** .
   a) To modify the settings on an access rule, navigate to a row in the rules table, and either click on the name of rule or click on the ellipsis (**...**) at the end of the row, and then click **Edit**.
   b) To modify the destinations in an access rule from the **Rule Name** column in the rules table, click on the name of rule in the access rules table, navigate to **Destinations**, and then click **Edit**.
   c) To modify the destinations in an access rule from the **Destinations** column in the rules table, click on a destination or **+[number-of-selected-destinations]**, click **View details** and then click **Edit**.
2. Navigate to **Specify Access** and then navigate to the search bar under **To**.



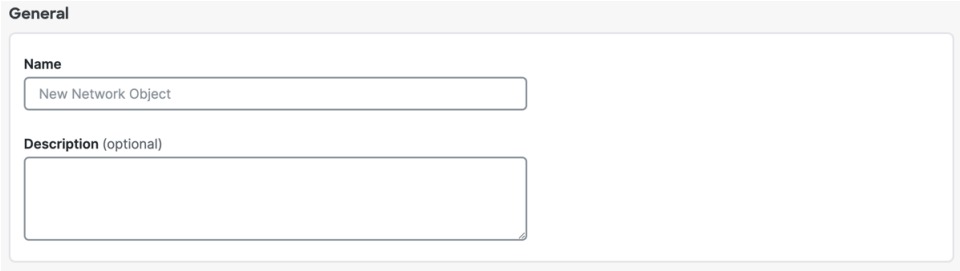
3. Navigate to **Destinations**.



   a) To edit the settings on a reusable network object, click in the blank space in the **Destinations** search bar, navigate to **Select destinations** > **Network Objects and Network Object Groups** > **Network Objects**, click on a network object, and then click **Edit**.

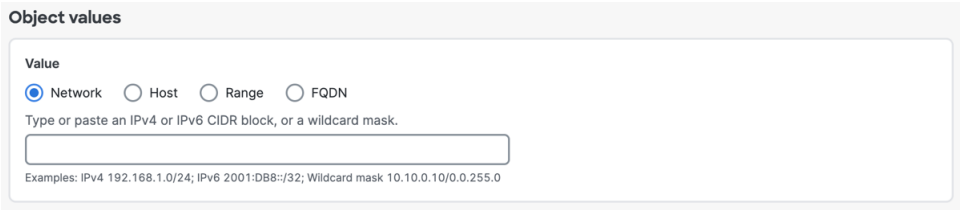


4. In **Edit Network Object**, modify the settings on the network object.



   a) For **Network Object Name**, enter a unique name for the network object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) (Optional) For **Description**, enter text that describes the network object.

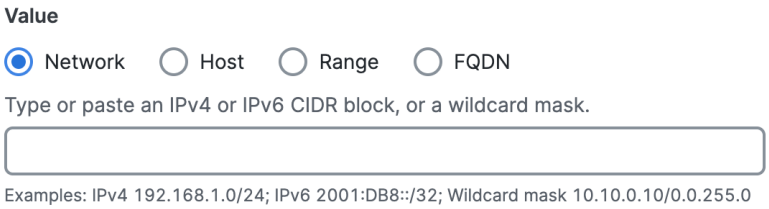
5. Navigate to **Object values**.



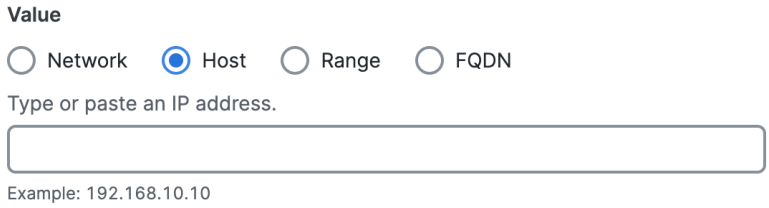
6. For **Value**, choose either **Network**, **Host**, **Range**, or **FQDN**.

> **Note**
>
> You must choose the type of the network object and enter the IP address information.

a) Click **Network**, and then enter an IPv4 CIDR block, IPv6 address, or Wildcard mask.

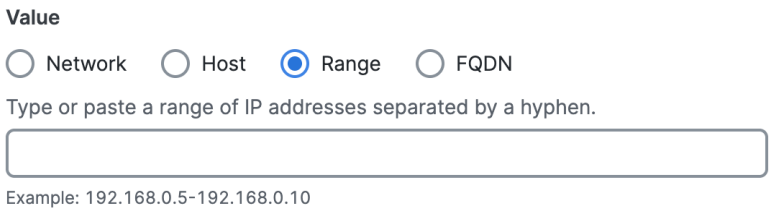


b) Click **Host**, and then enter an IPv4 address.

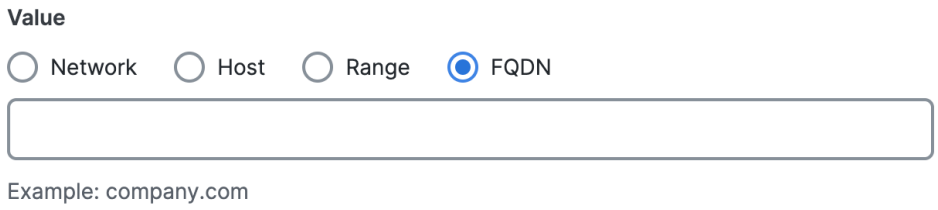


c) Click **Range**, and then enter a range of IPv4 addresses separated by a hyphen (**-**).

For example: **192.168.0.0-192.168.0.10**.



d) Click **FQDN**, and then enter a fully-qualified domain name (FQDN).



7. Click **Save**.

Add Reusable Service Objects on Rules

Provides instructions for completing the Add Reusable Service Objects on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can add a reusable Service Object resource for the destination component on the internet access rules in the Access policy. A Service Object represents a port, range of ports, specific protocols, or any protocols of a service.

Before you begin

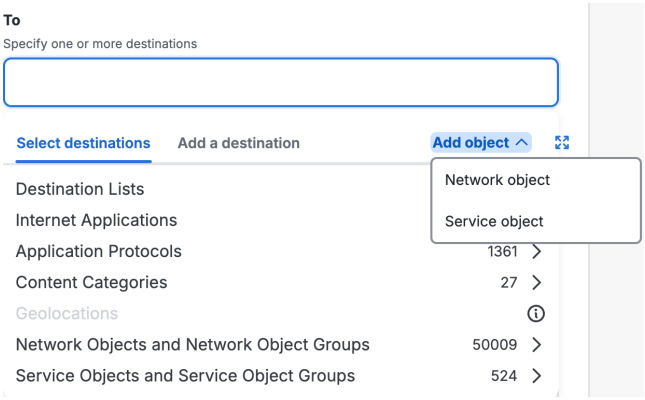
- Full Admin user role. For more information, see Manage Accounts.

Procedure

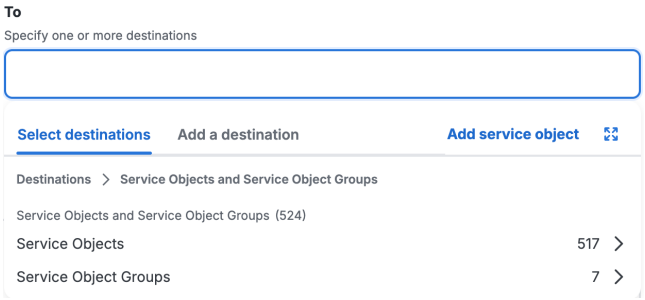
1. Navigate to **Secure** > **Access Policy**.
   a) To add a service object on a new access rule, click **Add Rule** > **Internet Access**.
   b) To add a service object on an existing access rule, click on the name of rule in the access rules table and then click **Edit**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



3. Navigate to **Select destinations**.
   a) Option 1: Click in the search bar for a network or service object, click **Add object**, and then choose **Service object**.



   b) Option 2: Navigate to **Service Objects and Service Object Groups** > **Service Objects**, and then click **Add service object**.



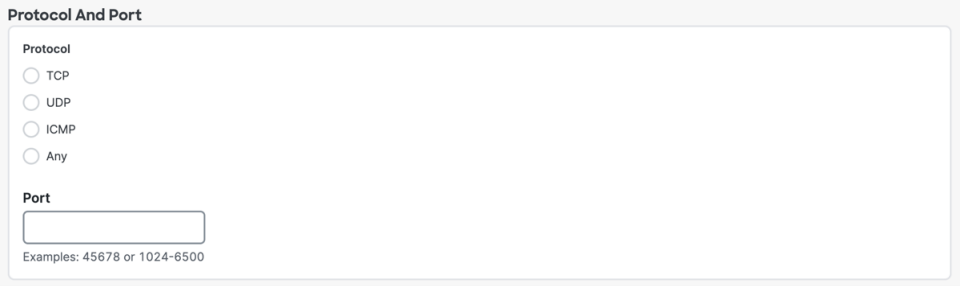
4. On **Add Service Object**, add a name and description for the service object.
   a) For **Service Object Name**, enter a unique name for the service object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters for the name of the service object.
   b) (Optional) For **Description**, enter text that describes the service object.
5. Navigate to **Protocol And Port**.

a) For **Protocol**, choose a protocol for the service object.

> **Note**
>
> Select **Any** to add any protocols for the service object.

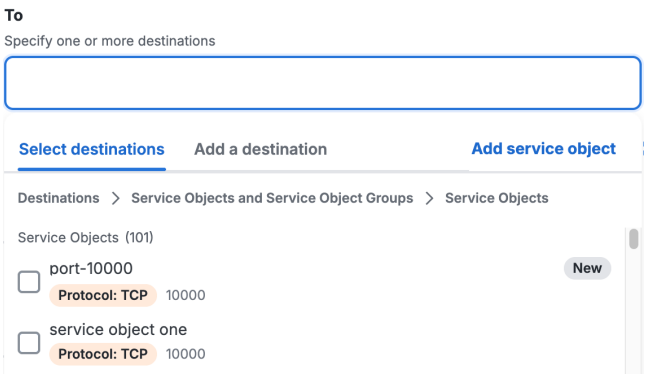
b) For **Port**, enter a port or range of ports.

Separate the range of ports with a hyphen (-), for example, **1024-6500**.



6. Click **Add service object**.

Secure Access displays the object with the **New** label in the list of Service Objects.



Edit Service Objects on Rules

Provides instructions for completing the Edit Service Objects on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Edit the properties of a reusable service object directly on the internet rules in the Access policy.

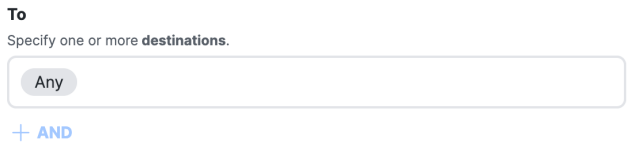
> **Note**
>
> If an VPN profile references a service object, you cannot edit the service object.

Before you begin

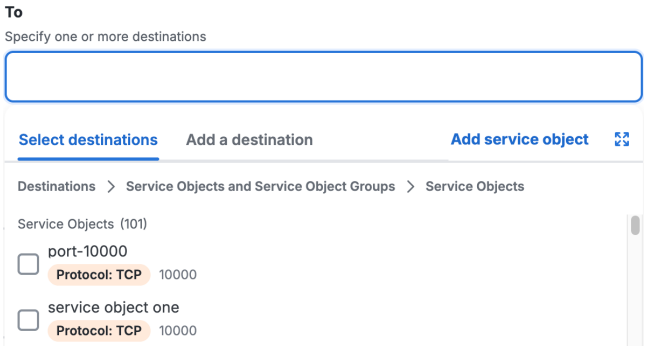
- Full Admin user role. For more information, see Manage Accounts.

Procedure

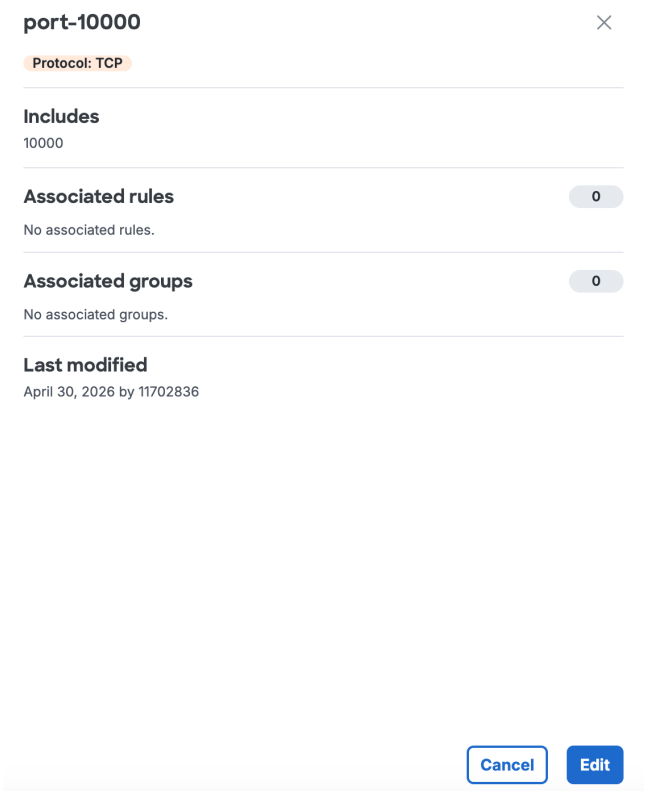
1. Navigate to **Secure** > **Access Policy**.
   a) To modify the settings on an access rule, navigate to a row in the rules table, and either click on the name of rule or click on the ellipsis (**...**) at the end of the row, and then click **Edit**.
   b) To modify the destinations in an access rule from the **Rule Name** column in the rules table, click on the name of rule in the access rules table, navigate to **Destinations**, and then click **Edit**.
   c) To modify the destinations in an access rule from the **Destinations** column in the rules table, click on a destination or **+[number-of-selected-destinations]**, click **View details** and then click **Edit**.
2. Navigate to **Specify Access** and then navigate to the search bar under **To**.



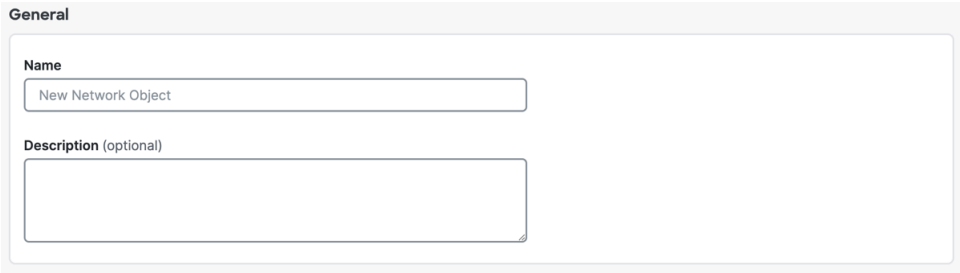
3. Navigate to **Destinations**.



   a) To edit the settings on a reusable service object, click in the blank space in the **Destinations** search bar, navigate to **Select destinations** > **Service Objects and Service Object Groups** > **Service Objects**, click on a service object, and then click **Edit**.



4. In **Edit Service Object**, modify the settings for the service object.



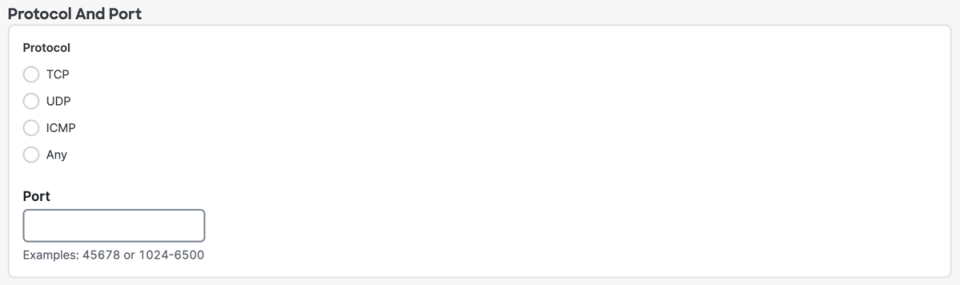
   a) For **Service Object Name**, enter a unique name for the service object. Secure Access supports a sequence of 1-255 alphanumeric, space, hyphen, and underscore characters.
   b) (Optional) For **Description**, enter text that describes the service object.

5. Navigate to **Protocol And Port**.
   a) For **Protocol**, choose a protocol for the service object.

> **Note**
>
> Select **Any** to add any protocols for the service object.

   b) For **Port**, enter a port or range of ports.

      Separate the range of ports with a hyphen (**-**), for example, **1024-6500**.



6. Click **Save**.

Add Composite Destinations on Rules

Provides instructions for completing the Add Composite Destinations on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can add a composite destination directly on an access rule in your Access policy. Compose destinations on a rule by entering network addresses, protocols, ports and port ranges. Destinations that you enter directly on a rule are not reusable components. For more information, see About Configuring Destinations for Internet Access Rules.

After you add destinations on an access rule, you can remove or modify the destinations. For more information, see Edit Composite Destinations on Rules.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

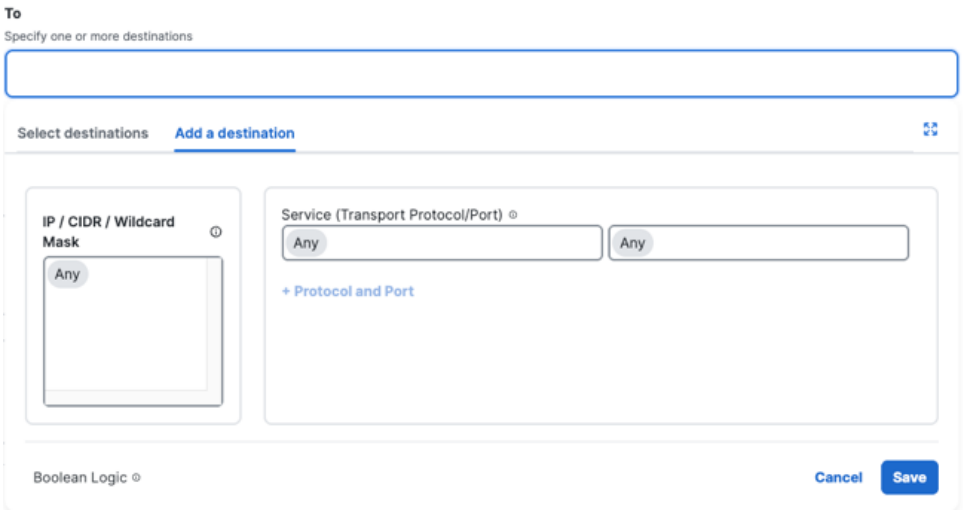
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. Click **Add a destination**.
   a) For **IP, CIDR, or Wildcard Mask**, enter an IPv4 address or CIDR block, or IPv4 address with wildcard mask.

      For example:

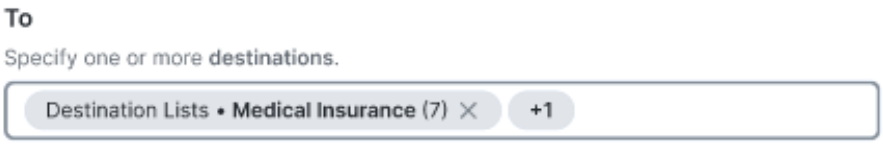
      - IPv4 address–**1.2.3.4**
      - CIDR block–**1.2.3.4/24**
      - Wildcard mask–**1.2.3.4/255.255.255.255**

        For **Wildcard Mask**, use the syntax: `<IP address>/<Wildcard Mask>`. For information about wildcard masks, see Using Wildcard Masks on Internet Rules .

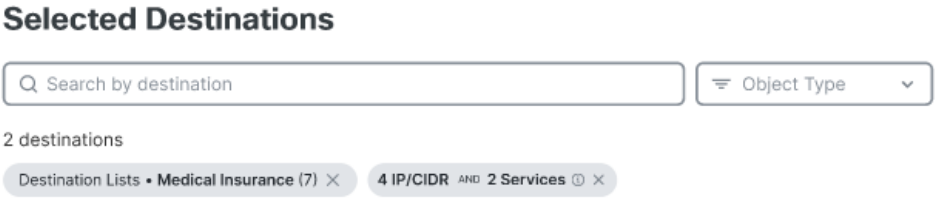
   b) For **Protocol**, choose from one of the supported protocols: **ANY**, **TCP**, **UDP**, or **ICMP**.
   c) For **Port/Port Range**, enter a port or range of ports separated by a hyphen (**-**).
   d) Click **+Protocol and Ports** to add a protocol, port or range of ports separated by a hyphen (**-**) and repeat this step to enter additional protocols and ports on the rule.
   e) Click **Save** to confirm the addition of the composite destination.



4. (Optional) After you add destinations on the access rule, you can view the selected destinations. In the **To** search bar, click on the selected destinations.



5. Click on the set of composite destinations.



6. After you view the selected destinations, click **Close**.

Edit Composite Destinations on Rules

Provides instructions for completing the Edit Composite Destinations on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add composite destinations on an access rule, you can modify or remove the destination directly on the rule.

Destinations that you enter directly on a rule are not reusable components. For more information, see About Configuring Destinations for Internet Access Rules.

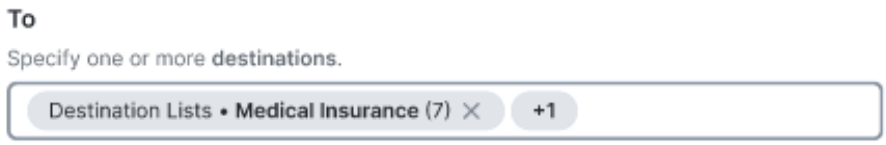
For a composite destination entered on a rule, you can deselect the entries in a component, remove an entire component, enter additional entries in a component, or add new components in a composite destination.

Before you begin

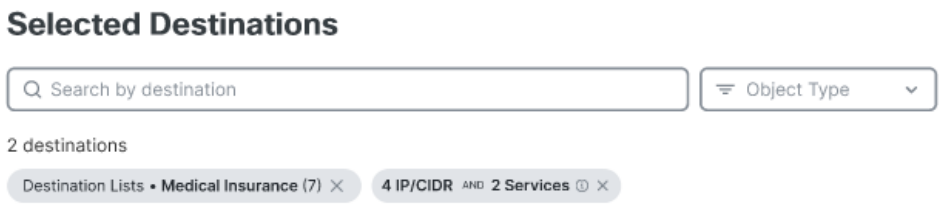
- Full Admin user role. For more information, see Manage Accounts.

Procedure

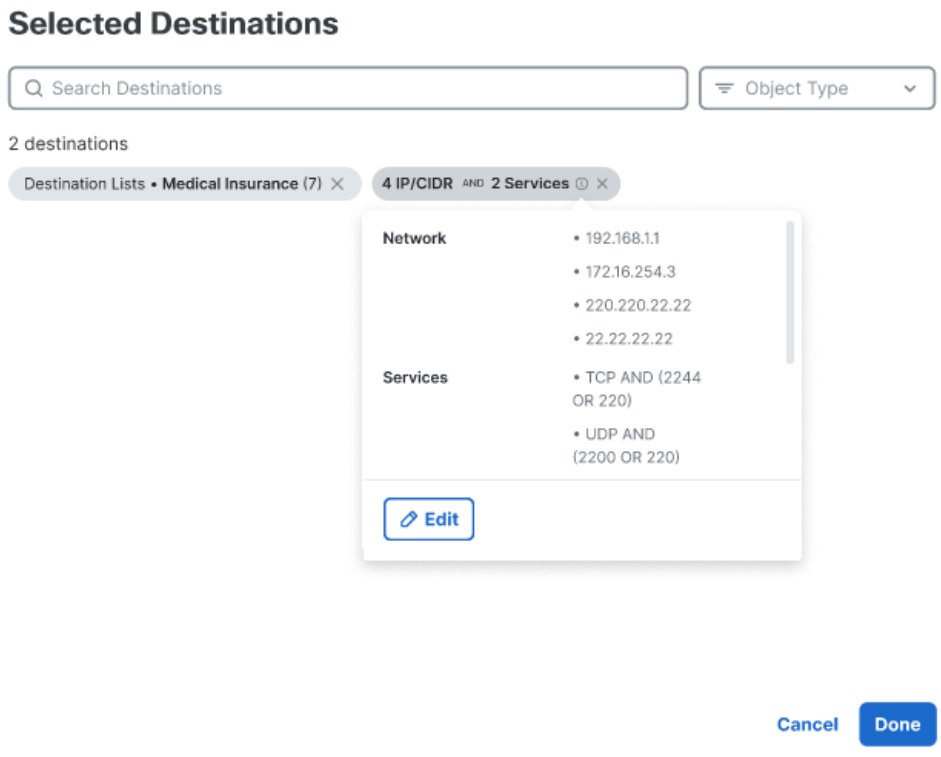
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access**, and then navigate to the search bar under **To**.
3. Click on the selected destinations.



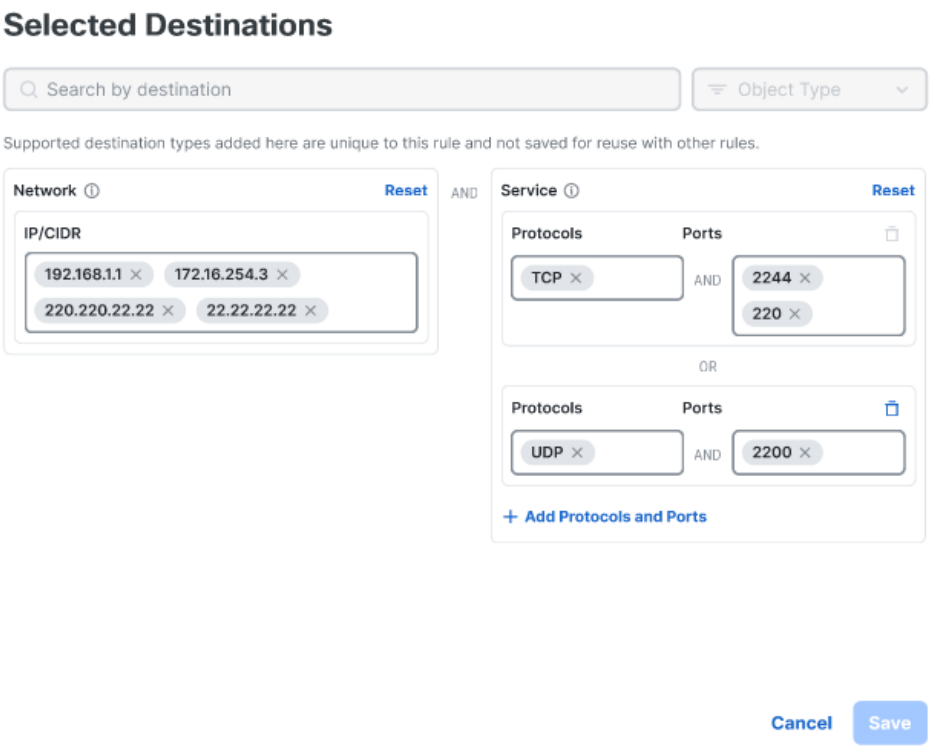
4. Click on the set of reusable destinations or click on the set of composite destinations.



5. You can view the selected destinations, then click **Close**.
6. To remove a reusable destination or an entire composite destination, click on the **X** next to the destination.
7. To modify the Network and Services composite destinations, click **Edit**.



   a) Click **Reset** to revert to the last saved state of the component on the composite destination.



b) Click on an **X** next to an entry to remove the entry in a destination component.
c) Click on a **trash can** (delete icon) to remove an entire set of entries.
d) Click **+Protocol and Ports** to add a protocol, port or range of ports separated by a hyphen (**-**). Repeat this step to enter additional protocols and ports on the rule.
e) Click **Save** to confirm the Network and Service components on the composite destination.

8. To confirm the selected destinations, click **Done**.

Select Application Protocols with Composite Destinations on Rules

Provides instructions for completing the Select Application Protocols with Composite Destinations on Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select application protocols on a internet rule. Once you add the application protocols, click **+AND** to add composite destinations with the application protocols on the internet access rule in the Access policy.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

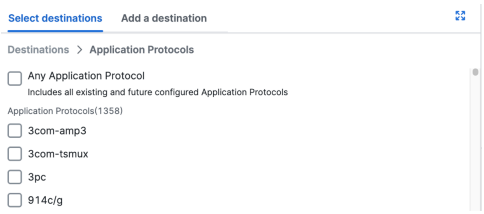
Procedure

---

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Internet Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



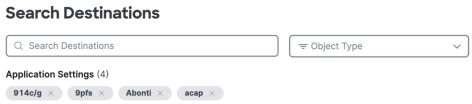
3. Click **Select destinations**, expand **Application Protocols**, and then select the application protocols to add to the internet rule.



4. Click **+More** to view the added application protocols.



5. View or search for the added application protocols.



6. (Optional) Click **+AND**, and then click on the **Select destinations** text area.

   Add composite destinations with Services (Transport protocols, and ports or port ranges) and combine with the application protocols that you added on the rule using the AND operator.

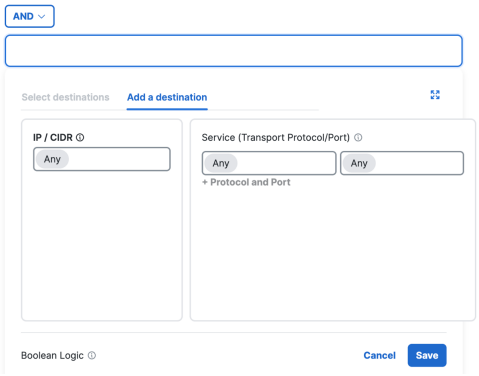
   a) Add IP addresses and CIDR blocks.

      Type or paste a comma-separated list of IPv4 addresses, IPv6 addresses, and CIDR blocks. For example: `192.168.1.1, 192.168.1.0/24, fd00:b0fc:8844:3345:186a:6fd7:bab:5f72`.

   b) Add Services.

      Select transport protocols or **Any**, and enter a comma-separated list of ports or port ranges.

      Example port ranges and lists of ports: `7800-7805, 7800, 8900, 9006`.



7. Click **Save**.

How Application Protocols Combine with Composite Destinations

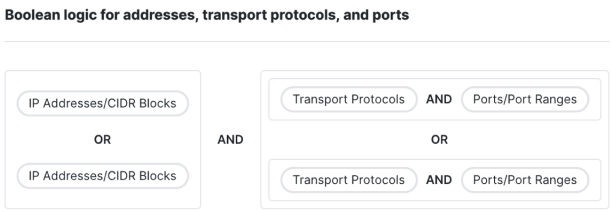
Describes How Application Protocols Combine with Composite Destinations in Cisco Secure Access. You can select application protocols on internet access rules in the Access policy.

You can select application protocols on internet access rules in the Access policy. Secure Access provides the option to add the logical AND operator on the rule with the application protocols and then add composite destinations. Composite

destinations are network addresses, transport protocols, ports and port ranges entered directly on an internet access rule.

Secure Access does not support selecting application lists, application categories, content categories, or destination lists combined with composite destinations.

Secure Access uses boolean logic to combine the composite destinations on a rule with Services. Services are groups of transport protocols and port or port ranges.



- First, Secure Access combines the individual network addresses (IP addresses or CIDR blocks) together with the OR operator.
- Next, Secure Access combines each set of selected Service components together with the AND operator. Transport protocols are ANDed with the ports or port ranges.
- Next, Secure Access combines the Services together with the OR operator.
- Then, Secure Access combines the set of composite destinations with the set of Services using the AND operator.

App Risk Profiles

Describes App Risk Profiles in Cisco Secure Access. If for Destination you have selected Any Internet Destination or a destination that includes an internet application, you will see the App Risk Profile section.

If for Destination you have selected Any Internet Destination or a destination that includes an internet application, you will see the App Risk Profile section. For more information, see App Risk Profile.

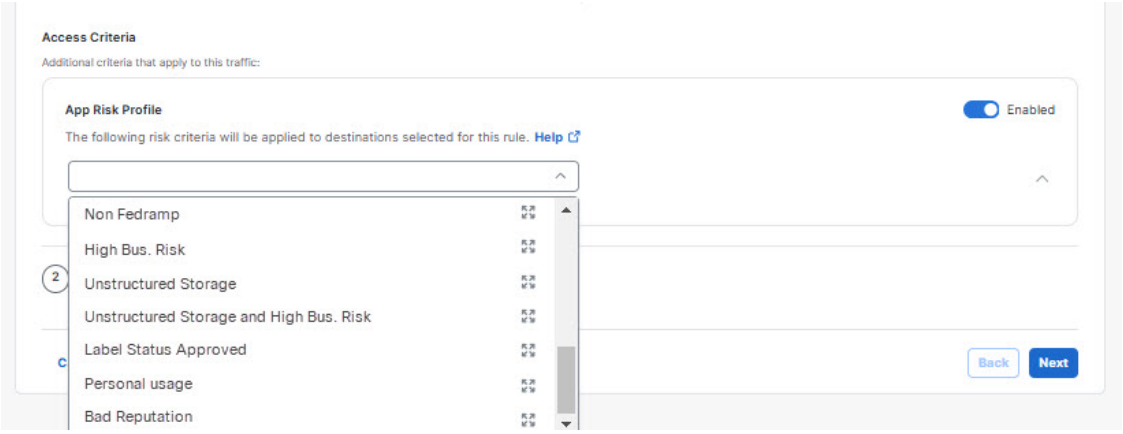
Once you create an App Risk profile, you may choose the profile to add the criteria it defines to your rule.

To incorporate an app risk profile in this rule:

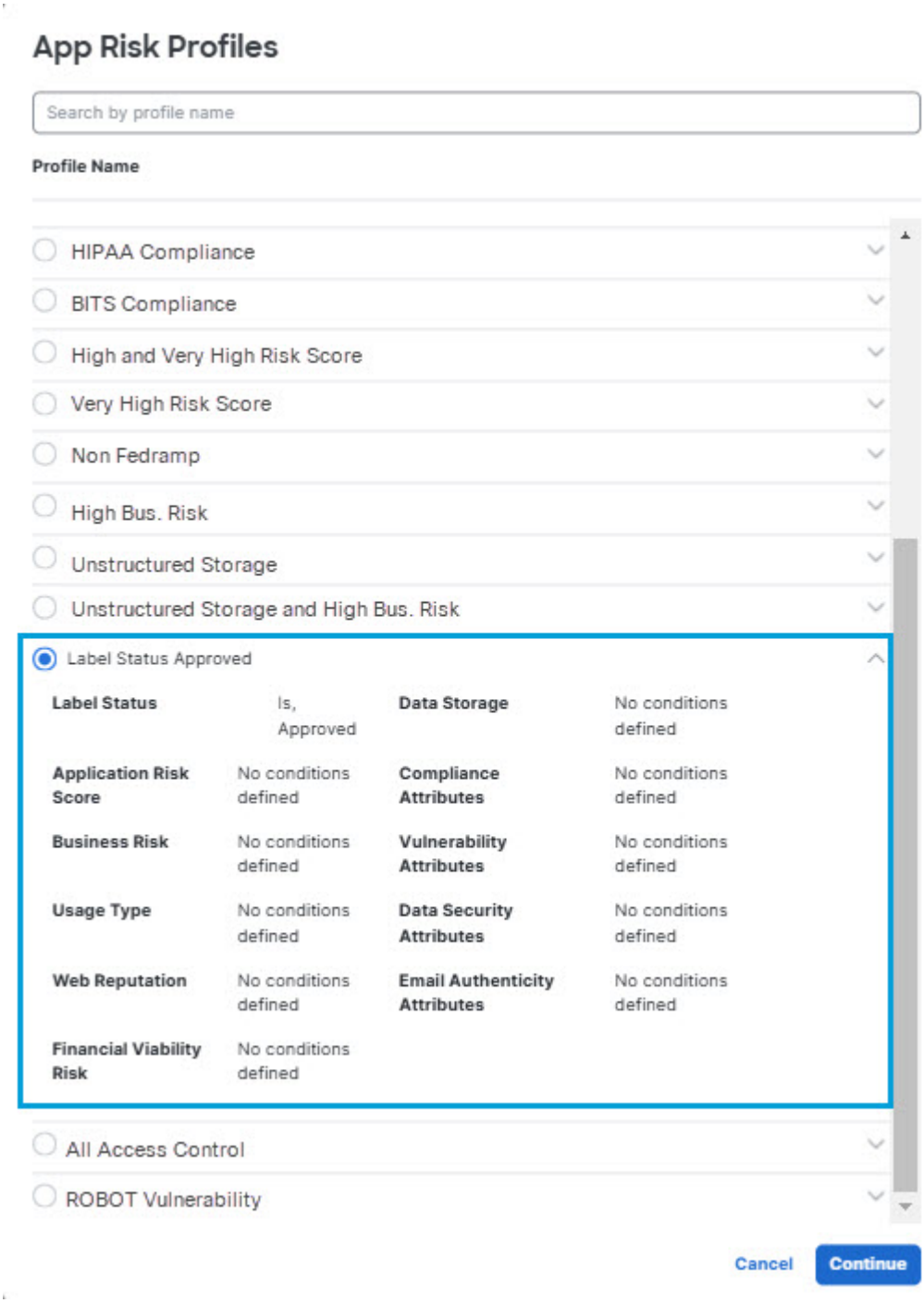
1. Click the toggle to the right of **App Risk Profile** to enable the feature.



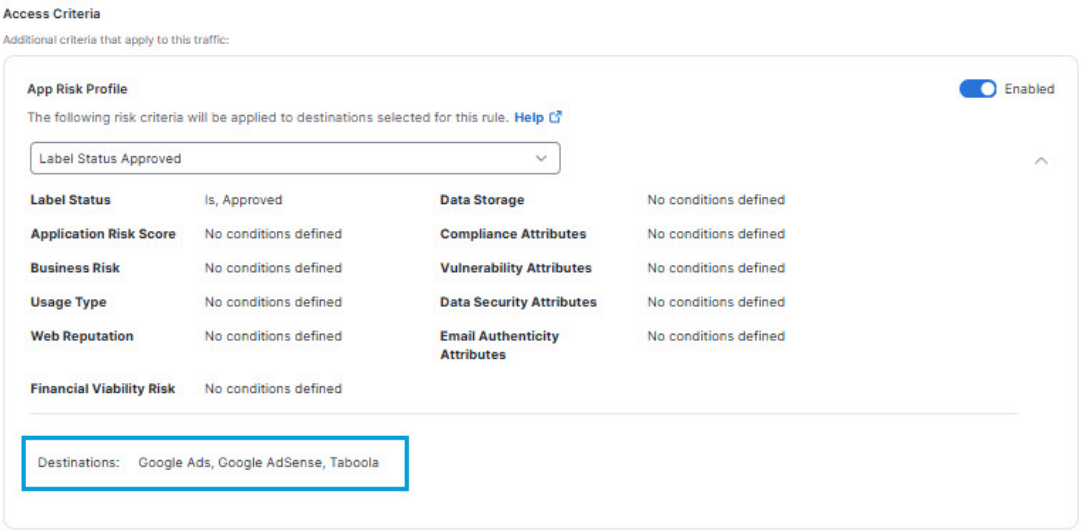
2. From the **Select profile** drop-down list, click on the name of an app risk profile to apply it to this rule.


Access Criteria
Additional criteria that apply to this traffic:
App Risk Profile
Enabled
The following risk criteria will be applied to destinations selected for this rule. Help
Non Fedramp
High Bus. Risk
Unstructured Storage
Unstructured Storage and High Bus. Risk
Label Status Approved
Personal usage
Bad Reputation
2
Back
Next

> **Tip**
>
> Alternatively, you may click the expand icon to the right of an app risk profile name to display a dialog showing the risk criteria it defines. Then click **Cancel** to dismiss the dialog, or click **Continue** to select the profile.



Once you select an app risk profile, a summary of the risk criteria the profile applies to your rule appears. Below it, a list of Destinations that match the profile appears. This list reflects the restriction the app risk profile places on the list of destinations you selected for the rule.



Advanced Application Controls

Describes Advanced Application Controls in Cisco Secure Access. Some web-based applications offer the option to allow users to access the site but not to perform activities such as uploading, downloading, posting, or sharing content on those sites.

Some web-based applications offer the option to allow users to access the site but not to perform activities such as uploading, downloading, posting, or sharing content on those sites.

Depending on the destinations you select in an internet access rule, you will see an Advanced Application Controls section.

This section appears only if destinations added to the rule include one or more applications that allow granular controls on activities. These applications must be included in application lists selected as destinations, or be individual applications selected from application categories.

For example:

- Configured destinations that include applications selected from Application Categories that support the ability to control uploads, downloads, posting, or sharing without entirely blocking access to the application.
- Application lists that include such applications.

Use these advanced controls if you want to allow access to the site but block certain actions. If you don't want to allow access to the site at all, select the application or application list in the destination list for the rule.

> **Note**
>
> Advanced controls for these applications have no impact in “Block,” “Warn,” or “Isolate” rules.

Applications with Advanced Controls

Describes Applications with Advanced Controls in Cisco Secure Access. If apps have advanced app controls, you can block all content for the app, block the app from uploading content including posts and shares, block the app from downloading content, or block the app from deleting content.

If apps have advanced app controls, you can block all content for the app, block the app from uploading content including posts and shares, block the app from downloading content, or block the app from deleting content.

> **Note**
>
> Be aware that the support status of each application list may change without prior notice due to specification changes implemented by the SaaS vendor.

> **Note**
>
> Both "posting" and "sharing" refer to exposing information to other accounts within the same application. Some applications refer to this action as "posting," and some refer to it as "sharing."

- Cloud Storage
- Collaboration on page 910
- Content Management on page 910
- Media on page 911
- Office Productivity on page 911
- P2P on page 911
- Social Networking on page 912

Cloud Storage

Describes Cloud Storage in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Applications	Category	Upload	Download	Post/Share	Delete
Box Cloud Storage	Cloud Storage	Yes	Yes	Yes	Yes
Dropbox	Cloud Storage	Yes	Yes	Yes	Yes
Flickr	Cloud Storage	Yes	Yes		
File Dropper	Cloud Storage	Yes			
GrosFichiers	Cloud Storage	Yes	Yes	Yes	Yes
Google Drive	Cloud Storage	Yes	Yes		Yes
Leap File	Cloud Storage	Yes	Yes		Yes
MediaFire	Cloud Storage	Yes	Yes	Yes	Yes
Microsoft OneDrive	Cloud Storage	Yes	Yes	Yes	Yes
OpenDrive	Cloud Storage	Yes			
Onehub	Cloud Storage	Yes			
PicDrop	Cloud Storage	Yes	Yes	Yes	Yes
SendThisFile	Cloud Storage	Yes	Yes		Yes
SmugMug	Cloud Storage	Yes	Yes		Yes

Applications	Category	Upload	Download	Post/Share	Delete
SlideShare	Cloud Storage	Yes	Yes		Yes
4shared	Cloud Storage	Yes	Yes		Yes

Collaboration

Describes Collaboration in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Applications	Category	Upload	Download	Post/Share	Delete	AI Mode	Notes
Cisco Webex Teams	Collaboration		Yes	Yes	Yes		
Microsoft Teams	Collaboration	Yes	Yes	Yes	Yes		
Google	Collaboration					Yes	AI Overview as part of Google Search cannot be blocked.
Gyazo Teams	Collaboration	Yes	Yes	Yes	Yes		
Slack	Collaboration	Yes	Yes	Yes	Yes		
WhatsApp	Collaboration	Yes	Yes				If you upload a Whatsapp file that has already been previously uploaded, Secure Access does block the upload of the file. As a workaround, manually delete the existing version of the file from the Whatsapp servers.

Content Management

Describes Content Management in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Applications	Category	Upload	Download	Post/Share	Delete
Egnyte Connect	Content Management	Yes			

Applications	Category	Upload	Download	Post/Share	Delete
Lucidchart	Content Management	Yes			
Pastebin	Content Management	Yes	Yes		Yes

Media

Describes Media in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Applications	Category	Upload	Download	Post/Share	Delete
Dailymotion	Media	Yes			Yes
Giphy	Media	Yes			
Veoh	Media	Yes			Yes
Vimeo	Media	Yes	Yes		Yes
YouTube	Media	Yes			Yes

Office Productivity

Describes Office Productivity in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Applications	Category	Upload	Download	Post/Share	Delete
Basecamp	Office Productivity	Yes	Yes	Yes	Yes
DocHub	Office Productivity	Yes	Yes	Yes	Yes
AOL Mail	Office Productivity		Yes		
Gmail	Office Productivity	Yes	Yes	Yes	Yes
Mail.ru	Office Productivity	Yes			
Smartsheet	Office Productivity	Yes	Yes	Yes	Yes
Trello	Office Productivity	Yes			Yes
Yandex Mail	Office Productivity	Yes			
Yahoo Mail	Office Productivity	Yes	Yes		Yes

P2P

Describes P2P in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Applications	Category	Upload	Download	Post/Share	Delete
Citrix ShareFile	P2P	Yes			
Filesend	P2P	Yes			
GigaFile	P2P		Yes		
Hightail	P2P	Yes			
WeTransfer	P2P	Yes	Yes		

Applications	Category	Upload	Download	Post/Share	Delete
Wikisend	P2P	Yes			

Social Networking

Describes Social Networking in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Applications	Category	Upload	Download	Post/Share	Delete
Facebook	Social Networking	Yes		Yes	Yes
Facebook Messenger	Social Networking	Yes			
Instagram	Social Networking	Yes		Yes	Yes
LinkedIn	Social Networking	Yes	Yes	Yes	Yes
Pinterest	Social Networking	Yes		Yes	Yes
Tik Tok	Social Networking	Yes	Yes	Yes	Yes
Twitter	Social Networking	Yes		Yes	Yes

Add Advanced Application Controls

Provides instructions for completing the Add Advanced Application Controls workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

When you create or edit an internet access rule, you can add specific applications or application lists as destinations. You can select applications from the Advanced Application Controls tables or use a configured application list.

Before you begin

- Full Admin user rule. For more information, see Manage Accounts.

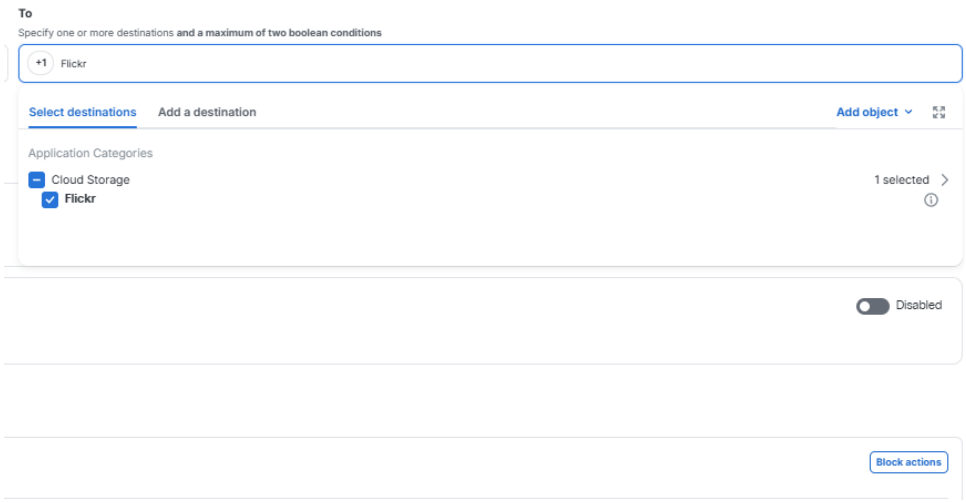
Procedure

1. When creating or editing an internet access rule, enter the application name in the **To** text box, and select the **Application categories** check box.

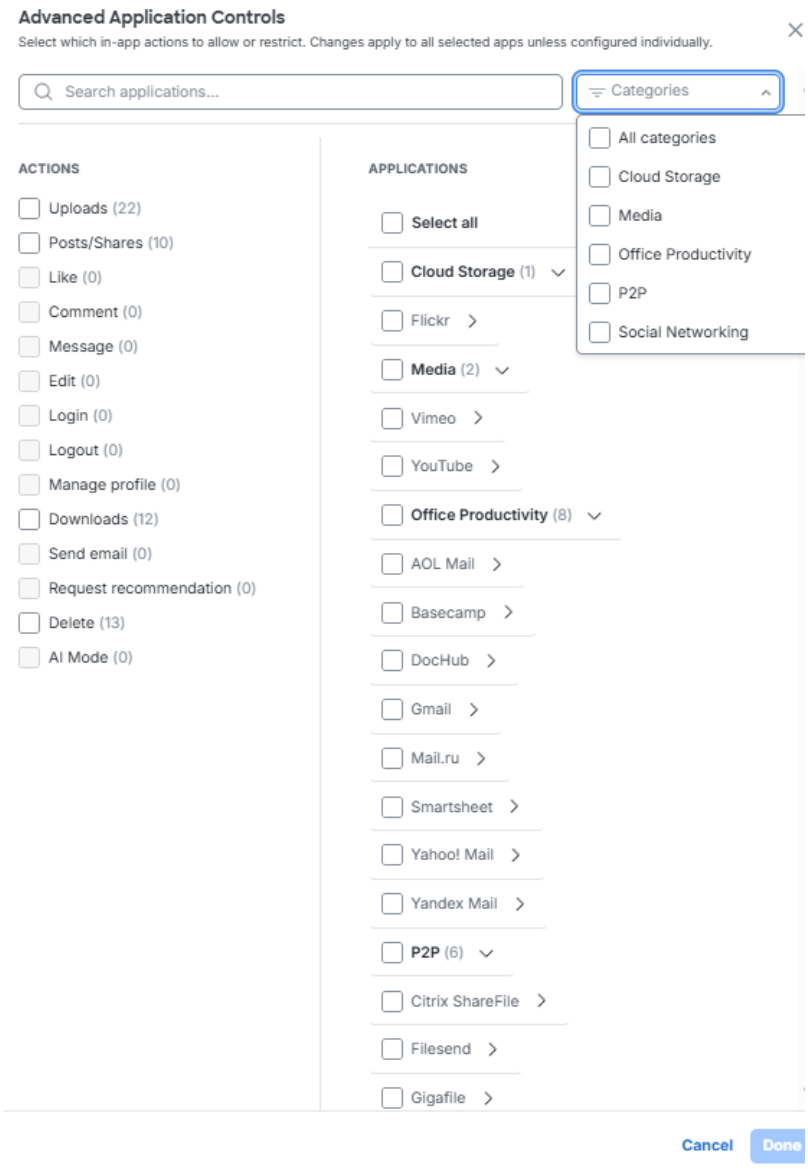
   Note

   You can select all applications or a single application in the **To** text box.

2. Click **Block actions** to restrict specific activities.



3. In the left pane, select the types of actions to block.



4. (Optional) Filter the list in the main pane by clicking **All categories** and choosing a specific category.
5. In the main pane, select the **Activities** to block for each application in the list.
6. (Optional) If you filtered the list, choose a different category, and then select the activities to block for that category. Repeat this process for each category as needed.
7. Click **Done** to apply your changes.

Troubleshooting Advanced Application Controls

Describes Troubleshooting Advanced Application Controls in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

If advanced application control is not working as expected, check the following:

- Decryption must be enabled in the security profile selected in the rule.
- The site must not be on the **Do Not Decrypt** list selected in the security profile.
- The domain—for example, dropbox.com—is not configured for **Bypass Web Proxy** on the **Connect > End User Connectivity> Internet Security** page. Any domains or IPs on this list will bypass Secure Access and be routed by your local DNS server. This list applies to PAC file and AnyConnect deployments.
- When an application is blocked, a web notification page will not be displayed. Instead, an error message will be displayed in the application.

About Configuring Threat Categories on Internet Access Rules

Describes About Configuring Threat Categories on Internet Access Rules in Cisco Secure Access. For internet access rules where the rule action is Isolate, you can add the threat categories for web destinations instead of pre-configured or composite destinations.

For internet access rules where the rule action is **Isolate**, you can add the threat categories for web destinations instead of pre-configured or composite destinations. Secure Access isolates the internet-bound traffic based on the threat categories assigned to the web destinations. For information about the requirements for isolating web traffic in Secure Access, see About Isolated Destinations.

Secure access supports these threat categories for selection on the internet access rules with the **Isolate** action:

- **Malware**
- **Command and Control**
- **Phishing Attacks**
- **Potentially Harmful Domains**

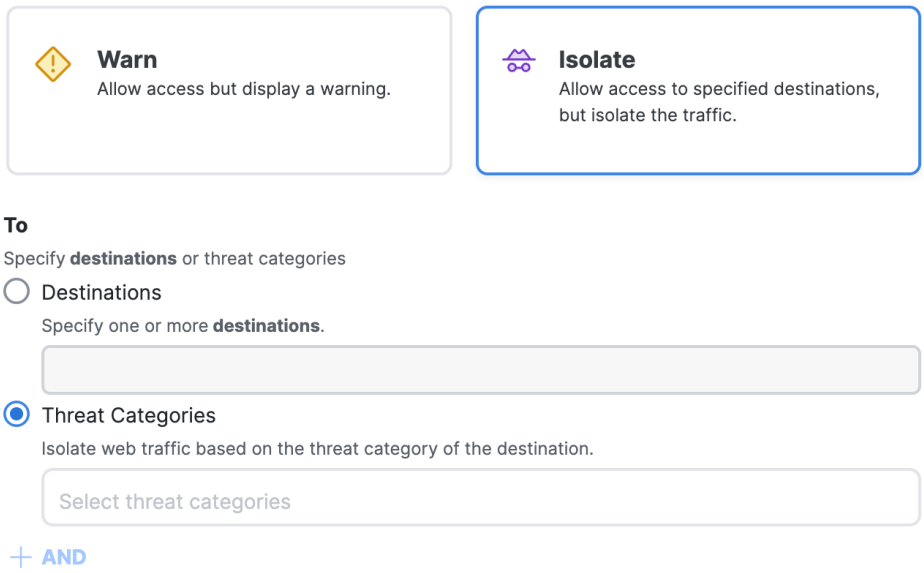
In Secure Access, you can also use a Security profile to add threat categories for internet destinations. After you add the Security profile in the organization, select the Security profile on the internet access rules in the Access policy.

For information about the Secure Access threat categories, see Manage Threat Categories.

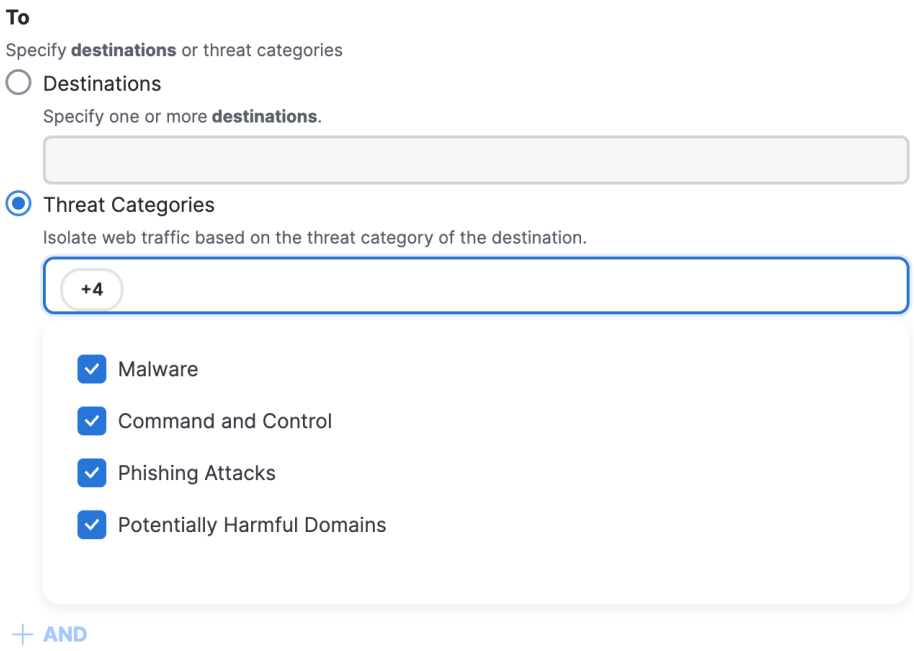
For information about Security profiles, see Manage Security Profiles.

How to Add Threat Categories on Internet Access Rules

1. Navigate to **Secure** > **Access Policy**.
2. Click **Add Rule** > **Internet Access.**.
3. Navigate to **Specify Access**, and then for the rule action click **Isolate**.



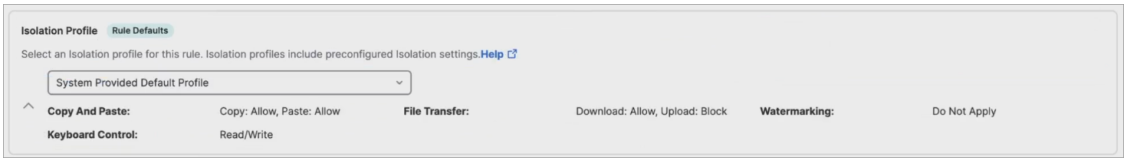
4. For the **To** side of the access rule, click **Threat Categories**.
5. Select the threat categories for the internet access rule.



Isolation Profile Configuration

Describes Isolation Profile Configuration in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

When you select the Isolate action, the Isolation Profile section appears. This allows you to apply specific security controls to the isolated session. In this section you can choose an Isolation Profile from the dropdown menu. The System Default Profile is selected by default. You can search for a profile by name using the search bar within the dropdown.



Once a profile is selected, a summary of its settings (such as watermarking, copy and paste restrictions, and document isolation) is displayed.

Security Control Options

Describes Security Control Options in Cisco Secure Access. Choose the IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule.

Intrusion Prevention (IPS) Profile

Choose the IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule. You can also disable intrusion prevention for this rule.

For more information, see Manage IPS Profiles.

Security Profile

- Choose the security profile that includes the web-related settings that you want applied to traffic that matches this rule.
- For all rules, including Block, Warn, and Isolate rules, unless you have good reason not to, choose a security profile that is configured to decrypt the traffic that will hit the rule. Decryption is required to accurately process traffic to most internet destinations.
  - Best practice: If decryption is disabled in a security profile, or if decryption is enabled only to show notifications, use that profile only in rules that include only trusted destinations.
  - For important information about decryption, see Security Profiles for Internet Access and Manage Traffic Decryption.
- If the rule will block traffic or warn users, you can choose a security profile that specifies the notifications to display to end users.

For more information, see Security Profiles for Internet Access.

Tenant Control Profile

Tenant controls affect access to Microsoft 365, Google G Suite, Slack, and Dropbox.

- For more information, see Manage Tenant Control Profiles.
- For additional requirements, see Use Tenant Controls in Access Rules.

Manage Advanced Security Controls

Provides instructions for completing the Manage Advanced Security Controls workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

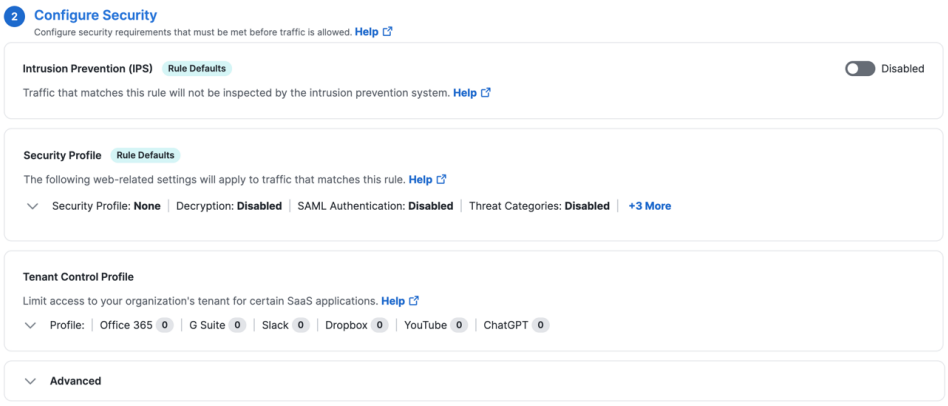
The Advanced Security Controls provides the option to skip the enforcement of certain security features. For example, you may want to disable advanced security controls for trusted destinations permanently or to troubleshoot an issue temporarily. Disable security features only when you have a specific reason to do so.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

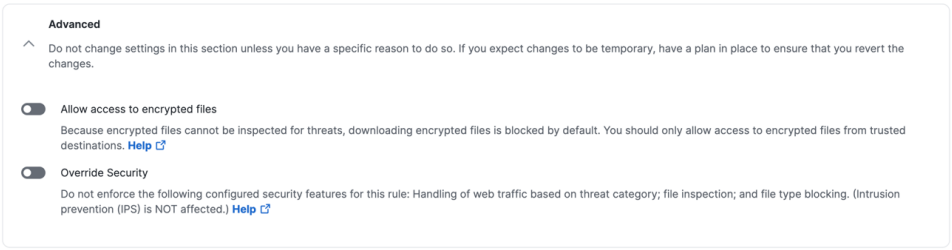
Procedure

1. Follow the general steps to add or edit an internet access rule, then navigate to **Configure Security** > **Advanced**.



   For more information, see Add an Internet Access Rule and Edit an Internet Access Rule.

2. Expand **Advanced** and choose the advanced security controls to enable on the internet access rule.



   a) Toggle on the **Allow access to encrypted files** option.

      When you enable the **Allow access to encrypted files**, Secure Access allows end users to access files that are encrypted.

      Because the system cannot inspect encrypted files for threats, the default setting is block downloads of encrypted files. You should only allow access to encrypted files from trusted destinations.

   b) To prevent Secure Access from applying threat category enforcement, file inspection, and file type control to traffic that matches the rule, turn on **Override Security**.

      The security override applies only to Secure Web Gateway controls.

Geolocation Sources and Internet Access Rules

Describes Geolocation Sources and Internet Access Rules in Cisco Secure Access. Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions.

Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions. The Geolocation source component is available on the internet and private access rules in the Access policy.

The Geolocation source component is a list of continents and the countries in these continents where Secure Access can manage the network traffic sent from these geographic locations.

> **Note**
>
> DNS resolution does not is not supported in source based geolocation policies. The geolocation source of a DNS lookup is not an indicator of where content is being delivered and as such source based geolocation checks and matches are enforced at other enforcement layers as part of unified policy based on your policy configuration.

You can select the Geolocation sources with the AD Users or AD Groups or only add the Geolocations on the access rules. Administrators of the organization are responsible for provisioning the AD Users and AD Groups. For more information, see Provision Users, Groups, and Endpoint Devices from Active Directory.

When you select the Geolocations on an access rule, Secure Access shows the AND option and the AD Users or AD Groups. When you select the AD Users and AD Groups for the source on an access rule, Secure Access shows the AND option and the list of continents and countries. Secure Access combines the selected AD Users or AD Groups and the geolocations with the boolean AND operator. You can only combine the Geolocation source component with the AD Users or AD Groups.

Monitoring Internet Traffic from Geolocations

Set up the attributes and conditions on the access rules in the Access policy to monitor and protect the network traffic from the end users located in specific geographic regions. To enforce the security controls on a rule, the network traffic must match the selected sources.

> **Note**
>
> Secure Internet Access (SIA) in Cisco Secure Access, policy enforcement passes through Zero Trust Access (ZTA) or through the firewall/secure gateway (SGW) depending on the traffic type and configuration; traffic is then tunneled to and inspected by the firewall.

For internet access rules, choose to allow or block all traffic from the geolocations or all traffic from the selected AD Users or AD Groups located in the countries and continents.

- The SWG detects and enforces the web traffic (TCP/80, TCP/443) sent from the end users located in the selected continents and countries.
- The Secure Access cloud-delivered firewall detects and enforces the network traffic on non-standard web ports sent from the end users located in the selected continents and countries.
- For internet traffic on Zero Trust Access connections, the Secure Access cloud-delivered firewall and Secure Web Gateway detects and enforces the traffic.

You can view the events and logs recorded by Secure Access for the traffic sent from the end users in the organization in certain geolocations. Secure Access reports on the traffic on standard web ports and non-web ports. For more information, see:

- View the Events Report
- Activity Search Reports: Filter by Firewall Requests
- Activity Search Reports: Filter by Web Requests

Sources

Describes Sources in Cisco Secure Access and outlines About Selecting Sources on an Access Rule and Number of Sources Supported in a Rule. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Sources on internet rules are either pre-configured, Geolocations, or composite components.

Pre-configured source components such as Registered Networks and Network Tunnel Groups acquire and manage the web traffic in your organization. For information about pre-configured source components, see Reusable Sources in Internet Access Rules.

Composite sources may include IP addresses, CIDR blocks, and wildcard masks, and ports and port ranges. For information about composite source components, see Composite Sources in Internet Access Rules.

About Selecting Sources on an Access Rule

If you select Network Tunnel Groups, Secure Access secures and controls the traffic access from the IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and look at the group configuration.

If you select a Network Tunnel Group, the destination also includes IP addresses configured in the network tunnel group for routing, in addition to all associated Internal Networks. IP addresses include routes advertised using Border Gateway Protocol, if that option is selected in the network tunnel group configuration.

If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in future.

Number of Sources Supported in a Rule

You can add up to 250 sources in an internet access rule. The total number of sources accepted in an access rule includes both pre-configured sources (resources) and sources that you enter directly on an access rule (composite sources).

You can add at most 10 composite sources in an internet access rule.

Add Geolocation Sources on Internet Access Rules

Provides instructions for completing the Add Geolocation Sources on Internet Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select Geolocation sources only on access rules or combine the Geolocation sources with AD Users or AD Groups using the boolean AND operator.

- Add the Geolocation sources on the access rule, select the AND button, and then choose the AD Users and Groups.
- Add pre-configured AD Users and Groups on the access rule, select the AND button, and then choose the Geolocation sources.

For information about Geolocation sources, see Geolocation Sources and Internet Access Rules. For information about AD Users and AD Groups, see Manage Users, Groups, and Endpoint Devices on page 581 .

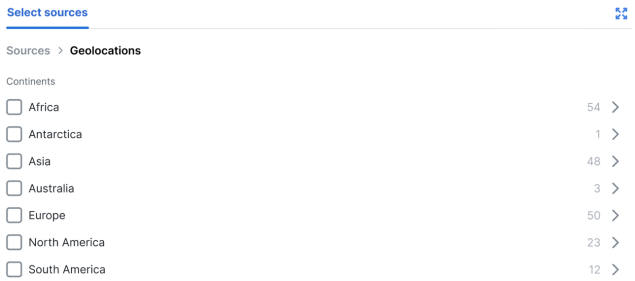
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Navigate to the rules table and choose an existing access rule to edit, or add a new access rule in the Access policy.

3. Navigate to **Specify Access** and then navigate to **From**.
4. Navigate to **Select sources** > **Geolocations**, choose a continent, which selects all countries in the continent, or choose the countries in each continent.



5. (Optional) Click **+ AND** and then add the AD Users or AD Groups.
   a) Navigate to **Select sources**, and then expand **Users** or **Groups**.
   b) Expand **Users**, and then select **AD Users** or select **Any AD Users**.



   c) Expand **Groups**, and then select **AD Groups** or select **Any AD Groups**.

View Events Report

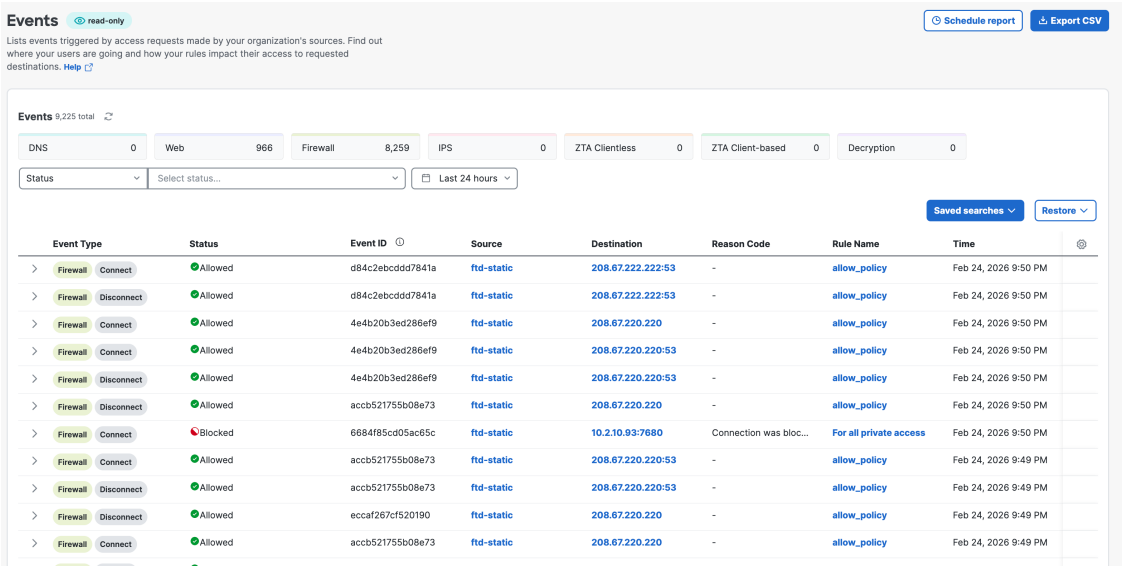
Provides instructions for completing the View Events Report workflow in Cisco Secure Access. Use the Events report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment.

Use the **Events** report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment. The Events report is a comprehensive record of event types, statuses, source and destination details, rule information, and reasons for actions. The Events reports helps you troubleshoot issues, verify policy enforcement, and adhere to compliance requirements.

Procedure

1. Navigate to **Monitor** > **Reports** > **Events**.
2. Choose a time frame.

   You can view events over the **Last 15 minutes**, **Last 30 minutes**, **Last 1 hour**, **Last 4 hours**, **Last 12 hours**, **Last 24 hours** (default), **Last 7 Days**, **Last 30 Days**, or a **Custom range**.



For firewall events, the report displays both **Connect** and **Disconnect** actions. A **Connect** event indicates the start of a connection, recorded at the TCP handshake, where application details are typically not yet known by the Firewall. A **Disconnect** event signifies the close of the session, often containing more comprehensive, application-specific information.

Specifically for Firewall Disconnect events, the Destination section of the Event Details Card includes the **Session Bytes Sent** and **Session Bytes Received** fields. These fields show the total amount of data sent and received during the firewall session, providing clear visibility into overall data transfer for each connection. This allows you to quickly assess the volume of data exchanged in a session and supports investigations into unusual or suspicious network activity.

The Events Report table displays key information for each event. For a detailed understanding of each event type, including their unique characteristics, specific status values, and relevant behaviors, see Event Type Specific Details.

- **Event Type**: Category of the event, for example, DNS, Web, Firewall.
- **Status**: Action taken (Allowed, Blocked, or Isolated).
- **Event ID**: A unique correlation ID generated for each request received by the policy broker, which is propagated downstream to maintain request tracking across network services.
- The Event ID is linked to the 5-tuple (source IP address, source port, destination IP address, destination port, and protocol) of each flow. This ensures that all the packets in the same flow share the same Event ID. However, if two different flows use the same 5-tuple within a short time, they too could get the same Event ID. This usually happens if a client quickly reuses the same source port for requests to the same destination.
- **Source**: Displays the originating identity for the event. This can be:
  - Source IP address (for network-based traffic).
  - User Identity (for authenticated users).
  - Device IP address (for client-based connections, typically representing the public IP address of the client device).
  - Public IP address of the client device (for ZTNA client-based connections). The ZTNA service also logs a specific ZTNA Device ID (a globally unique identifier) for the client, which is distinct from any IP address and helps identify the specific device regardless of its network location.
- **Destination**: The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and decryption requests.
- **Reason Code**: Cause of a particular event, for example, policy match, threat detected.

- **Rule Name**: The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
- Click a rule name to view the access policy in which the rule is configured. For more information, see Manage the Access Policy.
- **Time**: Date and time at which the event occurred.
- **Settings**: Gear icon to access table display settings, including options to adjust table density and to show or hide columns in the table.

  Column Behavior:

  - **Sorting**: Most columns can be sorted in ascending or descending order by clicking their header. Columns that are sortable will display an arrow icon (or similar visual indicator) in their header. Some columns, such as **Destination** and **Reason Code**, are currently not sortable to ensure optimal performance.
  - **Resizing**: Column widths can be adjusted by dragging the dividers between column headers.

> **Note**
>
> Note that the resize functionality is active across the entire column header area.

> **Note**
>
> If you have a block rule, for example, to block social media, and a user tries to access a blocked site such as facebook.com, the Events report will only display a Web block event. The Firewall does not log an event in this scenario because logging both a Firewall allow and a Web block could be confusing. This is intentional. When the Firewall allows the traffic, but the Secure Web Gateway (SWG) blocks it, only the Web block action is shown in the report.
>
> As a result, if you are looking to correlate events between the Firewall and Web layers for this type of traffic, you will not see a corresponding Firewall event. This is expected behavior and does not indicate a system issue.

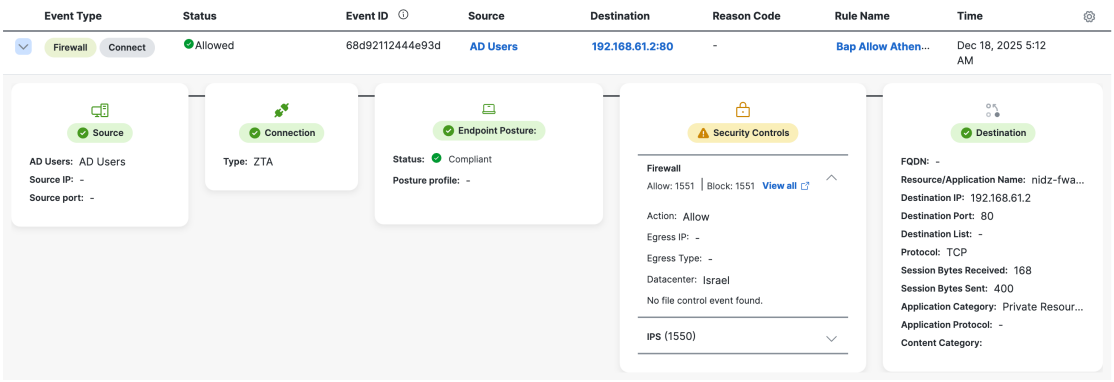
3. Select which security event types you want to view in the report. By default, all event types are selected to display activity for all event types.

   The Events report supports partial results if one or more event type queries (such as Proxy, Firewall, IP, Intrusion, or Decryption) fail due to an internal error. The report displays all available results from the successful queries, rather than showing an error for the entire request. Any unavailable event types will be clearly indicated in a message displayed on the screen.

   > **Note**
   >
   > This feature update ensures continued visibility into available security data, even when certain backend services encounter issues. All retrieved data remains accessible for review and export.

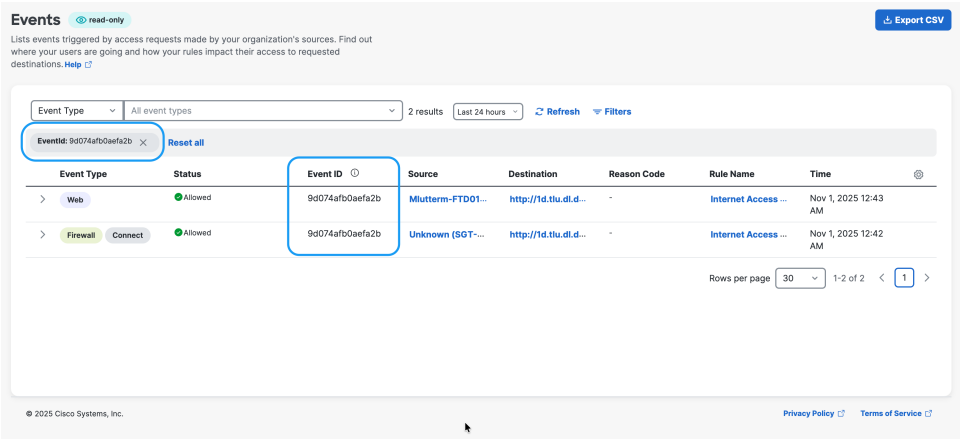
4. Click the **>** icon next to an event to view its Event Details Card.

This card provides a comprehensive, correlated view of the event, grouped by Source, Connection, Security Controls, and Destination. The card also details applied security controls and the final rule action (e.g., blocked or allowed) for the specific event.



> **Note**
>
> Interactive elements within the Event Details Card may display additional information upon hover or click.

Click on an Event ID within the table to automatically filter the report and display all correlated events.



5. (Optional) Refine your search using advanced filters. For detailed information on all available filtering and search options, see Filtering and Search Options.
6. (Optional) To export the events report, click the **Export CSV** button at the top-right corner of the table. This downloads the current view of the report in CSV format for further analysis or record-keeping. For detailed instructions on exporting report data, see Export Report Data to CSV.

Filter the Report by Firewall Requests

Provides instructions for completing the Filter the Report by Firewall Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

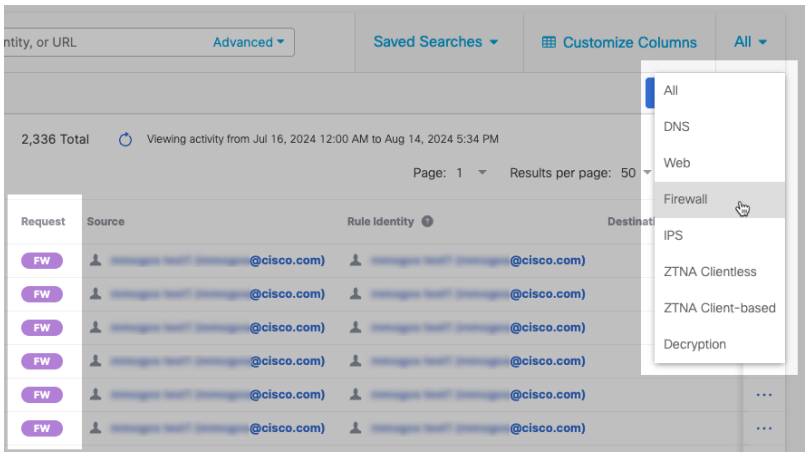
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view events from the **last 24 hours** (default), **Yesterday** , **Last 7 Days**, **Last 30 Days**, or a **Custom range**.

   The label **FW** in the **Request** column indicates a Firewall event.
3. Select the **Firewall** option from the dropdown menu at the top right to filter the report for Firewall events. Columns and Filter options update to those that are relevant to Firewall events.



4. Click the row to view Event Details.

   The Activity Search Report displays Event Details for each search result in a navigation drawer on the right. For more information, see View Activity Search Report Actions.

   Firewall event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see View and Customize the Activity Search Report.

   - **Action**
   - **Time**
   - **Rule Name**
   - **Source Geolocation**
   - **Source**
   - **Destination IP**
   - **Categories**
   - **File Name**
   - **Protocol**
   - **Application Protocol**

   Firewall event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Source IP	The source IPv4 or IPv6 address. Supports both compressed and long-form IPv6 address formats.
Source Port	The network port number on the source host from which the request originated.

Field Name	Description
Destination Port	The TCP or UDP port number on the destination host to which the request was sent. This field identifies the specific service or application targeted by the connection (for example, port 80 for HTTP or port 443 for HTTPS).
Resource/Application	The name of the resource or application.
Session Bytes Sent	The total number of bytes sent during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data sent from the source to the destination for the event session.
Session Bytes Received	The total number of bytes received during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data received from the destination by the source for the event session.
File Status (Disposition)	The file's Cisco AMP disposition: • **Clean**: Indicates that the AMP cloud categorized the file as clean. • **Malware**: Indicates that the AMP cloud categorized the file as malware, or local malware analysis identified malware. • **Unknown**: Indicates that the system queried the AMP cloud, but the AMP cloud has not assigned the file a disposition.
SHA256 Hash	The checksum of the file, if available and the event matched rules with File Type Control or File Inspection enabled.
File Transfer Direction	**DOWNLOAD**, **UPLOAD**, or **UNKNOWN**, if the event matched rules with File Type Control or File Inspection enabled.
Identified Threat	The name of the detected malware.
Malware Analysis Detected	If the event matched rules with File Inspection enabled, this field shows one of the following values as a result of file analysis by Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics. • **UNKNOWN** • **NOT ANALYZED** • **ANALYSIS COMPLETE NO VIRUS** • **ANALYSIS FAILED** • **ANALYSIS COMPLETE MALWARE DETECTED**
Threat Severity Score	The threat score most recently associated with this file. This is a value from 0 to 100.
File Type Identifiers	The type of file. For example, PDF or MSEXE.

Field Name	Description
File Size (bytes)	The size of the file in bytes, if the event matched rules with File Type Control or File Inspection enabled.
Archive File Name	The name of the archive file involved with the activity, if the event matched rules with File Type Control or File Inspection enabled.
Archive Extraction Depth	The level (if any) at which the file was nested in an archive file.
Archive SHA-256 Hash	The checksum of the archive file, if the event matched rules with File Type Control or File Inspection enabled.

Filter the Report by Web Requests

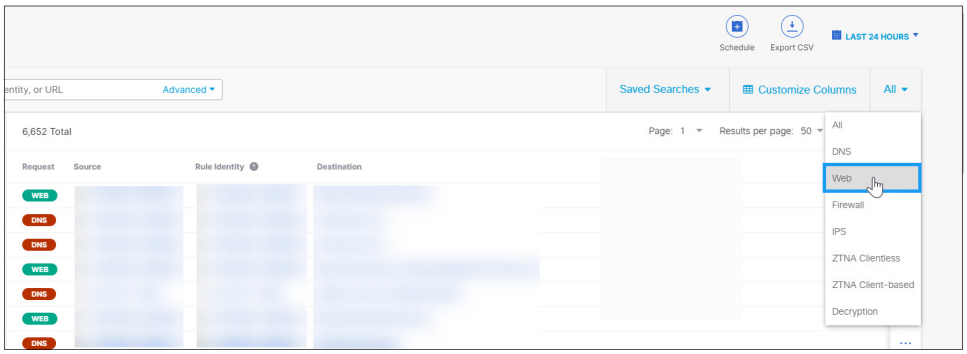
Provides instructions for completing the Filter the Report by Web Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

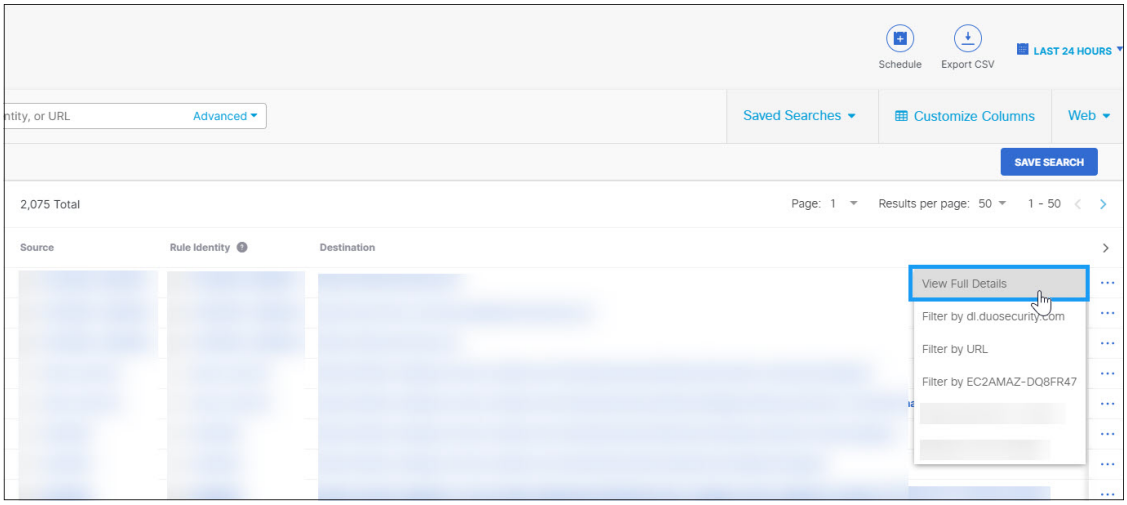
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **last 24 hours** (default), **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**.
3. From the drop-down menu at the top-right of the table, choose the **Web** option to filter the report for web events.



4. Click the ellipsis (**...**) and choose the **View Full Details** option to view web event details in the side panel.



5. The event details are displayed in the side panel. For more information, see View Activity Search Report Actions.

Web event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see Customize the Activity Search Report.

- **Action**
- **Time**
- **Rule Name**
- **Source Geolocation**
- **Source**
- **Rule Identity**
- **Internal IP Address**
- **External IP Address**
- **Destination**
- **Categories**
- **Resource/Application**
- **Application Category**
- **Content Type**
- **Request Method**
- **Referrer**
- **Status Code**

Web event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Hostname	Fully Qualified Domain Name (FQDN) of the machine or container from which the event originated.
File Action (Remote Browser Isolation)	Action taken on a file, such as Viewed, Original File Downloaded, Sanitized PDF File Downloaded.
Total Size, in Bytes	The number of bytes sent from the client for all the requests, including HTTP headers, for example, 234.
User Agent	The user agent string as captured by the proxy, for example, Mozilla 5.0 (X11; Linux x86_64; rv:12.0) Gecko 20100101 Firefox 21.0.
SHA256 Hash	This represents the SHA-256 hash of the response body.
Egress IP Address	The IP address is used by the proxy to communicate with the origin server. Dot notation is used for IPv4 and RFC 5952 is used for IPv6 , for example, 1.2.3.4, 2001:db8::1.
Egress Data Center	The data center that processed the request.
YouTube Channels	The YouTube channel name, such as @Cisco in the Cisco YouTube channel (https://www.youtube.com/@Cisco).

Field Name	Description
YouTube Categories	The set of YouTube categories, such as Education, Entertainment, Animation.

Edit an Internet Access Rule

Provides instructions for completing the Edit an Internet Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

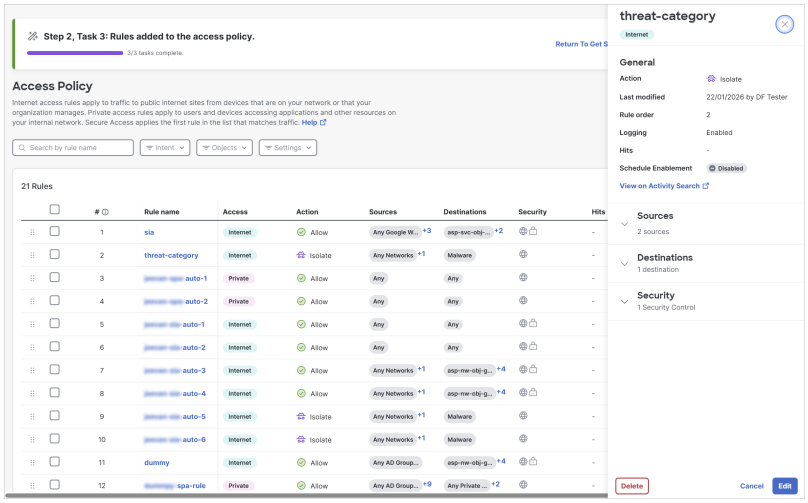
Once an internet access rule is created in Secure Access, you can modify the access rule's criteria and security control options.

Before you begin

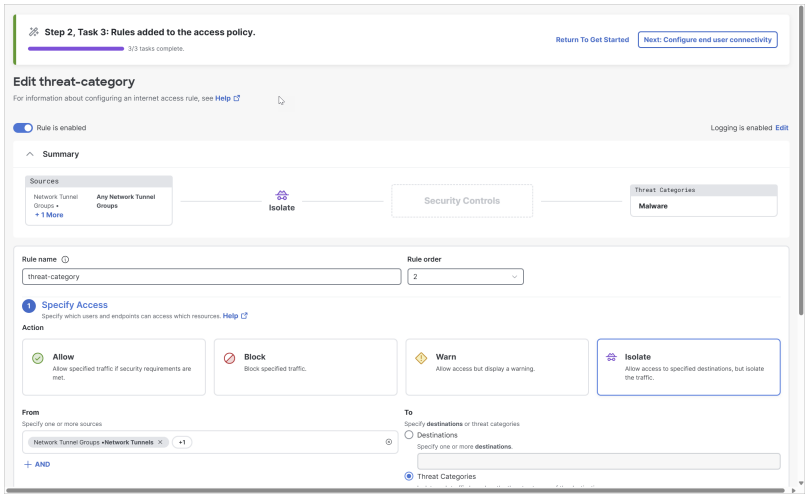
- Full Admin user role. For more information, see Manage Accounts.

Procedure

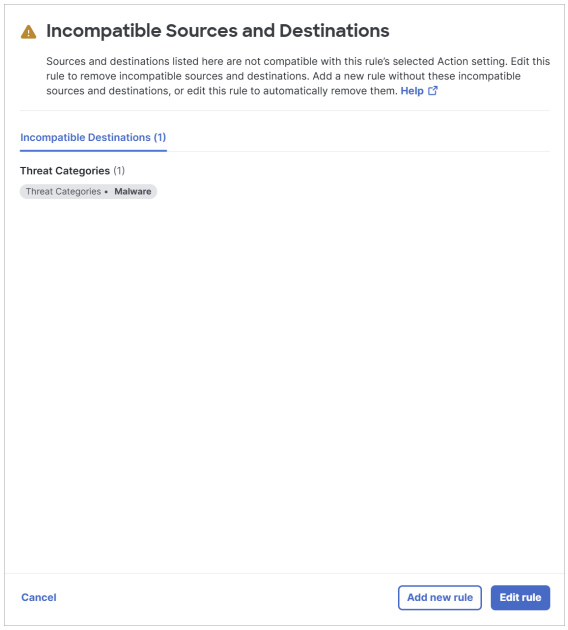
1. Navigate to **Secure** > **Access Policy**.
2. In the access rules table, click the name of an internet rule that you want to edit.



3. In the rule details section, click **Edit** to modify the access rule.



4. Change the access criteria.
   a) Edit the name and priority of the access rule.
   b) To change the rule action, choose the required **Action**.
      - The system automatically checks if the existing sources and destinations are compatible with the selected action. If the existing sources and destinations are not compatible with the selected Action, the **Incompatible Sources and Destinations** pop-up displays the incompatible sources and destinations.



   c) To edit the current rule and remove incompatible sources and destinations, click **Edit rule**.
   d) To create a new rule with all the other criteria same except the incompatible sources and destinations, click **Add new rule**.

      This opens a new rule creation page with the access criteria already replicated from the original rule.
      - The rule name is set to `<original rule name>_Copy 1`.
      - The rule order is set as the original rule and takes priority over the original rule.

   e) Edit the other criteria.

      For more information on other criteria, see Add an Internet Access Rule.

5. Click **Save**.

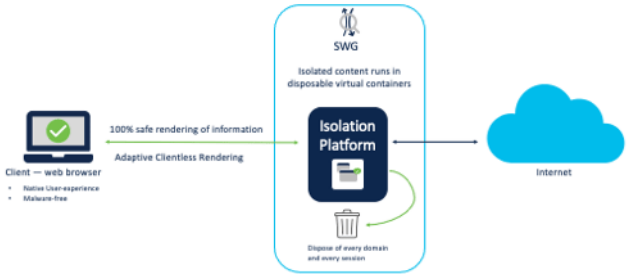
About Isolated Destinations

Describes About Isolated Destinations in Cisco Secure Access and outlines Browser Prerequisites and Secure Access Prerequisites. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

> **Note**
>
> **Secure Access Packages and Feature Availability**
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. See also, Cisco Secure Access Packages

Remote browser isolation (RBI) protects identities from potential malware and other threats by redirecting browsing to a cloud-based host. Destinations and threat categories supported by RBI can be isolated when added to an Internet access rule in a Secure Access policy. When you add a rule and specify an Isolate rule action, the selected destination or threat category in the rule will create a remote browser when users attempt to access the content. Instead of blocking identities from the endpoints, a cloud-based browser hosts the browsing session for that destination or threat category.

> **Note**
>
> RBI does not support mobile devices such as iOS and Android.



Before you can successfully isolate destinations, you must meet the prerequisites for Secure Access and the prerequisites for the use of RBI with the browsers deployed in the organization.

Browser Prerequisites

- Access to third-party cookies enabled.

> **Note**
>
> By default, most browsers (for example, Google Chrome) have third-party cookies blocked in incognito mode. You must update this setting to allow access to third-party cookies for isolation to work.

- Minimum supported browser versions:
  - Apple Safari 9
  - Google Chrome 34
  - Microsoft Edge 12
  - Mozilla Firefox 17
  - Samsung Internet 11
- The Cisco Secure Access root certificate or customer CA-signed certificate must be installed. For more information, see Manage Certificates.
- RBI **does not** support mobile devices such as iOS and Android.

> **Note**
>
> Browser extensions and plugins are not supported and browser-specific features are not guaranteed to work. Regardless of the browser the user initiates the browsing session with, the cloud-based browser for isolation will always be Google Chrome.

Secure Access Prerequisites

- **Decryption** must be enabled for the rule. Make sure it is enabled in the security profile selected in the rule.
- If a **Do Not Decrypt** list is specified in the security profile, the list cannot include destinations (within destination lists, content categories, or application settings) that are required for isolation to ensure those domains and URLs can be decrypted.
- Destinations required or intended for isolation should not be included your bypass lists. For more information see Manage Domains and Manage Internet Security.

Secure Access Package Support for RBI and Isolation Rules

Describes Secure Access Package Support for RBI and Isolation Rules. Secure Access remote browser isolation (RBI) provides an added layer of protection against browser-based security threats.

Secure Access remote browser isolation (RBI) provides an added layer of protection against browser-based security threats. RBI moves the most dangerous part of browsing the internet away from the end user's device and into the cloud. This makes it possible for users to visit web destinations safely, enabling users to be productive and access the web destinations they need without negative impacts.

Secure Access provides two levels of RBI support: RBI Advanced and RBI Risky.

RBI Advanced

Supported isolation controls include:

- Watermarking
- Copy and Paste
- Read-only and read/write
- Document isolation
- Downloads and uploads

Supported destinations include:

- All content categories
- Destination list entries including domains, URLs, IPv4 addresses, and CIDR block.

> **Note**
>
> Secure Access does not support RBI and isolation rules for IPv6 destinations.

- All applications
- All threat categories

RBI Risky

Supported destinations include:

- Uncategorized content categories
- Threat Categories: Malware, Command and Control, Phishing Attacks, and Potentially Harmful Domains

Secure Access Packages and RBI Support

When chosen as the rule action, the availability of isolation controls, destinations, and threat categories is based on your Secure Access package's RBI support.

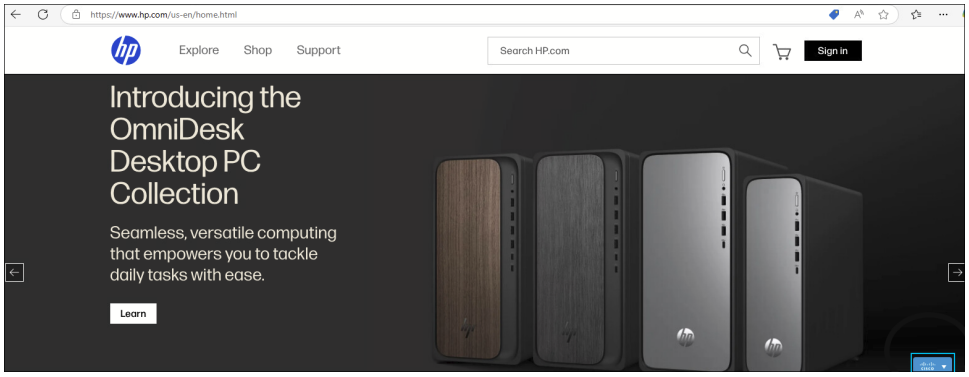
- RBI Advanced is bundled with the Secure Access Advantage and available as an add-on for Secure Access Essentials.
- RBI Risky is available as an add-on for Secure Access Essentials.

> **Note**
>
> Currently, isolation applies only to Internet Access rules.

Verifying Isolation

Describes Verifying Isolation in Cisco Secure Access. You can verify isolation by checking for a Cisco logo in the bottom right-hand corner of the browser when isolation is successful.

You can verify isolation by checking for a Cisco logo in the bottom right-hand corner of the browser when isolation is successful.



Limitations of Isolation

Describes Limitations of Isolation in Cisco Secure Access. You can isolate either destinations or threat categories in a Secure Access policy Internet access rule.

- You can isolate either **destinations** or **threat categories** in a Secure Access policy Internet access rule. You cannot specify both in the same rule. You can create a separate rule for each type.
- Only top-level page requests can be isolated and pages can either be entirely isolated (top-level request and resource requests) or not.
- 5 GB is the maximum file size that can be downloaded through the isolation environment when RBI is enforced on a browser connection.
- If your Secure Access package expires or downgrades, any rule with **Isolate** may no longer work as expected. You should review and update the **Action** setting for these rules as needed.

Isolate Downgrade

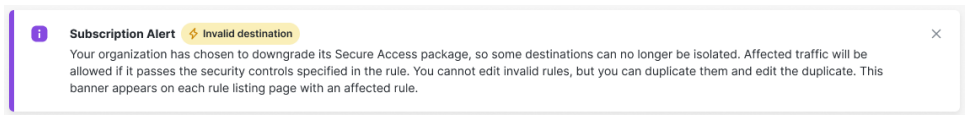
Describes Isolate Downgrade in Cisco Secure Access. When chosen as the rule action, the availability of isolation controls, destinations, and threat categories is based on your Secure Access package's RBI support.

When chosen as the rule action, the availability of isolation controls, destinations, and threat categories is based on your Secure Access package's RBI support.

- RBI Advanced is bundled with the Secure Access Advantage and available as an add-on for Secure Access Essentials.
- RBI Risky is available as an add-on for Secure Access Essentials.

Expired or Downgraded Package Support for RBI

If your Secure Access package expires or downgrades from RBI Advanced to RBI Risky, any rule with **Isolate** may no longer work as expected. When this happens you'll see a **Subscription Alert** banner on the **Access Policy** dashboard, as shown below.



Any rules that are impacted by a package downgrade are flagged in the rule list. You'll need to review the impacted rules and take appropriate action.

Filter Isolate Rules

Provides instructions for completing the Filter Isolate Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Note that the **Subscription Alert** banner for the package downgrade only appears when there is an Isolate rule visible on the current page that lists Access Policy rules. In other words, as you navigate through multiple pages of access rules, the banner appears only on pages that have an Isolate rule.

For ease of review, you can filter the rules by **Intent** to bring the Isolate rules to the beginning of the rules table.

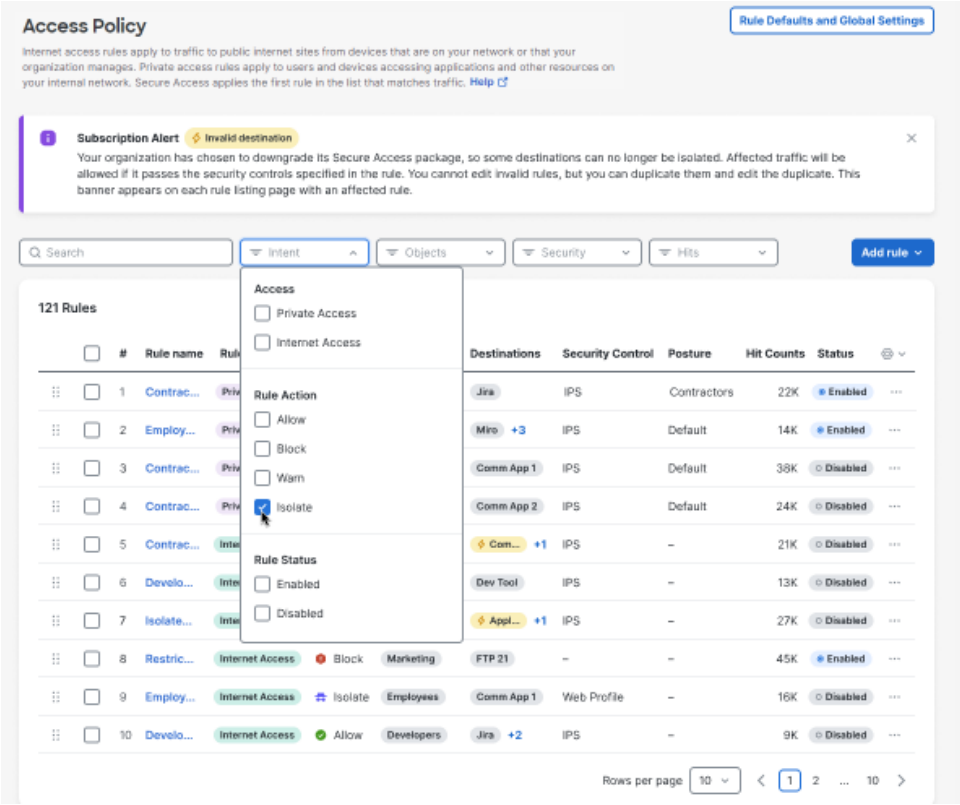
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- You should be familiar with the following internet access rules concepts:
  - Components for Internet Access Rules
  - Default Settings for Internet Access Rules
- For other factors involved in creating and enforcing internet access rules, see Manage Internet Access Rules.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

1. Navigate to **Secure > Access Rules**.
2. In the Search area at the top of the rule list, click **Intent** and check **Isolate** to sort the Isolate rules to the top of the rule list.



Duplicate a Downgraded Isolate Rule

Provides instructions for completing the Duplicate a Downgraded Isolate Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can duplicate a Secure Access internet access rule, which can be helpful in creating a new rule with the same criteria as the original rule. With respect to downgraded rules with unsupported destinations, you can duplicate the rule and then modify it as needed. The rule will be set to Allow only, and you can edit the source, destination, and security controls. Note that you cannot modify the original downgraded Isolate rule.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- You should be familiar with the following internet access rules concepts:
  - Components for Internet Access Rules
  - Default Settings for Internet Access Rules
- For other factors involved in creating and enforcing internet access rules, see Manage Internet Access Rules.

> **Note**
>
> Prerequisites for internet access rules are similar to but different from prerequisites for private access rules.

Procedure

1. Navigate to **Secure > Access Rules**.
2. In the sorted rule list, you can do a quick search for flagged Isolate rules you want to duplicate. Select the ellipses context menu (**...**) and choose **Duplicate**.

Troubleshoot Internet Access Rules

Describes Troubleshoot Internet Access Rules in Cisco Secure Access and outlines General Troubleshooting Tips, Guidelines for When Internet traffic is Unexpectedly Blocked, and Guidelines for When Internet Traffic is Unexpectedly Allowed. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To troubleshoot your internet access rules, review these guidelines.

General Troubleshooting Tips

- Navigate to the Overview page for possible status notifications.
- Use Activity Search to look for logged events.
- While creating an internet access rule, the **Next** button is not available until you give the rule a name and then click out of the Rule name field.

Guidelines for When Internet traffic is Unexpectedly Blocked

Try these suggestions, either to temporarily suspend problematic blocks and allow end users to access a needed resource, or to narrow down the cause of the problem.

- Because traffic to internet destinations is allowed by default, there may be one or more existing rules that explicitly block this traffic.
- You can temporarily disable a rule that blocks desired traffic.
- To allow immediate access to a necessary destination that is being blocked by another rule, create a new access rule (using the "Enter manually" option for source and/or destination if necessary) and put this rule at or near the top of the rule list on the Policy page so it hits before more general rules that would otherwise apply to the traffic.
- Try disabling enforcement of certain web security features for a rule, in the Advanced settings at the bottom of the Security Controls section of the rule.
- Try disabling intrusion prevention (IPS) for a rule.
- Try disabling intrusion prevention (IPS) on the Rule Defaults page, which disables it for all rules that are configured to use the default setting for IPS.
- Try disabling decryption for all rules in Global Settings, which effectively disables intrusion prevention and other specified features.
- If the issue involves Microsoft 365 applications or sites that use certificate pinning, check Global Settings.
- If all traffic is blocked, make sure you have not inadvertently blocked traffic to a destination that is required infrastructure for managing access. For example, make sure there is no Geolocation rule that blocks traffic to your identity services (IdP) provider.

Guidelines for When Internet Traffic is Unexpectedly Allowed

Try these suggestions, either to block problematic traffic, or to narrow down the cause of the problem.

- Verify that any existing rule blocking the traffic is enabled (toggle at the top of the rule page)
- To immediately block access to a problem destination that is unexpectedly being allowed, you can create a new access rule (using the "Enter manually" option for source and/or destination if necessary).
- Make sure decryption is not disabled in the security profile in the rule that matched the traffic, or in the security profile selected in Rule Defaults.
- Make sure IPS is not disabled in the rule default or in the rule
- Make sure Decryption and Certificate Pinning are not disabled in Global Settings.
- Make sure the destination is not on a Do Not Decrypt list used by the IPS feature or specified in the rule's security profile.
- Make sure web features are being enforced for the rule (Advanced settings at bottom of Security Controls section in the rule)
- Check the configured sources and destinations of the rule you expect to block the traffic to be sure they include the problematic source and destination.
- Check each rule component of the rule you expect to block the traffic (rule action and each security control) to be sure each specifies the behavior you expect.
- Check the rule order; traffic may be hitting a different rule than the one you expect.

Guidelines for When an Internet Access Rule Does not Match Traffic as Expected

Try these suggestions to narrow down the cause of the problem.

- Make sure the rule is enabled (toggle at top of rule page)
- Make sure web features are being enforced for the rule (Advanced settings at bottom of Security Controls section in the rule)
- Check the configured sources and destinations of the rule you expect to match the traffic to be sure they include the problematic source and destination.
- Check the rule order; traffic may be hitting a different rule than the one you expect.

28 Internet and SaaS Resources

Topics:

- Manage Internet and SaaS Resources
- Manage Destination Lists
- Manage Application Lists
- Manage Content Category Lists
- Manage Tenant Control Profiles

Provides an overview of Internet and SaaS Resources in Cisco Secure Access, including Manage Internet and SaaS Resources, Manage Destination Lists, and Manage Application Lists. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internet and SaaS Resources

Describes Manage Internet and SaaS Resources in Cisco Secure Access. Items on this page are reusable components (sometimes known as "objects") that can be used as destinations when configuring internet access rules.

Items on this page are reusable components (sometimes known as "objects") that can be used as destinations when configuring internet access rules.

Internet and SaaS resources include:

- Destination Lists
- Application Lists
- Content Category Lists
- Tenant Control Profiles

Manage Destination Lists

Describes Manage Destination Lists in Cisco Secure Access. A destination list is a collection of domains, URLs, IP addresses (IPv4 and IPv6), and CIDR blocks.

A destination list is a collection of domains, URLs, IP addresses (IPv4 and IPv6), and CIDR blocks. Use destination lists in internet access rules to block, allow, or isolate traffic, or in DLP rules to monitor or block sensitive data uploaded to the web.

Guidelines and Best Practices

- Domains in destination lists must comply with the format described in RFC-1035.
- Each fully qualified domain name that you add in a destination list must contain less than 253 characters.
- Secure Access assumes implied left asterisk wildcards in domains. You may not include wildcards in domains. For more information, see Control Access to Domains.
- In URLs, Secure Access assumes right-side wildcards by URL path segment. (i.e., `https://www.example.com` matches `https://www.example.com/abc/def` but not `https://www.sub.example.com/abc/def`.) You must use URLs that follow standard syntax rules. (See RFC-3986). Secure access normalizes the format. (See Control Access to Custom URLs.)

Destination List Examples

Valid destination list entries:

- `example.com` (Domain)
- `sub.domian.com` (Domain)
- `http://www.example.com/path.file.txt` (URL)
- `us` (Country code top-level domain)
- `com` (Top-level domain)
- `198.51.100.0` (IPv4 address)
- `2001:DB8::/32` (IPv6 CIDR)

- `102.9.2.0/24` (CIDR block)

Invalid destination list entries:

- `example.*` (Uses asterisk)
- `2001:DB8:/128` (Malformed address)
- `2001:DB8:/32` (Malformed CIDR)
- `http://www.example.com/path/file?.txt` (URL with ? wildcard)

Add a Destination List

Provides instructions for completing the Add a Destination List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access enables administrators to manage destinations that are grouped by destination lists. Destination lists either allow or block access to destinations. Destinations represent domains, URLs, CIDRs, and IPv4 and IPv6 addresses. For information about supported destination types and guidelines, see Manage Destination Lists.

After you add a destination list with destinations, you can select the destination list on the internet access rules in the organization's policy.

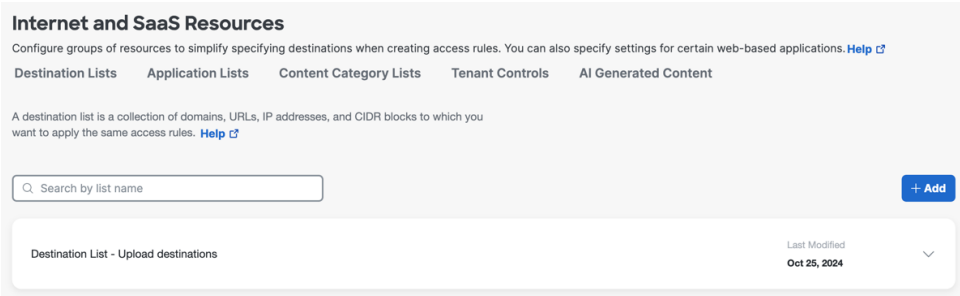
For information about uploading a list of destinations from a file, see Upload Destinations from a File.

Before you begin

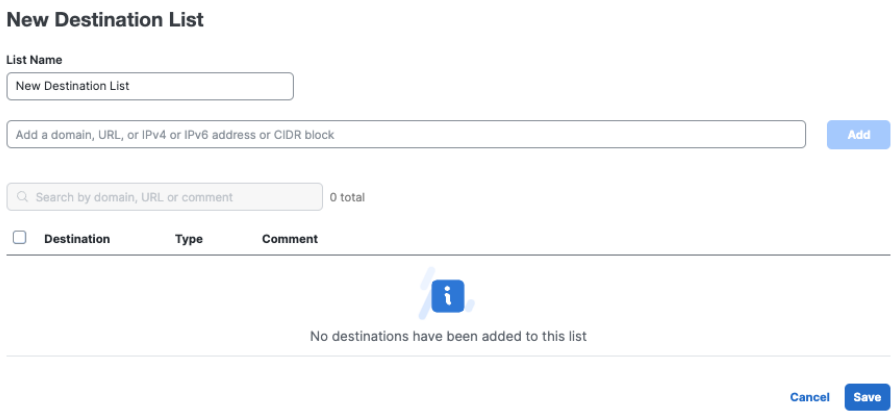
- Full Admin role in Secure Access. See Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Click **Add**.

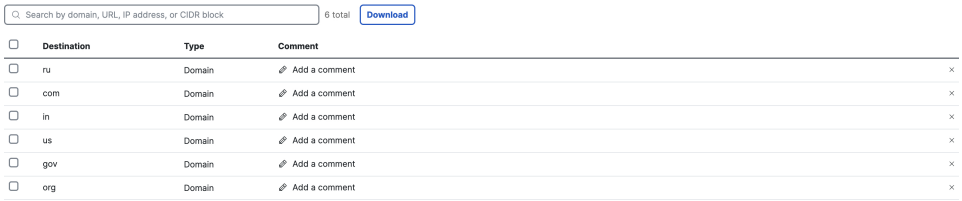


3.
4. For **List Name**, enter a descriptive name.



5. In the next field, enter a domain, URL, IPv4 or IPv6 address, or CIDR block.

> **Note**
>
> You can add a top-level domain (TLD) in the destination list.



6. Click **Add**.

> **Tip**
>
> You can upload destinations in bulk from a text or CSV file, but you must first save and edit the destination list. For more information, see Upload Destinations from a File.

7. Click **Save**.

   The destination list is available as a destination when you add an internet access rule.

Upload Destinations From a File

Provides instructions for completing the Upload Destinations From a File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access provides the option to import destinations from a text or CSV file into an existing destination list. Before you can upload a file with the destinations to Secure Access, create a destination list or use an existing destination list in the organization. For information about supported destination types and guidelines, see Manage Destination Lists.

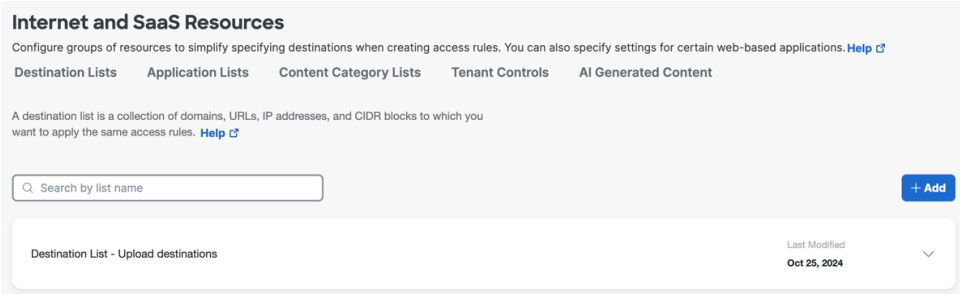
> **Note**
>
> **Supported files for upload**
>
> Files must be text or CSV files and must include only one destination per line. Before uploading, review your list for extra-space characters and commas. Exceptions to the format of a single destination per line can result in errors.

Before you begin

- Full Admin role in Secure Access. See Manage Accounts.

Procedure

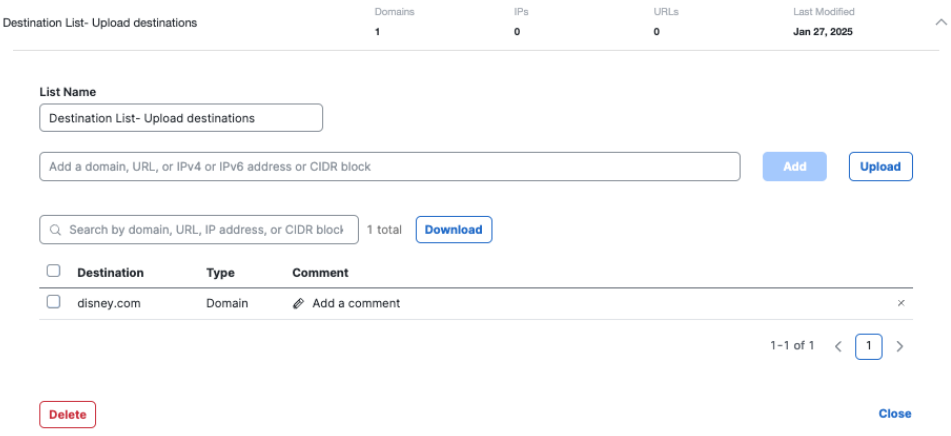
1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.



2. If you are uploading destinations to an existing destination list, navigate to the destination list and click the caret to expand the destination list.
3. If you require a new destination list for the destinations in the text file, add a destination list.

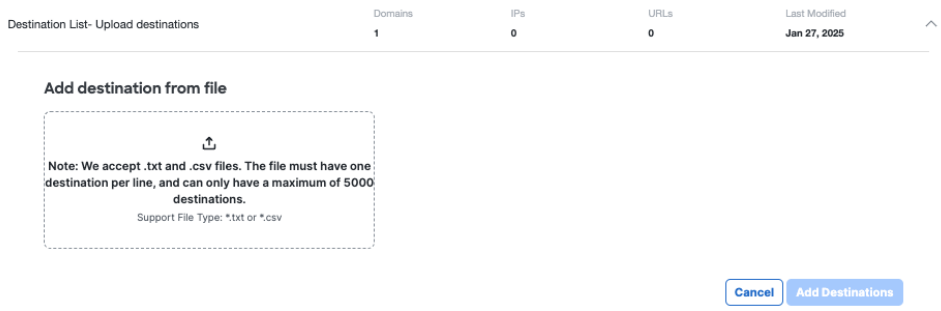
   You don't need to add any destinations.

   a) Save the new destination list.
   b) Click the caret in the table row to expand the new destination list.



4. Click **Upload**. The current uploader supports text and CSV files in the format of one destination per line. Excel files are not supported.
5. Select or drag and drop a .txt or CSV file that contains your destinations.

   If you want to remove the file and choose a different file, click **Replace**.



6. Click **Add Destinations**.

   Supported destinations in the file are added to your destination list.

   If your bulk upload includes unsupported destinations, the upload does not fail, but only supported destinations are added.

7. Immediately after uploading the destinations, look for a pop-up message. If the file contained unsupported destinations, this pop-up is displayed.



8. To download a spreadsheet that you can use to determine which destinations failed and why, click the link in the pop-up.
9. Click **Save**.

Edit a Destination List

Provides instructions for completing the Edit a Destination List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

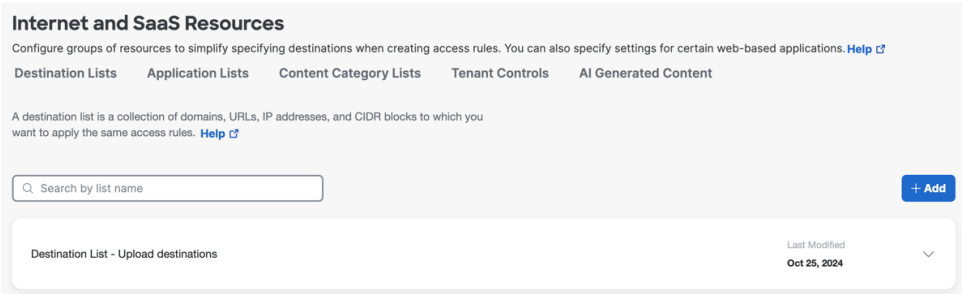
Cisco Secure Access supports creating and managing destination lists. After you add a destination list, you can edit the destination list or remove the destination list from the organization. If a destination list is part of an enabled internet access rule, changes are effective immediately.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

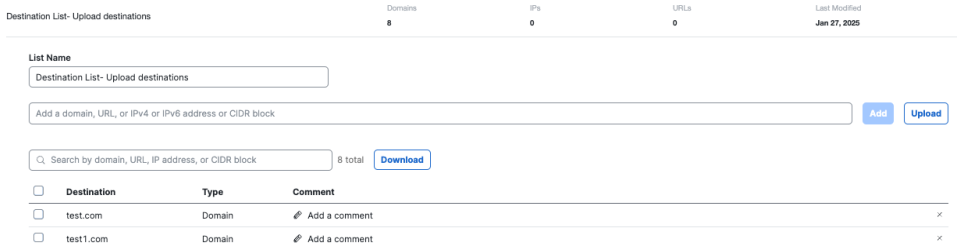
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list.



3. Make your changes.

> **Tip**
>
> You can upload destinations in bulk from a text or CSV file. For more information, see Upload Destinations from a File.



Search the Destination List

Provides instructions for completing the Search the Destination List workflow in Cisco Secure Access. Sign in to Secure Access or Umbrella with permission to view destination lists.

Use destination list search to find a destination list entry by destination list name, destination, or comment.

Before you begin

- Sign in to Secure Access or Umbrella with permission to view destination lists.
- Have a search term ready. You can search by destination list name, destination, or comment.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** page and click the **Destination Lists** tab.
2. In the primary search bar at the top of the screen, enter a keyword to search on and submit. Expand the compressed destination lists to view the keyword that matches.
3. Enter a full or partial search term. You can search for any of the following items:
   - A destination list name
   - A destination, such as a domain, URL, or IP address
   - A comment, such as a support ticket number or the name of an administrator
4. Press **Enter** or wait for the search results to appear.
5. Review the results. The search returns exact and partial matches. Matching text is emphasized in the results. If the item you need is not shown, request more results to display the next set of matches. The interface shows up to 10 matches at a time.
6. Select the result that matches the destination or comment you want to review.
7. (Optional) Expand a destination list and in the list's expanded view, enter additional keywords to the secondary search to further refine the search within the specified destination list. These additional keywords do not replace the primary search request and are not applied to other destination lists generated from the primary search.
8. Verify that the corresponding destination list opens to the matching line item.

9. To delete the current search, click **Reset all** from the primary search bar at the top of the window. This action does remove the refined search within the secondary search if you opted to perform Step 7.

Delete a Destination List

Provides instructions for completing the Delete a Destination List workflow in Cisco Secure Access. Use the following procedure to permamently delete a destination list from your organization.

Use the following procedure to permamently delete a destination list from your organization. This list is not visible or accessible after this action.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list.
3. Click **Delete** at the bottom of the row contaning the list.
4. In the pop-up window, click **Delete** again to confirm the action. Click **Cancel** if you want the destination list to remain.

Download Destinations to a CSV File

Provides instructions for completing the Download Destinations to a CSV File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access destination lists are reusable lists of destinations. After you've added a destination list to Secure Access, you can download a comma-separated values (CSV) file that contains the destinations in the destination list.

Downloading a CSV file of the destinations is useful for when you need to update the destinations or share the destinations with teams that do not have permission to view the destination list in Secure Access. The CSV file includes the information about the destinations in the destination list, including whether destinations are allowed and blocked.

You can remove or add entries in the CSV file, and then upload a file of destinations to a destination list. For more information, see Upload Destinations from a File.

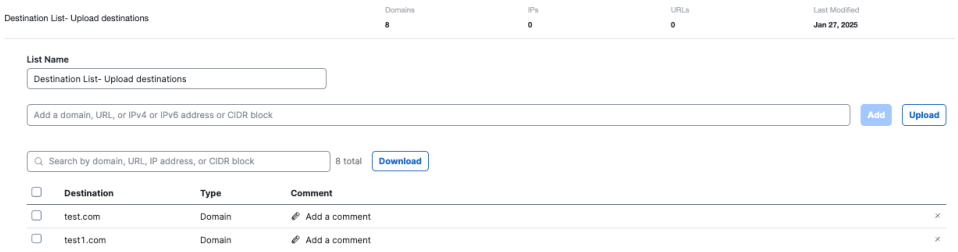
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.
2. Expand a destination list and click **Download**.

   The information for the destinations in the destination list are saved in a CSV file on your system.



Control Access to Custom URLs

Describes Control Access to Custom URLs in Cisco Secure Access. Adding custom URLs to a destination list allows Secure Access to extend a domain in a destination list to encompass full URLs.

Adding custom URLs to a destination list allows Secure Access to extend a domain in a destination list to encompass full URLs. This allows you to control access to a web site's pages based on the full URL of that portion of the web site pages.

Prerequisites

- Install a root certificate to support SSL decryption of URLs.
- The custom URL destination list is protocol-agnostic. This means that Secure Access does not expect that it's possible to know which protocol a web site will use in advance. Therefore, adding a protocol in front of a URL is not required when defining a destination list. Instead, with SSL decryption enabled, Secure Access can block a URL whether it's HTTP or HTTPS and thus minimize the difficulty of creating a destination list. For more information, see Manage Certificates.

Troubleshooting

If you encounter issues with the custom URL feature, contact Support and include the output of the following commands:

macOS

```
dig proxy.opendnstest.com
```

```
dig debug.opendns.com txt
```

Windows

```
nslookup proxy.opendnstest.com
```

```
nslookup -type=txt debug.opendns.com
```

Block a URL

Provides instructions for completing the Block a URL workflow in Cisco Secure Access. To block a URL, you can add it to a blocked destination list or create a new blocked destination list for URLs.

To block a URL, you can add it to a blocked destination list or create a new blocked destination list for URLs.

To add a URL to an existing blocked destination list:

Procedure

1. Navigate to **Secure** > **Access Policy**.

2. Expand a destination list
3. Add a URL.
4. Click **Save**.

> **Note**
>
> It is important to specify the URL correctly so that what's in your policy rule matches what the user is trying to access and is controlled correctly by access settings (block, allow, or warn—depending on the policy type).

URL Normalization

Describes URL Normalization in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

URLs normalize automatically using the following criteria:

URL Normalization	
Protocol Schema (the protocol should be stripped)	hxxp://xyz.com/test → xyz.com/test
Username: Password (should be stripped)	user: pass@xyz.com → xyz.com
Ports (should be stripped)	xyz.com:8080/abc → xyz.com/abc
Trailing slashes (stripped from the end of the URL)	xyz.com/abc/ → xyz.com/abc

URL Normalization for Destination Lists

Describes URL Normalization for Destination Lists in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

URL filtering conforms to URL normalization standards. Certain guidelines must be followed to ensure that the URL you are entering is what you want to block or allow. These can sometimes mean that the way a URL is displayed in the browser's address bar is not how it should be specified in a destination list. This is not done automatically. You must format the URL using the guidelines listed here for it to be blocked or allowed as intended. For guidelines, see URL Normalization.

Troubleshooting Unblocked URLs

Describes Troubleshooting Unblocked URLs in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

If the Secure Access block page does not display when navigating to a URL you expect to be blocked, ensure that the policy rule with the destination list enabled is higher in order than other rules that the enrolled resources may be part of.

Wait up to five minutes before testing again after any changes are made to ensure that enough time has passed for the changes to be replicated throughout Secure Access.

If problems persist, clear the local browser cache on your machine. Alternatively, clear your machine's DNS cache—a reboot will accomplish this.

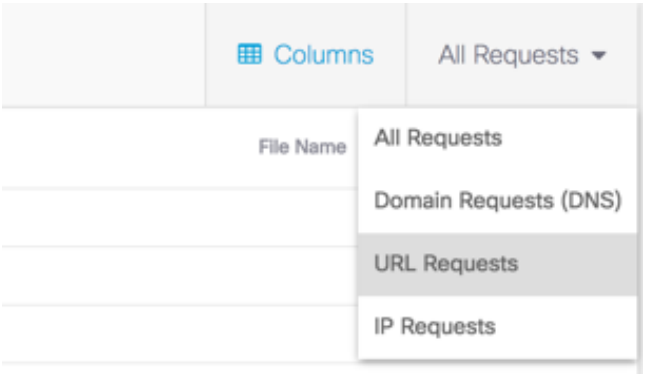
Also, check to see if you have a local—on-premise—proxy that is interfering.

Additionally, confirm that you have installed certificates. For more information, see Manage Certificates.

Reporting for Blocked URLs

Describes Reporting for Blocked URLs in Cisco Secure Access. The Secure Access Activity Search report supports the use of URLs as a search filter.

The Secure Access Activity Search report supports the use of URLs as a search filter.



After you've filtered for URLs, add another filter to show the custom block URLs that belong to your destination lists.

Examples

Describes Examples in Cisco Secure Access. The following examples show a single URL and what you can and cannot enter to have a block of that URL enforced.

The following examples show a single URL and what you can and cannot enter to have a block of that URL enforced. The list of URLs is built out from a single example, modifying a single parameter to show whether the URL "//a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes" would be blocked based on a URL.

In these examples, the protocol is stripped as it would be by the interface.

If you wanted to block this URL *a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes* the following logic would apply.

URL	Blocked?	Reason
a.co/cx/15195/100/setup_1848x19m.exe?z=z&super=bad&test=yes	Yes	The full URL is entered.
a.co/cx/15195/100/setup_1848x19m.exe?super=bad&test=yes&z=z	Yes	"&" is a delimiter; therefore, it's added as another level to the URL after the word "yes".
a.co/cx/15195/100/setup_1848x19m.exe?super=bad&test=yes	No	"?" is a delimiter so the URL still would begin at the "yes" and any enforcement would happen after that.
a.co/cx/15195/100/setup_1848x19m.exe?	No	Given the "?", it still means only characters after "yes" will be enforced; therefore, a direct download of this file would be allowed.
a.co/cx/15195/100/setup_1848x19m.exe	No	We will still only block any paths after "yes"; therefore, a direct download of this file would be allowed.

If you want to block this URL *g.com/a/d*, the following logic applies.

Note

These are only examples of destination list entries that would and would not block the URL `g.com/a/d`.

URL	Blocked?	Reason
g.com/a/d	Yes	The full URL is entered.
g.com/a/d?g	Yes	Delimits the path with the query "g" but still just a delimiter thus this will be enforced.
g.com/a/d?	Yes	URL + the "?" delimiter.
g.com/a/	No	The URL ends with "/d" so anything before "/d" would not be enforced.
g.com/a/?a	No	The URL ends with "/d" so anything before "/d" would not be enforced.

If you want to block this URL *d.co/cx/15195/100*, the following applies.

Note

These are only examples of which destination list entries would block the URL "d.co/cx/15195/100" and which would not.

URL	Enforced	Reason
d.co/cx/15195/100	Yes	The full URL is entered.
d.co/cx/15195/100/?	Yes	Everything after the delimited "/" after 100 would be blocked.
d.co/cx/15195/100/	Yes	Everything after the delimited "/" after 100 would be blocked.
d.co/cx/15195/100	Yes	Everything after the delimiting "/" after 100 would be blocked.
d.co/cx/15195/10	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195/1000	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195/	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.
d.co/cx/15195	No	The delimiter is only for paths after the "/" so any changes to the final path of /100/ would be ignored.

> **Note**
>
> There are normalization rules that most administrators never encounter. If you find that a URL is not being properly filtered and you've confirmed that all criteria are met, see the URL Normalization RFC.

Control Access to Domains

Describes Control Access to Domains in Cisco Secure Access. Domains in destination lists must comply with the format described in RFC-1035.

Domains in destination lists must comply with the format described in RFC-1035. You may not use wildcards in domains in destination lists; Secure Access assumes implied left wildcards in domain entries. A domain in a destination list matches traffic to all paths in that domain and its subdomains.

Destination list entry:	Matches all traffic where the domain matches:
`example.com`	`*.example.com`
`www.example.com`	`*.www.example.com`
`com`	`*.com`

For more information about troubleshooting possible error conditions with destination lists, see Troubleshoot Destination Lists.

Depending on what you want to do, you may need multiple internet access rules and destination lists. Remember:

- Order rules from specific to general.
- The default internet access rule is set to allow; the default private access rule is block. For more information, see View or Edit the Default Access Rules.
- Allowed traffic is still subject to security controls. For more information, see Security Controls for Internet Access Rules and Manage the Data Loss Prevention Policy.

The following internet access rule examples illustrate how you can use destination lists to control access to a public internet domain:

- To block all traffic to `example.com`:
  - Create Rule A with the block action, using a destination list containing `example.com`.
- To block traffic to a subdomain and allow traffic to the rest of the domain continue to match rules:
  - Create Rule A with the block action using a destination, list containing `sub.example.com`.
- To allow traffic to a subdomain, but block the rest of the domain:
  - Create Rule A with the allow action, using a destination list containing `sub.example.com`.
  - Create Rule B with the block action, using a destination list with `example.com`.

About Client Resolved Domain Destination List

Describes About Client Resolved Domain Destination List in Cisco Secure Access. The Client Resolved Domain destination list is a destination list that Secure Access creates only for organizations to manage trusted domains.

The Client Resolved Domain destination list is a destination list that Secure Access creates only for organizations to manage trusted domains.

To use the Client Resolved Domain destination list, enable the **Client Resolved Domain Destination List** global setting in the Access policy. For more information, see Client Resolved Domain Destination List.

When end users in the organization send a web request for a domain in the Client Resolved Domain destination list, the Secure Web Gateway (SWG) uses the IP address for the domain resolved by the client to connect to the destination. The Secure Web Gateway does not perform DNS lookups to resolve the IP address for the trusted domain.

Administrators can perform these operations on the Client Resolved Domain destination list:

- Add trusted domains directly in Secure Access or upload trusted domains in an CSV or TXT file. For more information, see Add Domains in Client Resolved Domain Destination List.
- Delete a trusted domain. For more information, see Delete Domains in Client Resolved Domain Destination List.
- Download the trusted domains to a CSV file. For more information, see Download Domains in Client Resolved Domain Destination List.

Add Domains in Client Resolved Domain Destination List

Provides instructions for completing the Add Domains in Client Resolved Domain Destination List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you enable the **Client Resolved Domain Destination List** global setting in the Access policy, Secure Access shows the Client Resolved Domain destination list in the organization. For more information, see About Client Resolved Domain Destination List.

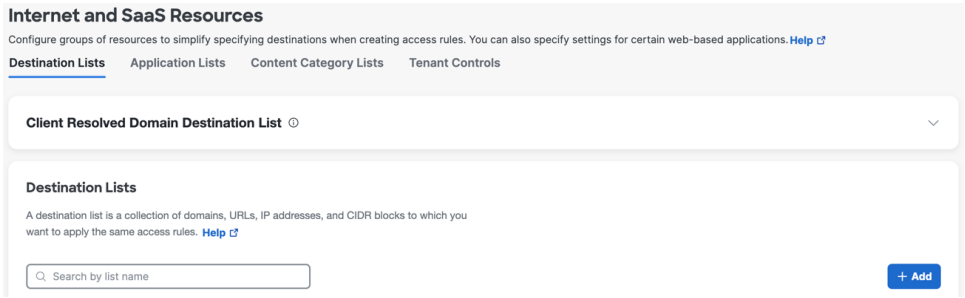
Administrators can add and manage trusted domains in the Client Resolved Domain destination list.

Before you begin

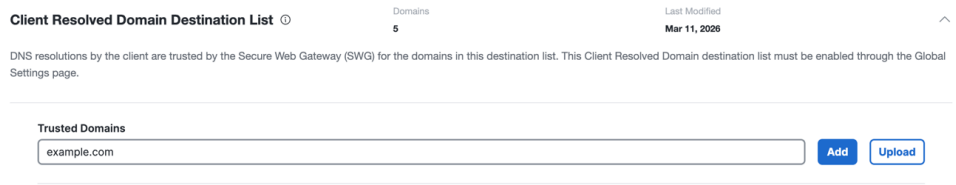
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.



2. Expand **Client Resolved Domain Destination List**.

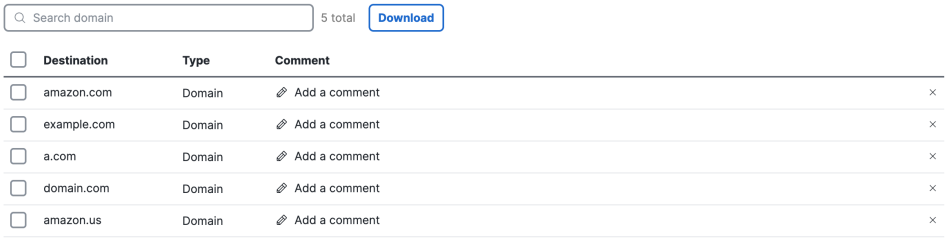


3. Navigate to **Trusted Domains**, enter a domain name, and then click **Add**.
4. (Optional) Click **Upload** to import a list of domain information in a file.



a) Click in the **Add destination from file** text area and then upload the trusted domains in a CSV or TXT file.
b) Click **Add destinations.**

5. (Optional) Add a comment for a domain in the Client Resolved Domain destination list.



a) Navigate to an entry in the destination list and click on the **pencil icon** (Add a comment).
b) Enter a comment in the text area and then click **Add**.

6. Click **Close**.

Download Domains in Client Resolved Destination List

Provides instructions for completing the Download Domains in Client Resolved Destination List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Once you add domains in the Client Resolved Domain destination list in Secure Access, you can download the domains in a comma-separated values (CSV) file.

Downloading the domains in a CSV file enables you to update the domains and then upload the domains in to Secure Access, or share the domains with teams that do not have permission to view the Client Resolved Domain destination list in Secure Access.

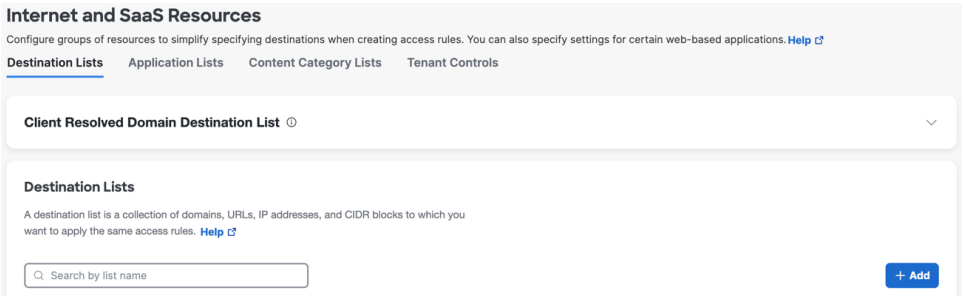
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

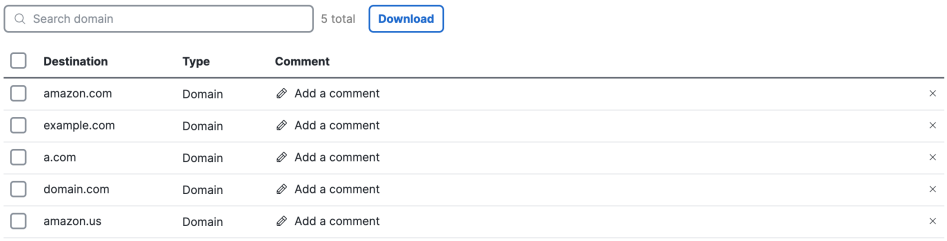
---

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.



2. Expand **Client Resolved Domain Destination List**.

3. Click **Download** to save the domains in the CSV file on your system.



4. Click **Close**.

Delete Domains in Client Resolved Domain Destination List

Provides instructions for completing the Delete Domains in Client Resolved Domain Destination List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you enable the **Client Resolved Domain Destination List** global setting in the Access policy, Secure Access makes the Client Resolved Domain destination list available in the organization. For more information, see About Client Resolved Domain Destination List.

Administrators can delete and manage trusted domains in the Client Resolved Domain destination list.

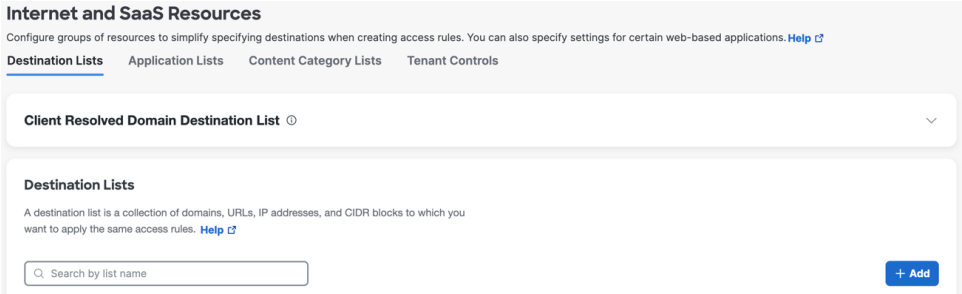
Before you begin

- Full Admin role in Secure Access. For more information, see Manage Accounts.

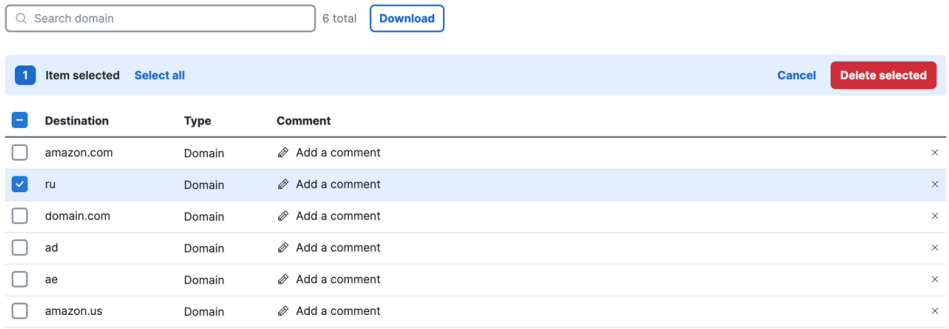
Procedure

---

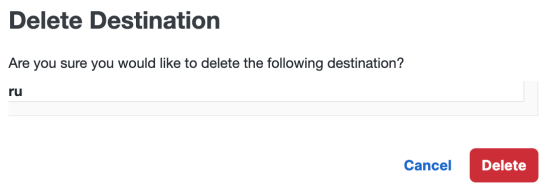
1. Navigate to **Resources** > **Internet and SaaS Resources** > **Destination Lists**.



2. Expand **Client Resolved Domain Destination List**.
3. Navigate to a row in the trusted domains table and either select the domain or click the **X** at the end of the row.
   a) If you selected the checkbox for the domain, click **Delete selected**.



4. Click **Delete** to confirm the removal of the domain in the Client Resolved Domain destination list.



5. Click **Close**.

Troubleshoot Destination Lists

Describes Troubleshoot Destination Lists in Cisco Secure Access. When you add a malformed destination or unsupported type of destination to a destination list, you may encounter an error condition.

When you add a malformed destination or unsupported type of destination to a destination list, you may encounter an error condition. In most cases, Secure Access displays an error message that describes the reasons for the error condition.

Destination lists support the following destination types:

- Fully-qualified domain name (FQDN). This may include a wildcard only if exact domain match is enabled at the time the domain is added to the list.
- Top-level domain (TLD)
- IP address
- URL

For more information about destination lists, see Add a Destination List.

Destination Lists and Common Error Conditions

Action	Error Message	Additional Information
Entered a destination that does not match the type and format expected by the destination list.	Invalid Domain, Invalid URL, Invalid IP	• Check the format and type of the destination that you added. • Enter the correct format of the destination.
Added a URL that has an error in the domain, path, or query.	Check to confirm that the URL was entered correctly.	• Secure Access requires that URLs follow RFC-3986 Uniform Resource Identifier (URI): Generic Syntax. • Check the characters in the URL. • Check the composition of the URL. • You can add a partial URL to leverage right-side wildcarding. For more information, see Control Access to Custom URLs.

Action	Error Message	Additional Information
Added a URL that is found in a high-volume domain list.	The URL belongs to a domain that does not present a security concern, but if proxied may impact Secure Access performance. Instead, consider adding only the domain.	• If you do not trust the destination, consider blocking the domain. • Generally, high-volume domains do not present a security risk and do not require additional inspection.
Added a destination that is found in the protected allow list.	The supplied destination matches the Secure Access global allow list and cannot be saved.	• Destinations in the protected allow list either host services other than HTTP or are critical to Secure Access operations. Secure Access only proxies services that use HTTP. • If the error occurs when you add a URL and you don't trust the destination, consider blocking the domain. • If you are not sure why the destination is considered protected, contact support.
Entered a URL that contains non-ASCII characters.	Invalid URL.	• Try percent-encoding the URL or block the domain.
Uploaded a list of destinations in which at least one of the URLs or domains contains an error.	There was an issue with one or more of the destinations in the uploaded list.	• A bulk upload error message. • Secure Access provides a link to the list of destinations that were not added from the uploaded destination list. • Correct or remove the destinations from your bulk upload list and try again. • Secure Access does not add destinations from an uploaded destination list unless all of the destinations are accepted.
Entered a destination that is not accepted by Secure Access.	Invalid destination.	• A generic error message. • Entered a destination that is not accepted by Secure Access. • You have encountered an error condition that is not categorized by Secure Access. We recommend that you contact Support.
Entered a destination that matches a destination in an existing destination list.	This destination already exists in the destination list.	• Secure Access does not add a destination that already appears in a destination list.

Action	Error Message	Additional Information
Entered a domain name in a destination list that contains more than 253 characters.	Destination too long.	• Check the number of characters in the domain name.

Manage Application Lists

Describes Manage Application Lists in Cisco Secure Access. Secure Access organizes application-based resources into categories based on the type of process or service provided, for example: shopping, education, or human resources.

Secure Access organizes application-based resources into categories based on the type of process or service provided, for example: shopping, education, or human resources. You can add applications or application categories to an application list. Once saved, application lists are available to choose as destinations in your internet access rules.

Use application lists to simplify destination management and apply access rules consistently. However, you can also choose individual applications and entire application categories directly in internet access rules.

For some applications, you can allow access to the application but block activities such as uploads, downloads, or posting. For more information and a list of applications that support these blocks, see Advanced Application Controls.

When a new application is added to a category, Secure Access automatically adds that application to all configuration settings that include that entire category. For each application list, the new application will use the same default action as that applies to the Application category as a whole.

Note: It is not possible to search for an application with fewer than three letters in its name—for example, "QQ" or "YY". These applications must be manually picked from the tree under their respective categories or wildcarded in search—for example, "QQ*". This behavior is by design.

To prevent decryption of traffic to specified applications, see Important Information About Do Not Decrypt Lists.

Add an Application List

Provides instructions for completing the Add an Application List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Secure Access application lists organize application-based destinations into categories. Categories are organized by the type of processes or services provided. Application lists can also include application protocols, which transport the traffic from your organization's sources to internet destinations. An application list may include a single application protocol or a list of application protocols.

To control the traffic to applications, add application categories and application protocols to an Application list. Then, select the application list in an internet rule. You can reuse application lists in multiple internet rules. For information about internet rules, see Components for Internet Access Rules.

Add an application list with applications and application protocols.

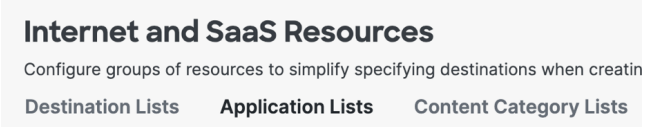
> **Note**
>
> When a new application is added to a category, Secure Access automatically adds that application to all configuration settings that include that entire category. For each application list, the new application will use the same default action as that applies to the Application category as a whole.

Before you begin

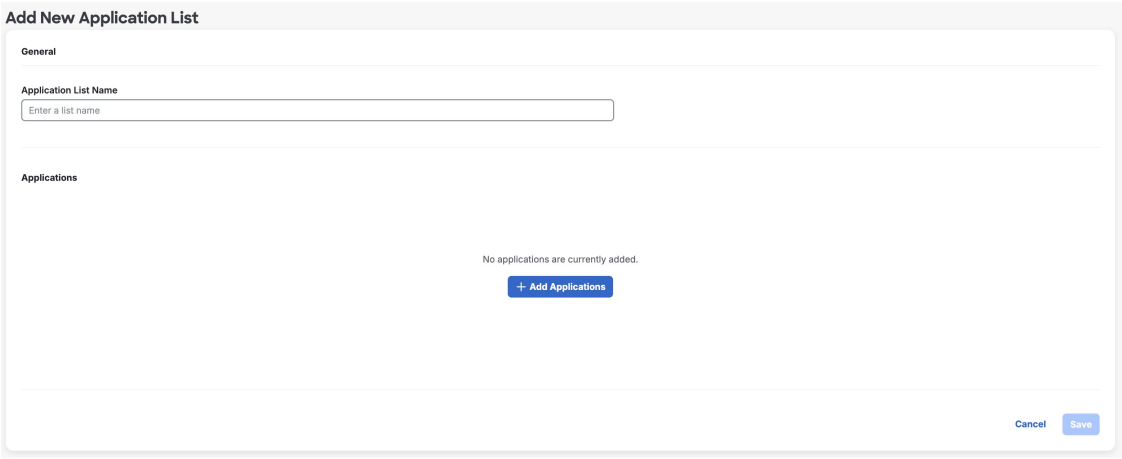
- Full Admin user role. For more information, see Manage Accounts.

Procedure

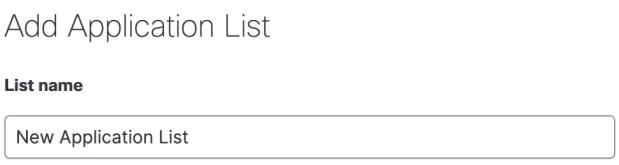
1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists**.



2. Click **Add application list**.

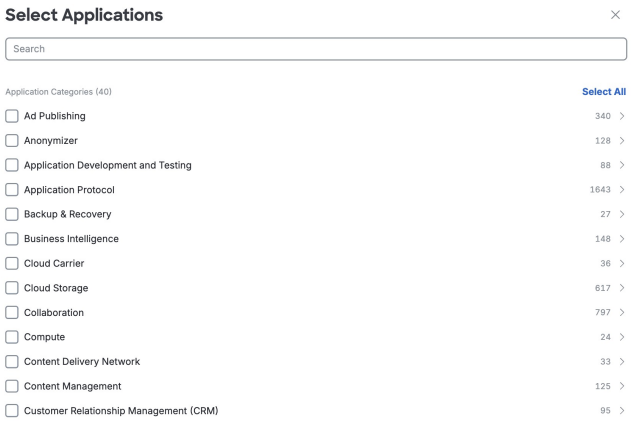


3. For **List name**, enter a descriptive name for the application list.



4. Select applications and application protocols for the application list.
   a. Search for applications and then select applications, or expand each application category and choose the applications within the category. You can also select a category checkbox to include the entire category, or use **Select All** to select the full catalog.

> **Note**
>
> When you select only a few apps within a category, the category is marked with a dash. When you select an entire category, it is marked with a check. You can select the category row to view its applications. For information about the available categories, see Application Categories.

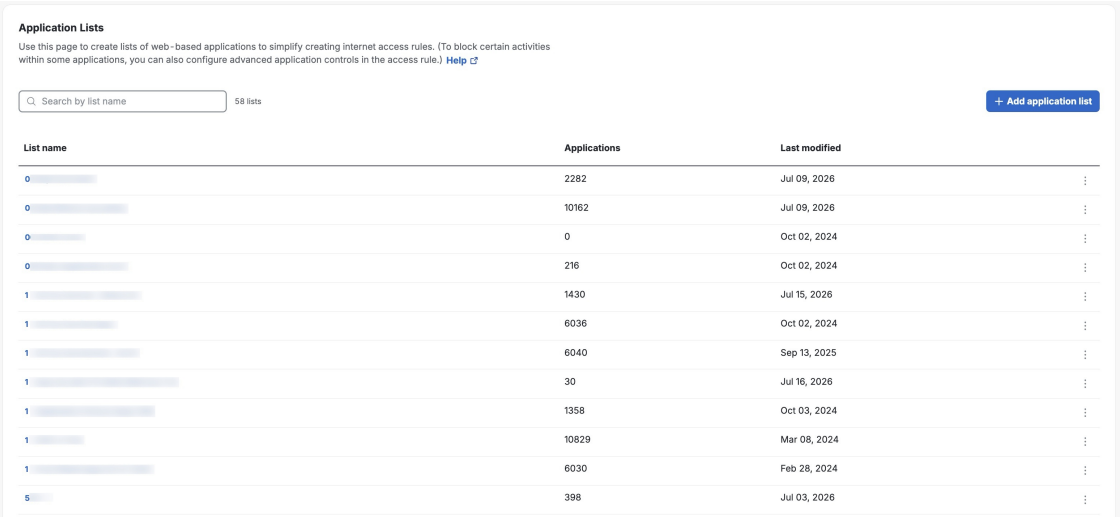


b. Select all application protocols or choose the application protocols to add to the application list.

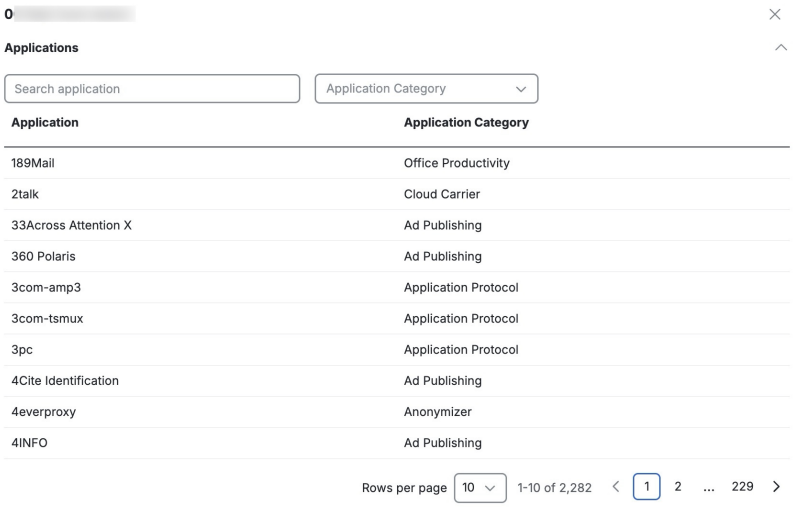


> **Note**
>
> Click **Internet Applications** to return to the category level. Closing the drawer retains the page draft, instead of saving or cancelling the changes you have made. Use the page level **Save** button to save your changes.

5. Click **Save**.



6. To view an application list, click the three dots on the right side of your selected list and select **View details**.



What to do next

After you add the application list, you can select the application list as a destination in an internet rule. For more information, see Add an Internet Access Rule.

For some applications, you can allow access to the application but block activities such as uploads, downloads, or posting. For more information and a list of applications that support these blocks, see Advanced Application Controls

Application Categories

Describes Application Categories in Cisco Secure Access. The system is capable of discovering thousands of apps; these are divided into categories for ease of reference.

The system is capable of discovering thousands of apps; these are divided into categories for ease of reference. Categorization of discoverable apps is conducted by a team of researchers, and based on similarities among apps as well as a number of other quantitative application feature sets.

Category Descriptions

Discovered apps are assigned to the following categories:

- **Ad Publishing**–Applications that enable publishers and ad networks to manage ad serving and trafficking.
- **Anonymizer**–Services that provide an anonymous proxy tool that attempts to make activity on the Internet untraceable.
- **Application Development and Testing**–Applications suited for application development and testing cycles, or for building integration applications in the cloud and within the enterprise.
- **Application Protocols** –Application layer protocols that govern how data is transmitted and received over a network, enabling different services such as web browsing, email, file transfer, and online transactions as well as allowing software applications to communicate with each other. These include SSH, FTP, SMTP and other such applications.
- **Backup and Recovery**–Applications for backup and recovery of file systems and raw data stores on servers and desktop systems.
- **Business Intelligence**–Applications for analytics such as dashboards, reporting systems, scenario modeling, and data analysis.

- **Cloud Broker**–Applications that manage the use, performance, and delivery of cloud services and negotiate relationships between cloud providers and cloud consumers.
- **Cloud Carrier**–Intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers through a network, telecommunication, and other access devices.
- **Cloud Service Provider**–Based on NIST definition of a cloud service, which we believe is being (slowly) adopted as the industry standard. The NIST definition includes the following criteria: on-demand self-service, rapid elasticity, and measured service. CASI additionally adds vendor intent to provide computing-related services (Compute, Network, Storage and/or Software Application). If in doubt whether web or cloud, we will be conservative and assume cloud until we can prove otherwise.
- **Cloud Storage**–Applications that offer massively scalable storage capacity that can be used for applications, and file storage.
- **Collaboration**–Applications that enhance communication and collaboration in workgroups, within enterprises, and across enterprises.
- **Compute**–Fundamental computing resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- **Content Delivery Network (CDN)**–Applications that store content and files to improve the performance and cost of delivering content for web-based systems by offering a large distributed system of servers deployed in multiple data centers across the Internet.
- **Content Management**–Applications for managing the production of and access to content, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
- **Customer Relationship Management (CRM)**–Applications that manage interactions with current and future customers, including organization and automation across sales, marketing, and customer service functions.
- **Database Management**–Applications offering scalable data management solutions for structured or unstructured data, relational database solutions or scalable non-SQL datastores.
- **E-Commerce**–Applications that facilitate the buying and selling of products or services.
- **Education**–Applications that provide educational or training courses, general learning opportunities or specific employee training independent of their location.
- **Enterprise Resource Planning (ERP)**–Applications that manage operations or management of a business; which can include internal and external resources, including tangible assets, financial resources, materials, and human resources.
- **Financial Services**–Applications for managing financial processes and information.
- **Games**–Online and mobile games.
- **Generative AI**–Applications that enable access to large language models (LLM) and artificial intelligence (AI) tools.
- **Healthcare**–Applications that provide access to health, medical, and personal fitness systems.
- **Hosting Services**–Applications that enable corporate or individual websites or other content to be accessible over the internet.
- **Human Resources**–Applications for managing human resources and HR functions.
- **IT Service Management**–Applications that support specific IT functions to plan, deliver, operate and control IT services.
- **Legal**–Applications that provide access to legal documents and public records and support legal content.
- **Marketing & Sales**–Applications that are specifically designed for marketing and sales functions.
- **Media**–Applications that host or stream media as a service.

- **Office Productivity**–Applications for producing information and other standard office-oriented tasks such as documentation, presentations, project management, and so on.
- **Others**–Used for those services where no existing categorization would fit.
- **P2P**–Peer to Peer torrents like apps and protocols.
- **Search**–Web or app-based search.
- **Security**–Applications that support security activities to ensure adherence to regulatory compliance rules and protect information, data applications, and infrastructure.
- **Service Management**–Applications that support general operational activities outside of the IT function.
- **Shopping**–Web or app-based basic online shopping.
- **Social Networking**–Applications that establish and maintain a connection among users that are tied in one or more specific types of interdependency.
- **Software Repository**–Software repositories.
- **Support**–Applications that provide access to customer support services.
- **Travel**–Applications that provide travel management services.
- **Web Content**–Mostly app-based services that provide content. It can be through a login or paid portal.

For some applications, you can allow access to the application but block activities such as uploads, downloads, or posting. For more information and a list of applications that support these blocks, see Advanced Application Controls.

Edit an Application List

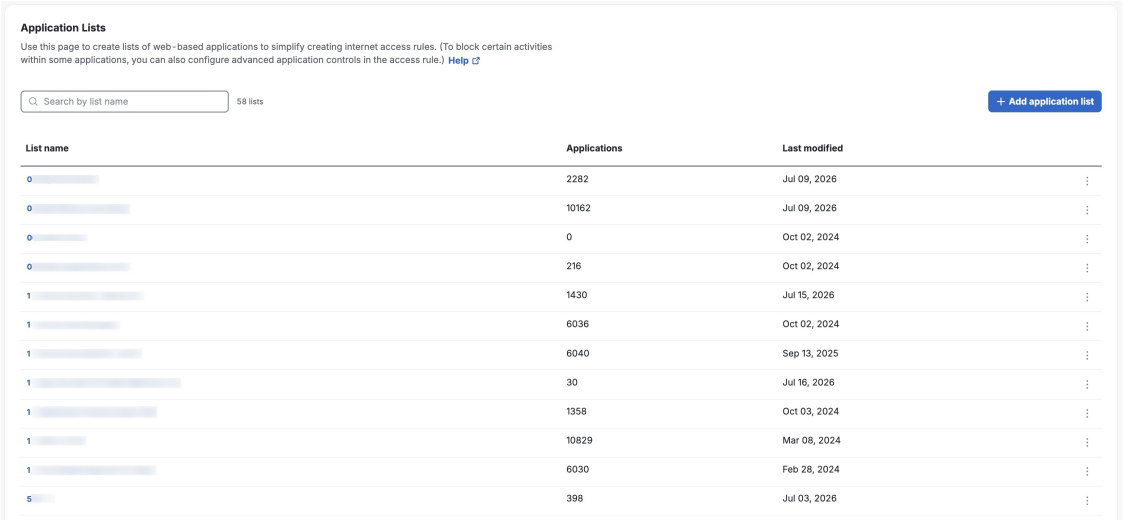
Provides instructions for completing the Edit an Application List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

Full Admin user role. For more information, see Manage Accounts.

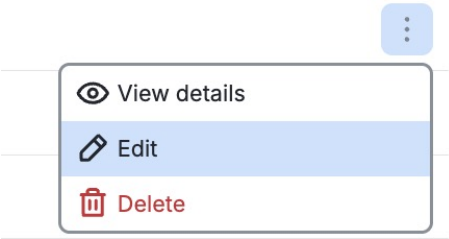
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists**.

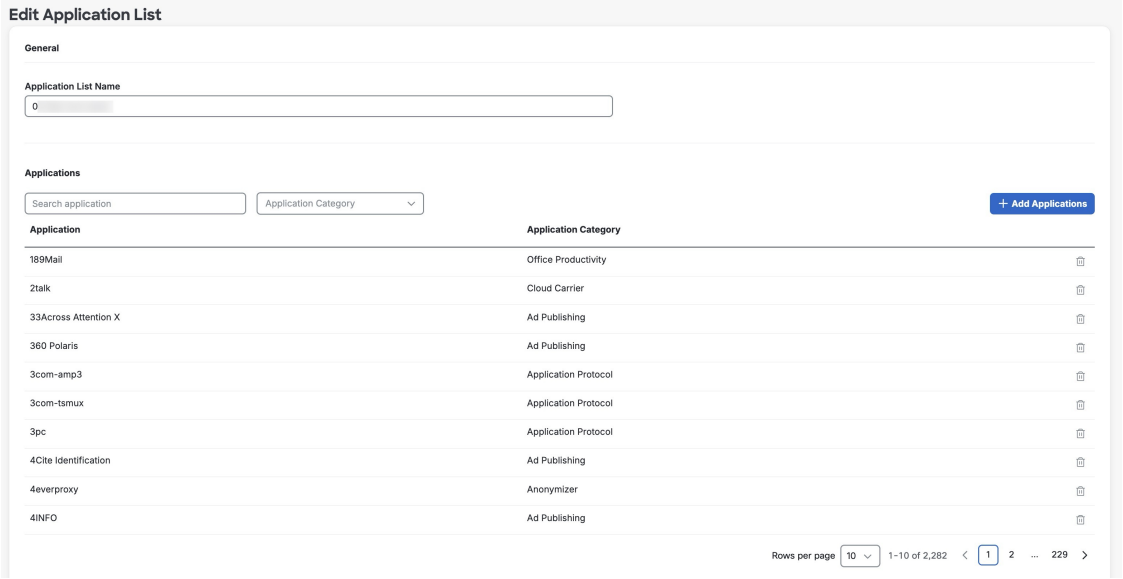


2. Select the three dots **Actions** menu on the right side of your chosen application list.

3. Click **Edit**.



4. Perform any of the following actions:
   - Edit the list name.
   - Search or filter the current applications.
   - Remove applications.
   - Select **Add Applications**.



5. Select **Save** to save your changes to the application list.
   (Optional) Select **Cancel** to discard your changes.
   (Optional Select **Delete** to delete the selected application list.

Delete an Application List

Provides instructions for completing the Delete an Application List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you create an application list, you can delete the list from Secure Access.

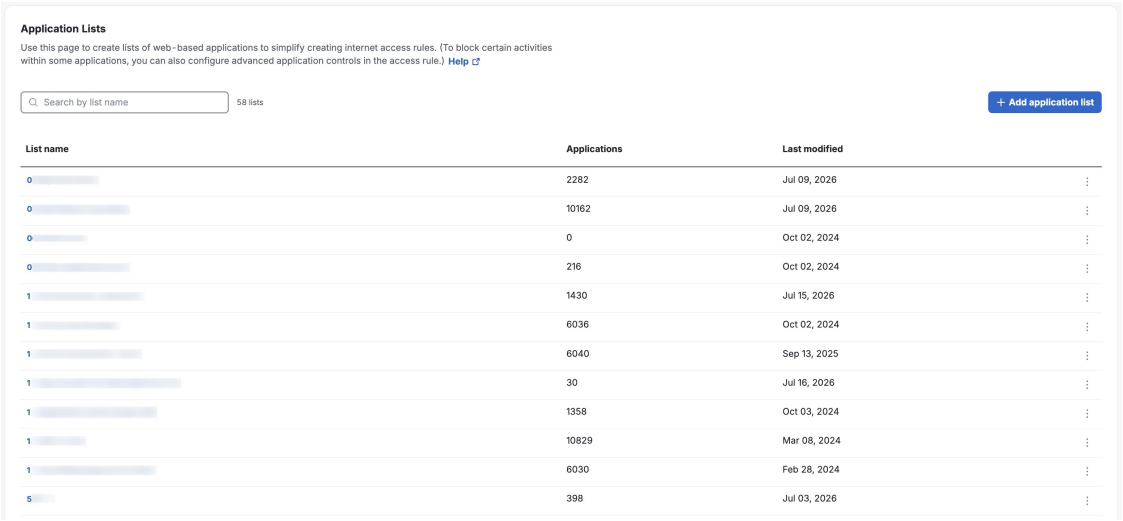
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

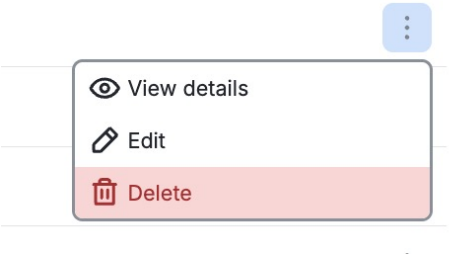
Procedure

---

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Application Lists**.



2. Select the three dots **Actions** menu on the right side of your chosen application list.
3. Click **Delete**.



Note

If the list is used in any rules, you will see a list of those rules. You cannot delete the list if it is used in rules. Delete the list from the rules or delete the rules, then try again.

Manage Content Category Lists

Describes Manage Content Category Lists in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access classifies internet destinations using content-based categories. Examples of content categories are: gambling, social networking, and alcohol.

To speed rule creation and to apply rules consistently to groups of categories, you can create content category lists. For example, you can create a list of categories that you want to block, and another list that you will use in rules with the Warn action.

Then, when you select a destination in an internet access rule, you can select one or more content category lists. You can also select individual categories.

To prevent decryption of traffic to internet destinations based on content category, see Important Information About Do Not Decrypt Lists.

Available Content Categories

Describes Available Content Categories in Cisco Secure Access. You can use the following content categories as destinations in internet access rules.

You can use the following content categories as destinations in internet access rules. Web sites that Cisco Talos classifies as belonging to a category destination are handled by the rule.

- **Adult**–Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers), general information about sex, non-pornographic in nature, genital piercing, adult products or greeting cards, information about sex not in the context of health or disease.
- **Advertisements**–Banner and pop-up advertisements that often accompany a web page, other advertising websites that provide advertisement content. Advertising services and sales are classified as Business and Industry.
- **Alcohol**–Alcohol as a pleasurable activity, beer and wine making, cocktail recipes, liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as Health and Medicine. Bars and restaurants are classified as Dining and Drinking.
- **Animals and Pets**–Information about domestic animals, livestock, service animals, pets and their care. Veterinary services, medicines, and animal health. Pet and animal training, aquariums, zoos, and animal shows. Includes animal shelters, humane societies, animal centric charities, and sanctuaries, bee keeping, training, and animal husbandry; dinosaurs and extinct animals.
- **Arts**–Galleries and exhibitions, artists and art, photography, literature and books, performing arts and theater, musicals, ballet, design, architecture. Cinema and television are classified as Entertainment.
- **Astrology**–Astrology, horoscope, fortune telling, numerology, psychic advice, tarot.
- **Auctions**–Online and offline auctions, auction houses, and classified advertisements.
- **Business and Industry**–Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital, office supplies, industrial equipment (process equipment), machines and mechanical systems, heating equipment, cooling equipment, materials handling equipment, packaging equipment, manufacturing: solids handling, metal fabrication, construction and building, passenger transportation, commerce, industrial design, construction, building materials, shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).
- **Cannabis**–Websites that focus on the recreational and medicinal consumption of cannabis. Sites may include marketing, discussions about legal and regulatory issues, growth and production, paraphernalia, research, and investment in the cannabis industry. Dispensaries, cannabinoid (CBD oil, THC, etc.) based products are also included.
- **Chat and Instant Messaging**–Web-based instant messaging and chat rooms.
- **Cheating and Plagiarism**–Promoting cheating and selling written work, such as term papers, for plagiarism.
- **Child Abuse Content**–Worldwide illegal child sexual abuse content. Secure Access blocks all web requests that match the Child Abuse Content category. Traffic is enforced globally by the secure web gateway (SWG) and default security profile.
- **Cloud and Data Centers**–Platforms used to serve cloud infrastructure or data center hosting to support an organization's applications, services, or data processing. Due to the de-centralized nature of these domains and IP addresses, a more specific category cannot be applied based on content or ownership.
- **Computer Security**–Offering security products and services for corporate and home users.
- **Computers and Internet**–Information about computers and software, such as hardware, software, software support, information for software engineers, programming and networking, website design, the web and Internet in general, computer science, and computer graphics. Freeware and Shareware is a separate category.

- **Conventions, Conferences, and Trade Shows**–Seminars, trade shows, conventions and conferences themed around a particular industry, market, or common interest. May include information about acquiring tickets, registration, abstract or presentation proposal guidelines, workshops, sponsorship details, vendor or exhibitor information, and other marketing or promotional material. This category includes academic, professional, as well as pop-culture events, all of which tend to be a short-lived or annual event.
- **Cryptocurrency**–Online brokerages and websites that enable users to trade cryptocurrencies; information regarding cryptocurrencies including analysis, commentary, advice, performance indexes, and price charts. General information about cryptomining and mining businesses are included in this category but domains and IP addresses directly involved in mining activities are categorized as Cryptomining.
- **Dating**–Dating, online personals, matrimonial agencies.
- **Digital Postcards**–Enabling sending of digital postcards and e-cards.
- **Dining and Drinking**–Eating and drinking establishments, restaurants, bars, taverns, and pubs, restaurant guides and reviews.
- **DIY Projects**–Guidance and information to create, improve, modify, decorate and repair something without the aid of experts or professionals.
- **Encrypted DNS*** – These protocols are typically used as a layer of security and privacy by end-users, but the encryption hides the destination of the request and passes it through a third-party.
- **Dynamic and Residential**–IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.
- **Education**–Education-related, such as schools, colleges, universities, teaching materials, and teachers' resources, technical and vocational training, online training, education issues and policies, financial aid, school funding, standards and testing.
- **Entertainment**–Details or discussion of films, music and bands, television, celebrities and fan websites, entertainment news, celebrity gossip, entertainment venues. Compare the Arts category.
- **Extreme**–Material of a sexually violent or criminal nature, violence and violent behavior, tasteless, often gory photographs, such as autopsy photos, photos of crime scenes, crime and accident victims, excessive obscene material, shock websites.
- **Fashion**–Clothing and fashion, hair salons, cosmetics, accessories, jewelry, perfume, pictures and text relating to body modification, tattoos and piercing, modeling agencies. Dermatological products are classified as Health and Medicine.
- **File Transfer Services**–File transfer services with the primary purpose of providing download services and hosted file sharing.
- **Filter Avoidance**–Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.
- **Finance**–Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as Online Trading.
- **Freeware and Shareware**–Providing downloads of free and shareware software.
- **Gambling**–Casinos and online gambling, bookmakers and odds, gambling advice, competitive racing in a gambling context, sports booking, sports gambling, services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as Health and Medicine. Government-run lotteries are classified as Lotteries.
- **Games**–Various card games, board games, word games, and video games, combat games, sports games, downloadable games, game reviews, cheat sheets, computer games and Internet games, such as role-playing games.

- **Generative AI** - Websites mainly focused on using artificial intelligence models to create content such as text, audio, video, or images based on user prompts. This category does not include sites where generative AI is used only as a minor or supplementary feature.
- **Government and Law**—Government websites, foreign relations, news and information relating to government and elections, information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations, legislation and court decisions, civil rights issues, immigration, patents and copyrights, information relating to law enforcement and correctional systems, crime reporting, law enforcement, and crime statistics.
- **Hacking**—Discussing ways to bypass the security of websites, software, and computers.
- **Hate Speech**—Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity, sites promoting racism, sexism, racist theology, hate music, neo-Nazi organizations, supremacism, Holocaust denial.
- **Health and Medicine**—Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care).
- **Humor**—Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as Adult.
- **Hunting**—Professional or sport hunting, gun clubs and other hunting related sites.
- **Illegal Activities**—Promoting crime, such as stealing, fraud, illegally accessing telephone networks, computer viruses, bombs, and anarchy, websites depicting murder and suicide as well as explaining ways to commit them.
- **Illegal Downloads**—Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as Peer File Transfer.
- **Illegal Drugs**—Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.
- **Infrastructure and Content Delivery Networks**—Content delivery infrastructure and dynamically generated content, websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.
- **Internet of Things**—Domains used to monitor the general health, activity, or aid in the configuration of Internet of Things (IoT) and other network-aware electronics. Additionally these sites may provide software or firmware updates or allow remote access to administer the device. IoT exists in both consumer and professional segments, in products such as printers, televisions, thermostats, system monitoring, automation, and smart appliances.
- **Internet Telephony**—Telephonic services using the internet.
- **Job Search**—Career advice, resume writing and interviewing skills, job placement services, job databanks, permanent and temporary employment agencies, employer websites.
- **Lingerie and Swimsuits**—Intimate apparel and swimwear, especially when modeled.
- **Lotteries**—Sweepstakes, contests, and state-sponsored lotteries.
- **Military**—Military, such as the armed forces, military bases, military organizations, anti-terrorism.
- **Mobile Phones**—Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the Business and Industry category.
- **Museums**—Museums and exhibits, both online and physical, dedicated to preserving information regarding subjects that could be of general interest or highly specialized. Subjects could range from art, history, science, or be of cultural importance.
- **Nature and Conservation**—Sites related to natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation,

forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry).

- **News**–News, headlines, newspapers, television stations, magazines, weather, ski conditions.
- **Non-governmental Organizations**–Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.
- **Non-sexual Nudity**–Nudism and nudity, naturism, nudist camps, artistic nudes.
- **Not Actionable**–Sites that have been inspected but are unreachable or do not have enough content to be assigned a category.
- **Online Communities**–Affinity groups, special interest groups, web newsgroups, message boards. Excludes websites classified as Professional Networking or Social Networking.
- **Online Document Sharing and Collaboration**–Cloud-based software used to create, convert, or edit documents. Collaboration and sharing features may be available with access permissions typically configured by the author. Documents may be stored online or available to download.
- **Online Meetings**–Online meetings, desktop sharing, remote access and other tools that facilitate multi-location collaboration.
- **Online Storage and Backup**–Offsite and peer-to-peer storage for backup, sharing, and hosting.
- **Online Trading**–Online brokerages, websites that enable the user to trade stocks online, information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as Gambling. Other financial services are classified as Finance.
- **Organizational Email**–Websites used to access business email (often via Outlook Web Access).
- **Paranormal**–UFOs, ghosts, cryptid, telekenesis, urban legends and myths.
- **Parked Domains**–Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by 'squatters' hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.
- **Peer File Transfer**–Peer-to-peer file request websites. This does not track the file transfers themselves.
- **Personal Sites**–Websites about and from private individuals, personal homepage servers, websites with personal contents, personal blogs with no particular theme.
- **Personal VPN**–Virtual private network (VPN) sites or tools that are typically for personal use,and, may or may not be approved for corporate usage.
- **Photo Search and Images**–Facilitating the storing and searching for, images, photographs, and clip-art.
- **Politics**–Websites of politicians, political parties, news and information on politics, elections, democracy, and voting.
- **Pornography**–Sexually explicit text or depictions. Includes explicit anime and cartoons, general explicit depictions, other fetish material, explicit chat rooms, sex simulators, strip poker, adult movies, lewd art, web-based explicit email.
- **Private IP Addresses as Host**–Private IP addresses which are used as the host part of a URL. Private IP addresses are meant for internal use behind border routers only, so they are not publicly routable.
- **Professional Networking**–Social networking for the purpose of career or professional development. See also Social Networking.

- **Real Estate**–Information that would support the search for real estate, office and commercial space, real estate listings, such as rentals, apartments, and homes, house building.
- **Recipes and Food**–Sites dedicated to sharing or discussing information about cooking, recipes, and food or non-alcoholic beverages; cultural aspects of cuisine and food; diet descriptions and adherence tips, general nutrition information about foods. Use and instruction on cooking appliances and utensils. Food celebrity, lifestyle, and enthusiast blogs.
- **Reference**–City and state guides, maps, time, reference sources, dictionaries, libraries.
- **Regional Restricted Law (Germany)**–URLs that are restricted in Germany due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Great Britain)**–URLs that are restricted in Great Britain due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Italy)**–URLs that are restricted in Italy due to content which may be unlawful as determined by the regional government.
- **Regional Restricted Law (Poland)**–URLs that are restricted in Poland due to content which may be unlawful as determined by the regional government.
- **Religion**–Religious content, information about religions, religious communities.
- **SaaS and B2B**–Web portals for online business services.
- **Safe for Kids**–Directed at, and specifically approved for, young children.
- **Science and Technology**–Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects, space exploration, meteorology, geography, energy (fossil, nuclear, renewable), communications (telephones, telecommunications).
- **Search Engines and Portals**–Search engines and other initial points of access to information on the Internet.
- **Sex Education**–Factual websites dealing with sex, sexual health, contraception, pregnancy.
- **Shopping**–Bartering, online purchasing, coupons and free offers, general office supplies, online catalogs, online malls.
- **Social Networking**–Social networking. See also Professional Networking.
- **Social Science**–Sciences and history related to society, archaeology, anthropology, cultural studies, history, linguistics, geography, philosophy, psychology, women's studies.
- **Society and Culture**–Family and relationships, ethnicity, social organizations, genealogy, seniors, child-care.
- **Software Updates**–Websites that host updates for software packages.
- **Sports and Recreation**–All sports, professional and amateur, recreational activities, fishing, fantasy sports, public parks, amusement parks, water parks, theme parks, spas.
- **Streaming Audio**–Real-time streaming audio content including Internet radio and audio feeds.
- **Streaming Video**–Real-time streaming video including Internet television, web casts, and video sharing.
- **Terrorism and Violent Extremism**–Terrorist or extremist websites that promote death or violence as part of their ideology. Sites may contain graphic or disturbing images, videos, and text. Some sites may not advocate terrorism but share first-hand material of a violent nature.
- **Tobacco**–Pro-tobacco websites, tobacco manufacturers, pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as Health and Medicine.
- **Transportation**–Personal transportation, information about cars and motorcycles, shopping for new and used cars and motorcycles, car clubs, boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as Sports and Recreation.

- **Travel**–Business and personal travel, travel information, travel resources, travel agents, vacation packages, cruises, lodging and accommodation, travel transportation, flight booking, airfares, car rental, vacation homes.
- **Uncategorized**–Any site (domain, URL, or IP address) that has not been categorized–that does not match a security or content category–is blocked. Note that Cisco Talos does not categorize IP addresses as content, only domains, and URLs. IP addresses found to be malicious are placed into a relevant security category. If a URL does not resolve to a content category, Umbrella looks for the URL's domain for a category. If the domain is not categorized then Umbrella treats the URL as uncategorized.

  Note

  Use caution when enabling this category as it will match any domain or URL that has not been categorized by Cisco Talos. This may have unintended results, blocking access to sites not meant to be blocked. Before enabling this setting, we recommend that you first monitor your "Uncategorized" traffic through the Activity Search report. This will help you determine what type of impact that enabling the Uncategorized content category will have on your organization. For more information about monitoring uncategorised traffic, see Activity Search Report.

- **URL Shortener**–Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink.
- **Weapons**–Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training, general information about guns, other weapons may be included. Government military websites are classified as Military.
- **Web Cache and Archives**–Cached or archived web content often stored for preservation or to decrease load times.
- **Web Hosting**–Website hosting, bandwidth services.
- **Web Page Translation**–Translation of web pages between languages.
- **Web-based Email**–Public web-based email services. Websites enabling individuals to access their company or organizations email service are classified as Organizational Email.

To make a request to categorize an uncategorized destination:

1. Log into talosintellgence.com with your cisco.com credentials.
2. Click **My Account** .
3. Submit a request to recategorize the domain.

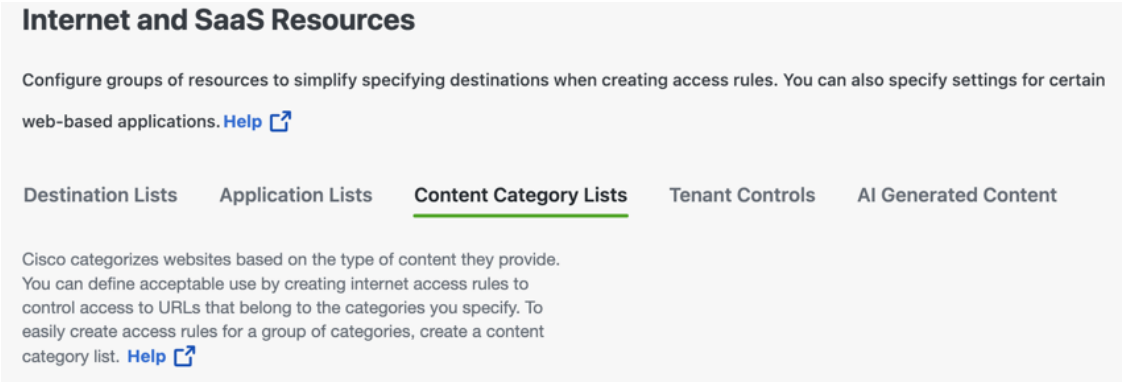
Add a Content Category List

Provides instructions for completing the Add a Content Category List workflow in Cisco Secure Access. Content category lists allow you to speed rule creation and apply rules consistently to groups of categories.

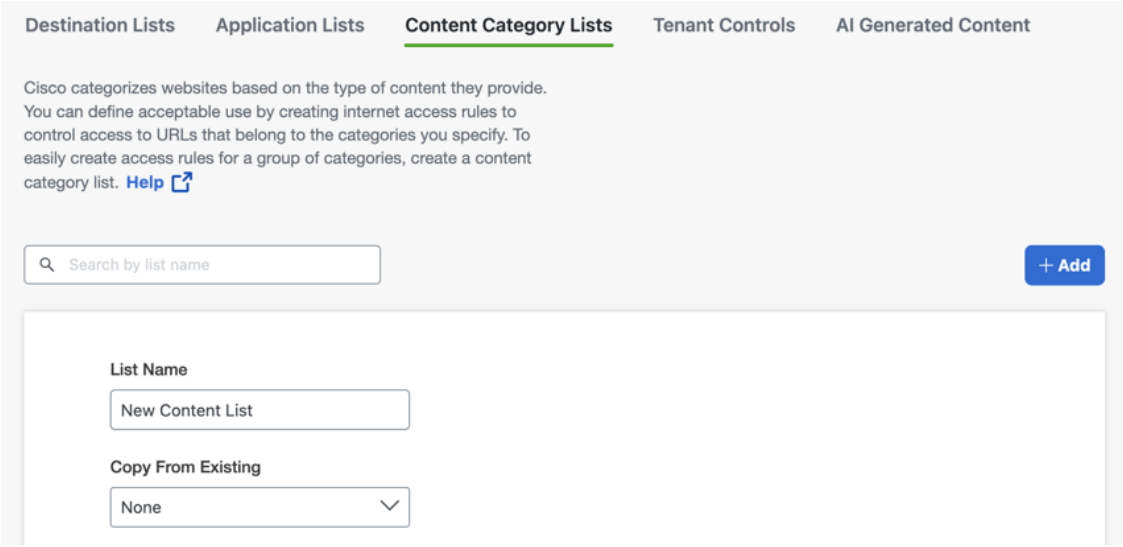
Content category lists allow you to speed rule creation and apply rules consistently to groups of categories.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** > **Content Category Lists**.
2. Click **Add**.



3. Give your configuration a descriptive **List Name**.



4. Select the content categories you want to add to the list.
5. Click **Save**.

   The new Content Category list is now available as a destination in internet access rules.

Delete a Content Category List

Provides instructions for completing the Delete a Content Category List workflow in Cisco Secure Access. Use the following procedure to permanently delete a content category list from your organization.

Use the following procedure to permanently delete a content category list from your organization.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources** and select the **Content Category Lists** tab.
2. Expand the category content list you want to delete.
3. At the bottom of the row of the content category list, click **Delete**.
4. In the pop-up window, click **Delete** again to confirm the action. If you want to keep the list, click **Cancel**.

Request a Category for an Uncategorized Destination

Provides instructions for completing the Request a Category for an Uncategorized Destination workflow in Cisco Secure Access. You must have credentials for your Cisco account.

You can ask Cisco to categorize an uncategorized destination.

Before you begin

- You must have credentials for your Cisco account.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow the onscreen instructions to submit a request to recategorize the domain.

Dispute a Content Category

Provides instructions for completing the Dispute a Content Category workflow in Cisco Secure Access. You must have credentials for your Cisco account.

Secure Access uses the content categories that are maintained by Cisco Talos. If you disagree with a destination's content-category classification, you can dispute it.

Before you begin

- You must have credentials for your Cisco account.

Procedure

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow the onscreen instructions.

View Content Categories in Reports

Describes View Content Categories in Reports in Cisco Secure Access. You can view information about content categories, such as requests that Secure Access blocked because of content categories.

You can view information about content categories, such as requests that Secure Access blocked because of content categories.

Prerequisites

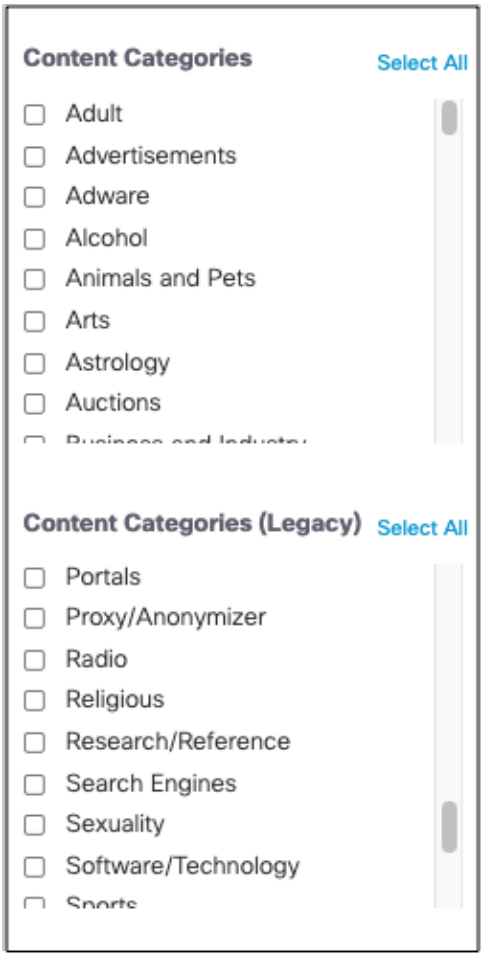
- A minimum user role of Read-only. For more information, see Manage Accounts.

View Content Categories in Activity Search Report

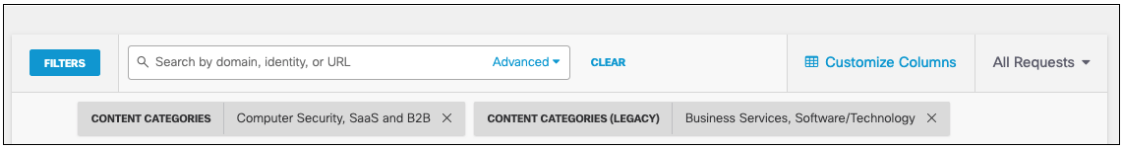
Provides instructions for completing the View Content Categories in Activity Search Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. Scroll down to Content Categories and select your desired filters.



Your filtered categories appear at the top of the report.



The Categories column of the report displays both legacy and new Talos content categories.

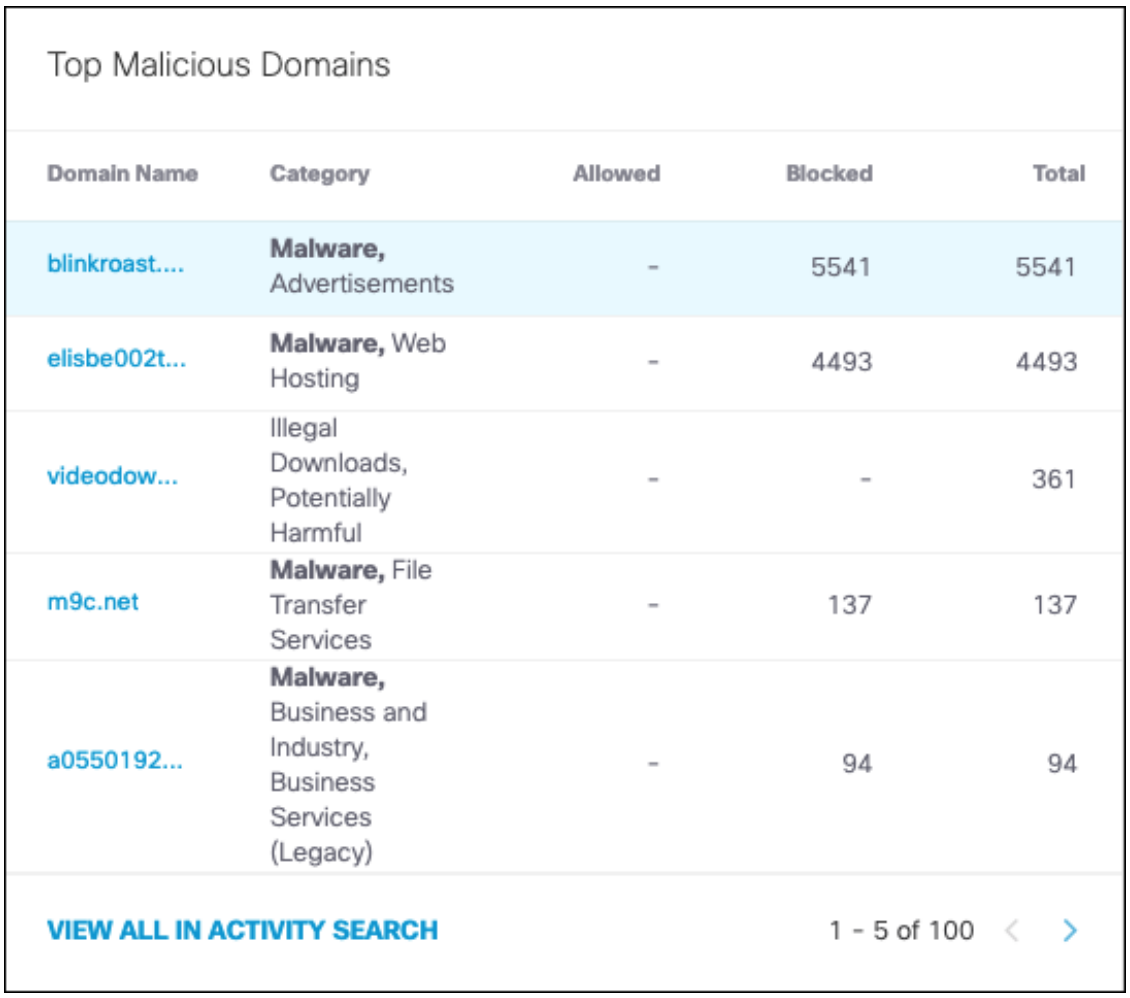
Categories
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Business Services (Legacy), Computer Security, SaaS and B2B
Software/Technology (Legacy), Cloud and Data Centers
Software/Technology (Legacy), Cloud and Data Centers
Software/Technology (Legacy), SaaS and B2B
Software/Technology (Legacy), Computers and Internet
Software/Technology (Legacy), Computers and Internet
Software/Technology (Legacy), SaaS and B2B

View Content Categories in Top Threats Report

Provides instructions for completing the View Content Categories in Top Threats Report workflow in Cisco Secure Access. Navigate to Monitor Top Threats Top Malicious Domains .

Procedure

Navigate to **Monitor** > **Top Threats** > **Top Malicious Domains**.

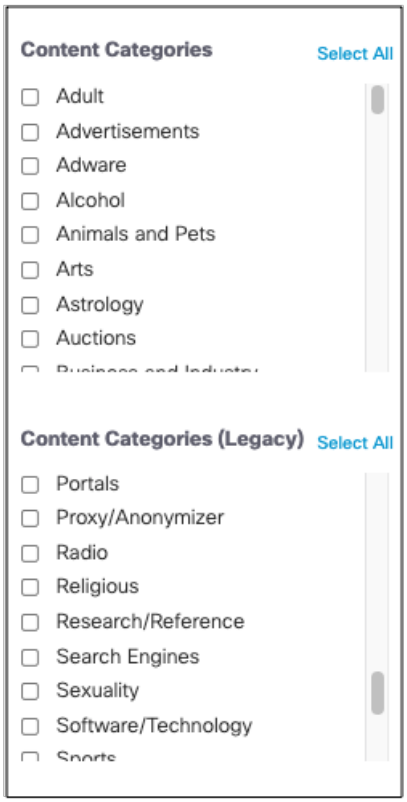


View Content Categories in Total Requests Report

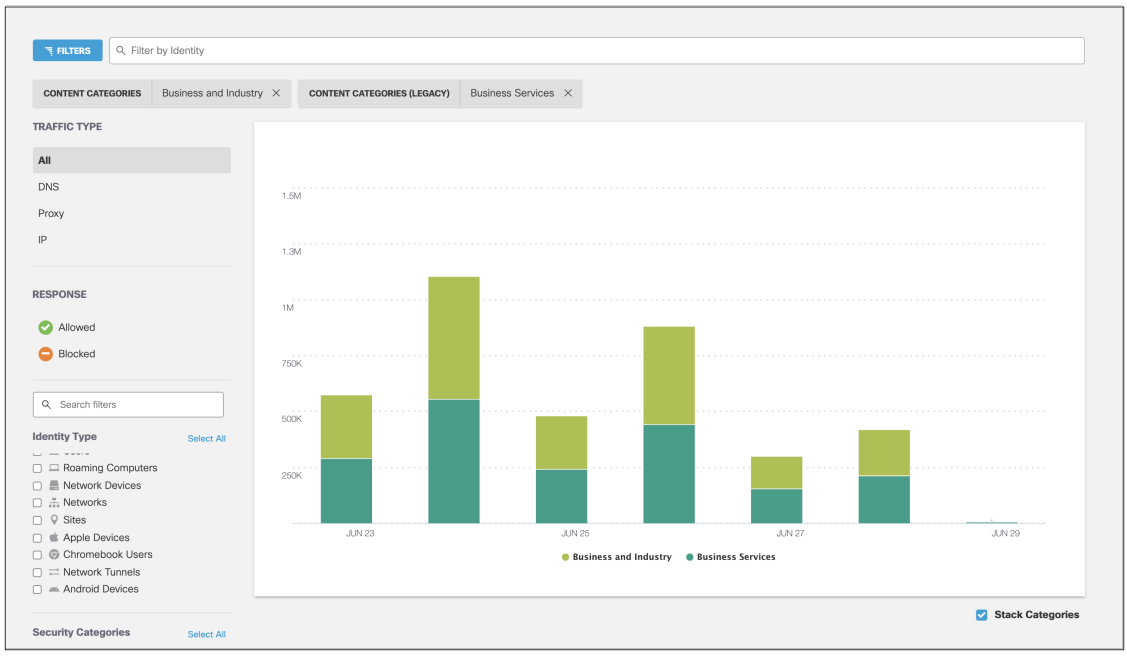
Provides instructions for completing the View Content Categories in Total Requests Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Additional Reports** > **Total Requests**.
2. Filter by content categories. Click **Apply**.



The graph displays data for the selected Talos content categories.



View Content Categories in Activity Volume Report

Provides instructions for completing the View Content Categories in Activity Volume Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

Navigate to **Monitor** > **Additional Reports** > **Activity Volume**. The table displays data for both the Talos content categories.

Requests

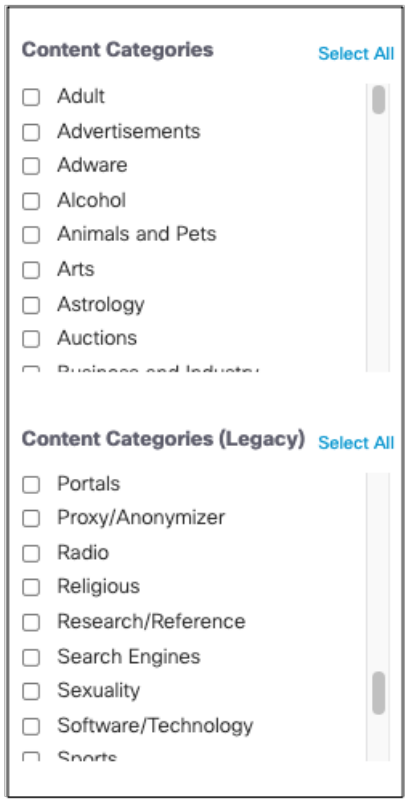
Name	Allowed	Blocked	Total	% of Total
⊕ Security	8,465	11	8,476	3.18%
Categories	-	294	294	0.11%
Categories (Legacy)	-	0	0	0.00%
Destination Lists	0	0	0	0.00%
Permitted	257,994	-	257,994	96.71%
Total	266,459	305	266,764	100%

View Content Categories in Top Destinations Report

Provides instructions for completing the View Content Categories in Top Destinations Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Top Destinations**.
2. Filter by content categories.



The category column of the report displays the Talos content categories.

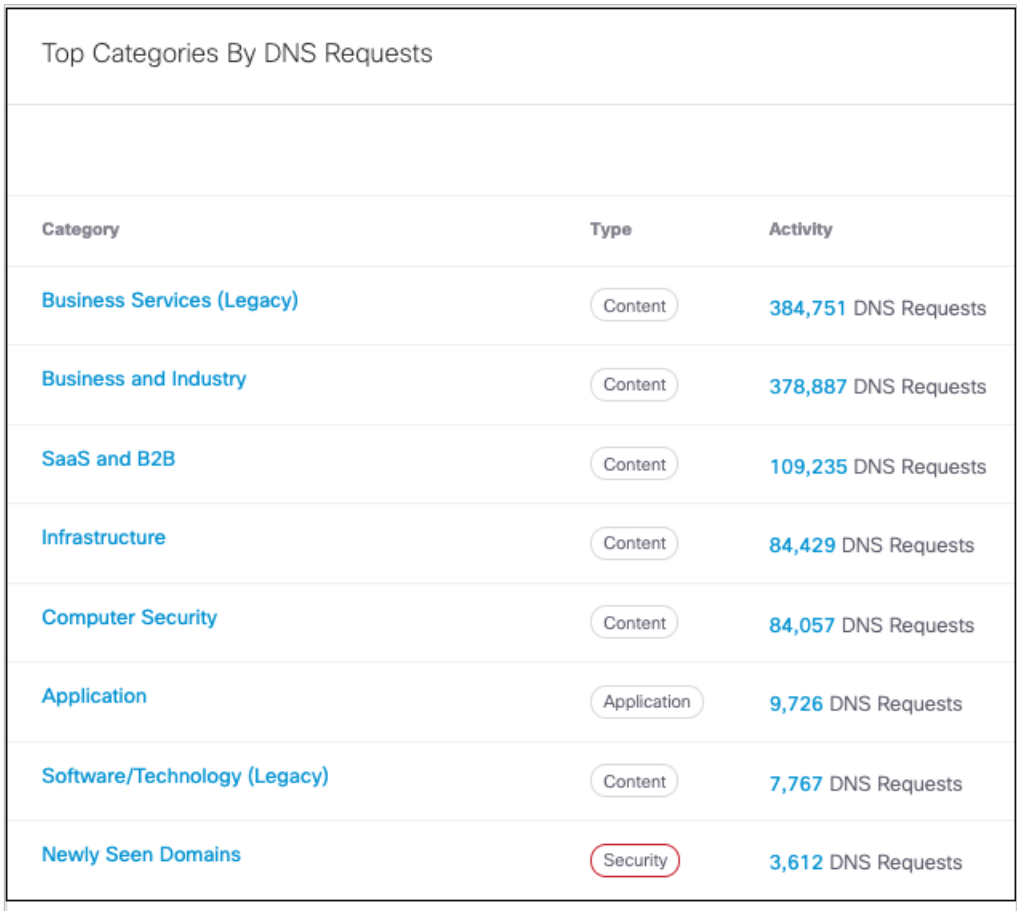
47990.xc.zhongguohao123.com	**Malware,** Business and Industry, Business Services (Legacy)
dl.dell.com	Computers and Internet, Ecommerce/Shopping (Legacy), Infrastructure, Software/Technology (Legacy), Business Services (Legacy)
47992.xc.zhongguohao123.com	**Malware,** Business and Industry, Business Services (Legacy)

View Content Categories in Top Categories Report

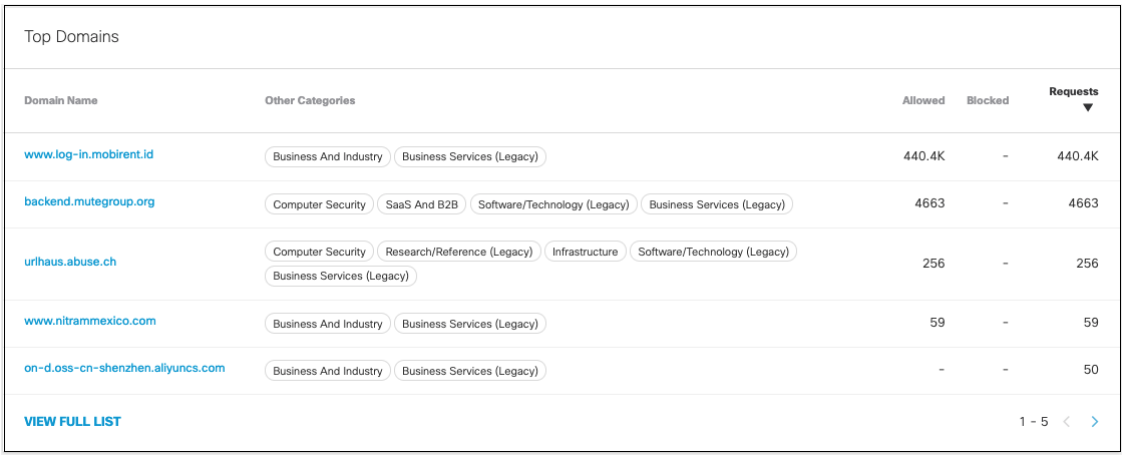
Provides instructions for completing the View Content Categories in Top Categories Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Top Categories**. The category column of the report displays the Talos content categories.



2. Click a category to see its details.
   - If you scroll down to**Top Domains,** in the Other Categories column, you can see the Talos content categories among the categories.



Manage Tenant Control Profiles

Describes Manage Tenant Control Profiles in Cisco Secure Access.

Secure Access tenant controls allow you to provision user connectivity to certain SaaS applications in the cloud. After the tenant is configured, access is limited to only those resources that are approved for your organization. The result is that your organization is protected and secure when users and devices reach those resources in the cloud that are running on shared domain names.

Secure Access supports tenant controls for the following platforms:

- Microsoft 365
- Google G Suite
- Slack
- Dropbox
- YouTube
- ChatGPT
- GitHub

You can create tenant control profiles for one or more applications.

To use a tenant control profile in an access rule, see Use Tenant Controls in Access Rules.

Control Cloud Access to Microsoft 365

Provides instructions for completing the Control Cloud Access to Microsoft 365 workflow in Cisco Secure Access. You must have full admin permission in Secure Access.

Use a tenant-control profile to manage access to the cloud-based application Microsoft 365. Once added, you can select the profile in an internet-access rule.

Microsoft 365 Compatibility allows Microsoft 365 traffic to pass through Secure Access without inspection or policy enforcement. This lets the traffic pass through Secure Access unaltered. Secure Access decrypts, the following Microsoft login domains:

- **login.microsoftonline.com**

- **login.live.com**
- **login.microsoft.com**
- **login.windows.net**

which decryption enables enforcement of tenant restrictions.

For more information, see the official Microsoft documentation and Microsoft 365 Compatibility.

> **Note**
>
> Microsoft 365 tenant restrictions do not block personal or consumer accounts, such as Hotmail or Outlook.

Before you begin

- You must have full admin permission in Secure Access. For more information, see Manage Accounts.
- You need the **Tenant Domain** and **Tenant Directory ID** to configure Tenant Controls settings and allow access to the cloud-based application Microsoft 365.

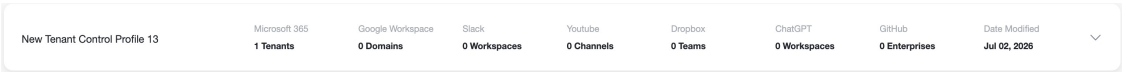
  For more information about this data and how to acquire it, see Azure Active Directory documentation.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources**.
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

   Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.

   > **Note**
   >
   > If you do not configure Tenant Control settings for a ruleset, Secure Access uses the default control settings.

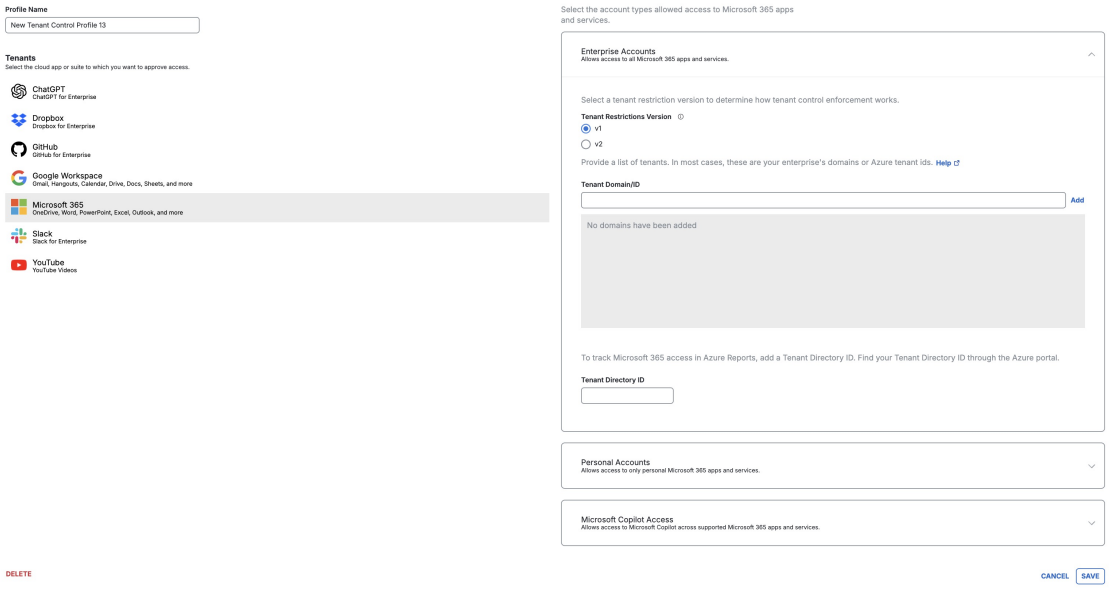


4. Choose the version of tenant restrictions you want to configure and follow the corresponding steps below.
5. To configure Tenant Restriction Version 1 (v1):
   a) Click the **Tenant Restriction Version 1 (v1)** radio button, to add a Microsoft 365 tenant domain to your organization.
   b) Add your organization's Microsoft 365 **Tenant Domain/ID** and click **Add**.

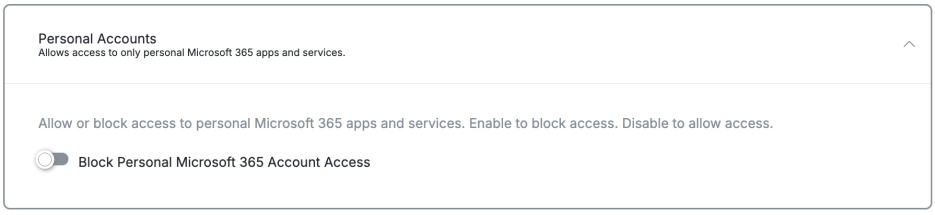
> **Note**
>
> You can add multiple Tenant Domains.

c) (Optional) Add your organization's **Tenant Directory ID** for Microsoft 365 to track Office 365 access in Azure reports.

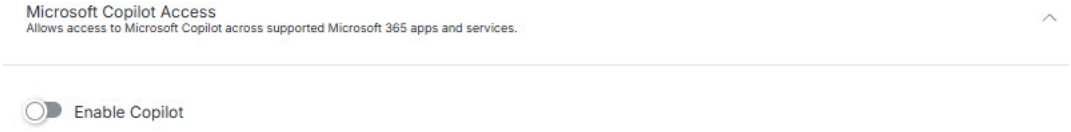
> **Note**
>
> For more information about how to acquire the Tenant Directory ID, see Microsoft's documentation or contact Microsoft Support.



d) (Optional) Click the **Block Personal Microsoft 365 accounts** toggle to restrict access to personal accounts.



e) (Optional) Click the **Enable Copilot** toggle button to allow Microsoft Copilot to access Microsoft 365 applications and services.

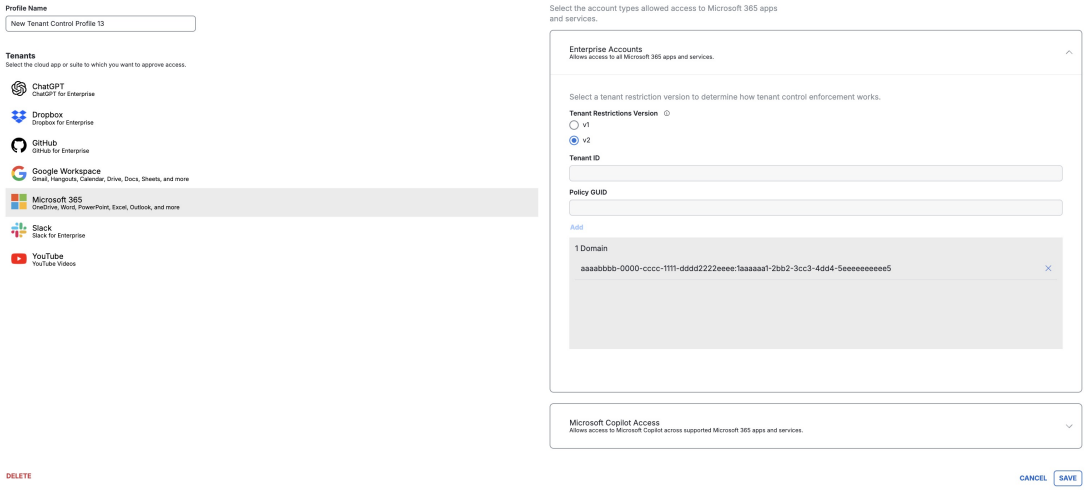


6. Configure Tenant Restriction Version 2 (v2).

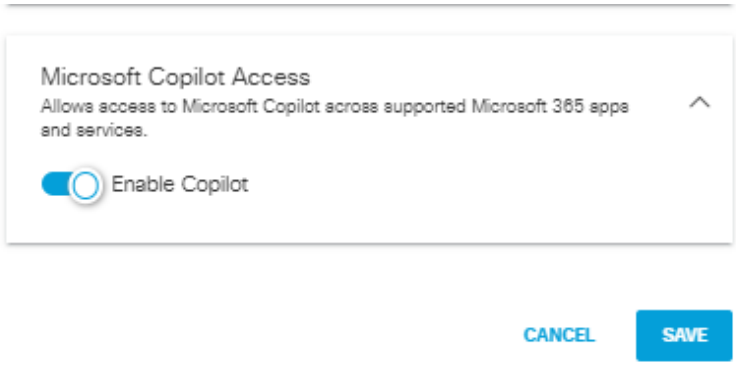
a) Click the **Tenant Restriction Version 2 (v2)** radio button, to add a list of tenants, such as enterprise domains or Azure tenant IDs to your organization.

b) Add your organization's Microsoft 365 **Tenant ID** and **Policy GUID**, then click **Add**.

> **Note**
>
> You can obtain your Microsoft 365 Tenant ID and Policy GUID from the Microsoft Entra portal at entramicrosoft.com. Refer to https://learn.microsoft.com/en-us/entra/external-id/tenant-restrictions-v2#compare-tenant-restrictions-v1-and-v2.



c) (Optional) Click the **Enable Copilot** toggle button to allow Microsoft Copilot to access Microsoft 365 applications and services.



7. Click **Save**.

   The new Tenant Controls profile is now available for selection when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Google Workspace

Provides instructions for completing the Control Cloud Access to Google Workspace workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Secure Access tenant controls profile manages access to the cloud-based application Google Workspace (formerly Google G Suite). Once added, you can select this profile in an internet access rule.

Limitations

- You can manage Google Workspace access only on the domain level; Secure Access does not support managing access for individual Gmail accounts.

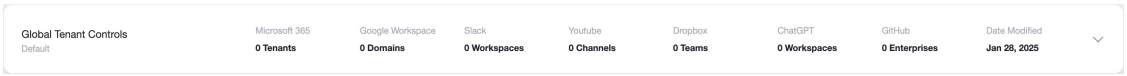
Before you begin

- Full admin user role. For more information, see Manage Accounts.
- The following Google Workspace specific data is required to configure Tenant Controls settings and allow access to to the cloud-based suite Google Workspace:
  - **Domains**. For more information about this data and how to acquire it, scroll to "Use a web proxy server to block accounts" in Google Workspace Admin Help.
  - **Google Workspace**. A Google Workspace account must be associated with your domain.

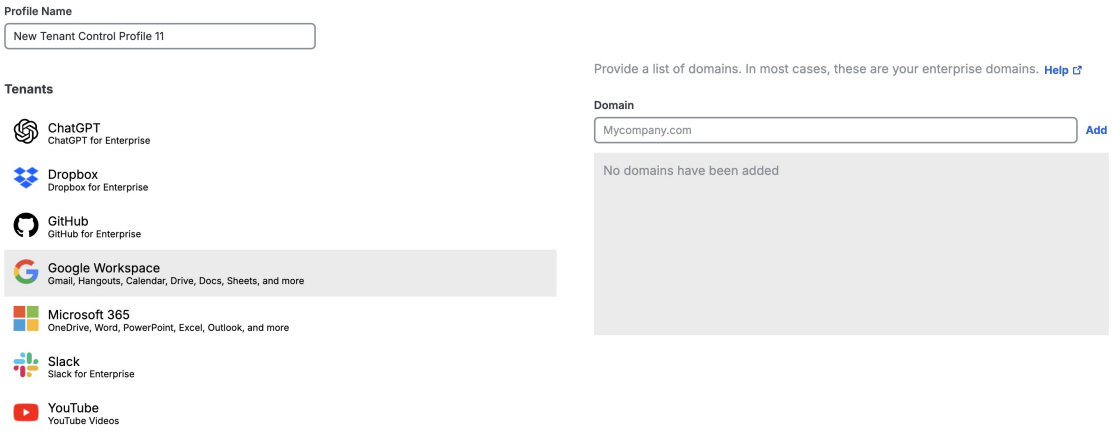
Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources**
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.



4. Give your configuration a descriptive **Profile Name** and select **Google Workspace**.



5. Grant access to Google Workspace from within your organization.
   a) Add an enterprise domain and click **Add**.

      You can add multiple domains.

6. Click **Save**.

   The new Tenant Controls setting is now available for selection when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Slack

Provides instructions for completing the Control Cloud Access to Slack workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Secure Access tenant controls profile manages access to the cloud-based application Slack.

Before you begin

- Full admin user role. For more information, see Manage Accounts.
- Slack requires the following data to configure tenant controls for access to the cloud-based application:
  - **Workspace ID**
  - **Requester ID** (for Business+ or Enterprise Slack Workspace ID)

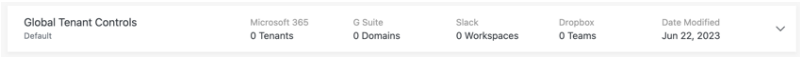
  For more information about this data, see Approve Slack workspaces for your network.

Procedure

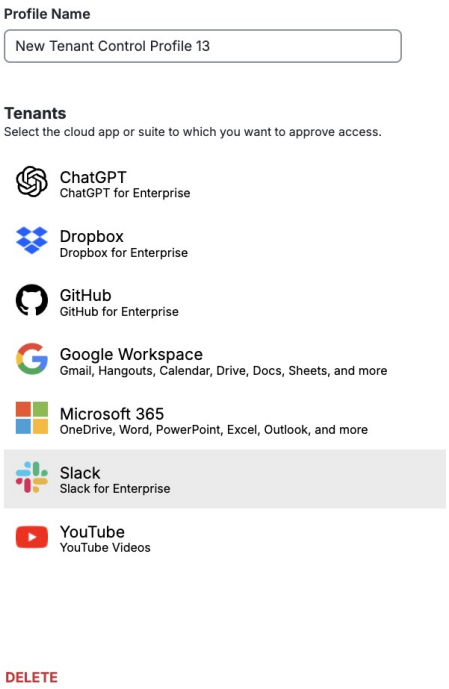
1. Navigate to **Resources** > **Internet and SaaS Resources**.
2. Select **Tenant Controls.**
3. Click **Add** or expand the default **Global Tenant Controls** profile.

   Note

   Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.

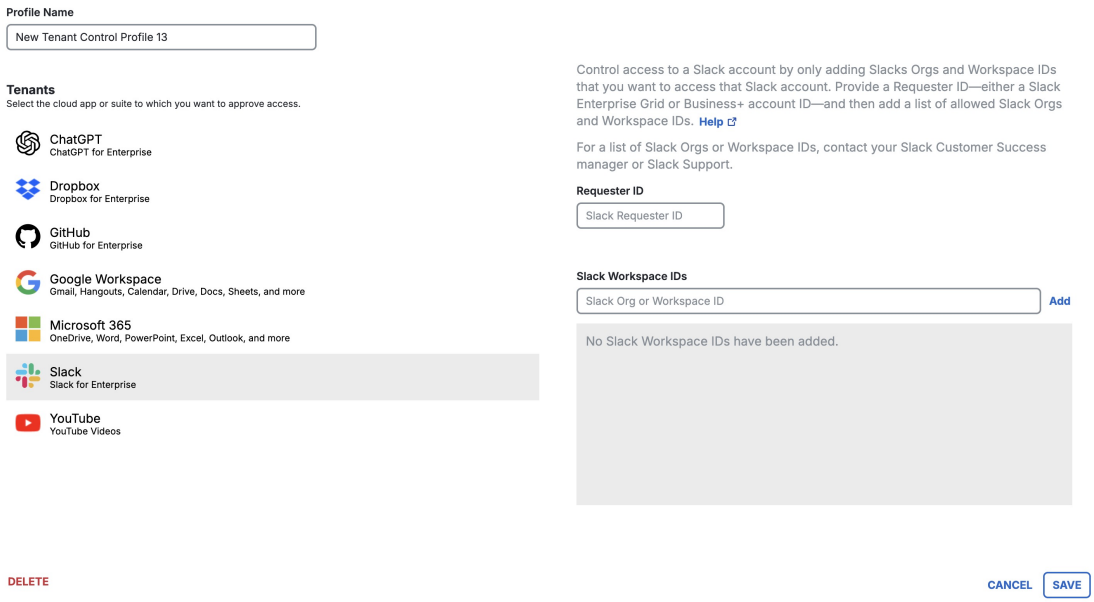


4. Give your configuration a descriptive **Profile Name** and select **Slack**.



5. Grant access to Slack from within your organization.
   a) Enter a **Requester ID** and a **Workspace ID**.

      You can add multiple workspace IDs.



6. Click **Save**.

   The new tenant controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to Dropbox

Provides instructions for completing the Control Cloud Access to Dropbox workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Secure Access tenant controls profile manages access to the cloud-based application Dropbox.

Before you begin

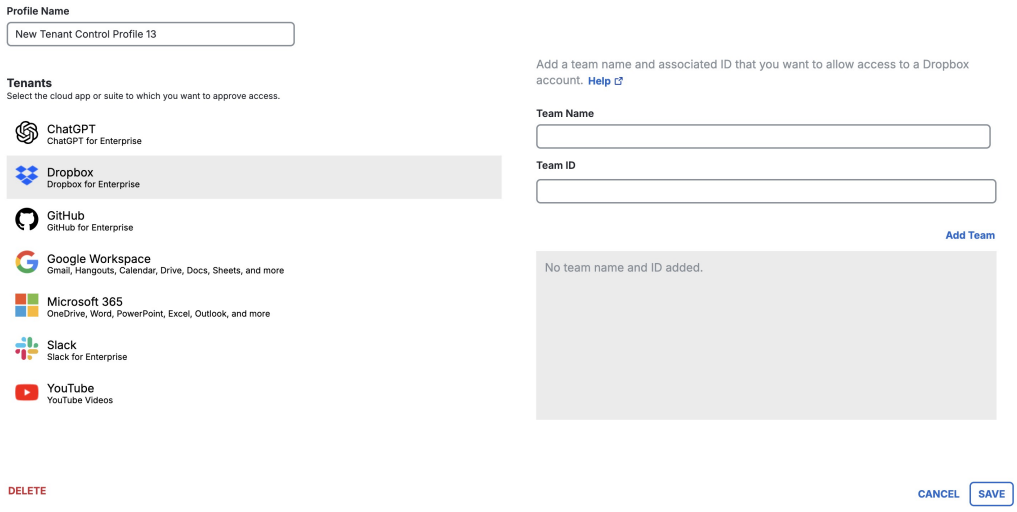
- Full admin user role. For more information, see Manage Accounts.
- Dropbox requires the following data to configure tenant controls for access to the cloud-based application:
  - Team Name. Choose the Team Name to provide a mnemonic identifier for the team.
  - Team ID. For information about the Team ID and how to find it using Dropbox developer tools, see Dropbox for HTTP developers.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources.**.
2. Select **Tenant Controls**.
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.

4. Give your configuration a good descriptive **Profile Name** and select **Dropbox**.
5. Grant access to Dropbox from within your organization.
   a) Enter a **Team Name** and a **Team ID**. You can add multiple teams.



6. Click **Save**.

The new Tenant Controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to YouTube

This procedure describes how to add new tenant control settings to Secure Access and enable access to the cloud-based application, YouTube.

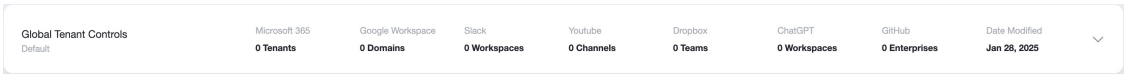
Before you begin

- Full admin user role. For more information, see Manage Accounts.
- YouTube-specific data is required to configure tenant controls and allow access to the cloud-based application:
  - YouTube Channels
  - YouTube Categories

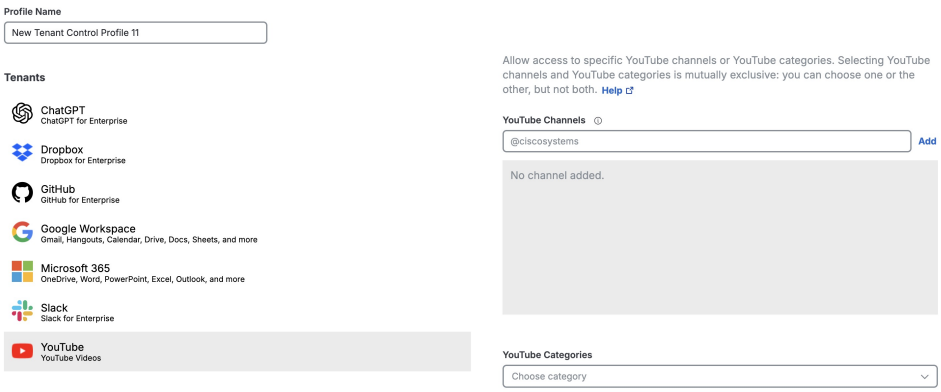
Procedure

1. Navigate to **Resources > Internet and SaaS Resources.**
2. Select **Tenant Controls**.
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant control is enabled by default for a rule. A rule uses the default global tenant control profile if no other tenant control profile is configured for that rule.

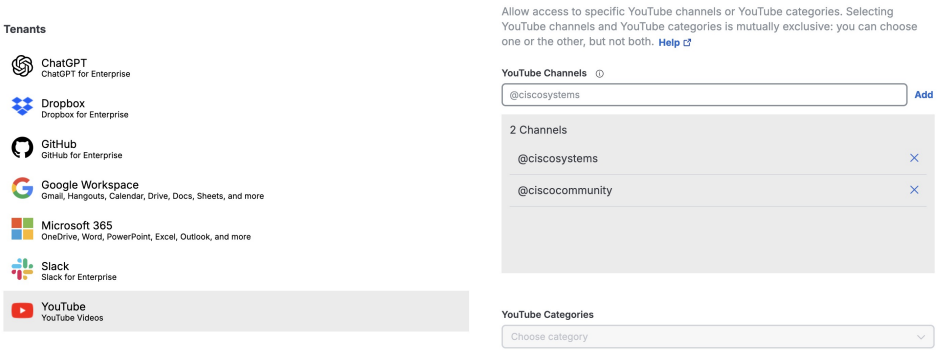


4. Give your configuration a descriptive **Profile Name** and click **YouTube**.

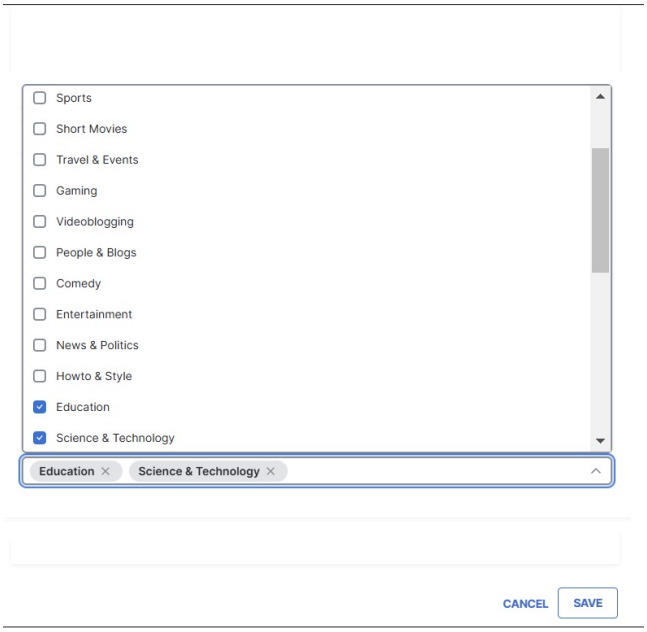


5. Grant access to YouTube from within your organization.
   a) Enter the channel handle in the **YouTube Channels** field and click **Add**.

> **Note**
>
> You can add multiple channels using the respective channel handles. For example: **@ciscosystems** and **@ciscocommunity**.



6. Optionally, choose categories from the **YouTube Categories** drop-down list, for example, **Education, Science & Technology**.



7. Click **Save**.

Blocking Behavior for YouTube Tenant Control

Learn how the YouTube Tenant Control feature handles blocked requests during direct URL access and in-app navigation.

When the YouTube Tenant Control feature is enabled, the blocking behavior varies depending on how the user accesses the content. The following scenarios describe the expected user experience when a request is blocked.

Direct Video Access

This scenario occurs when a user attempts to access a specific video directly. This includes the following actions:

- User pastes a YouTube video URL directly into the browser.
- User bookmarks and opens a specific video.
- User refreshes an already opened video page.

If the request is blocked in this scenario, the user experiences the following:

- The browser is redirected to the organization's block page.
- The block page loads normally.
- The user clearly sees that access to the video is restricted.

In-app Navigation

This scenario occurs when a user navigates to a video from within the YouTube interface. This includes the following actions:

- User opens YouTube.
- User clicks a video from the homepage feed.
- User clicks a suggested video while browsing.

If the request is blocked in this scenario, the user experiences the following:

- The video player does not load the video.
- The browser is not redirected to the block page; instead, the video player displays an error message.
- The page remains on YouTube.
- The video area displays a playback error, such as:
  - "An error occurred."
  - "Playback error."
  - A spinning loader followed by failure.

Control Access to ChatGPT

Provides instructions for completing the Control Access to ChatGPT workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Secure Access tenant controls profile manages access to the cloud-based AI application ChatGPT.

Before you begin

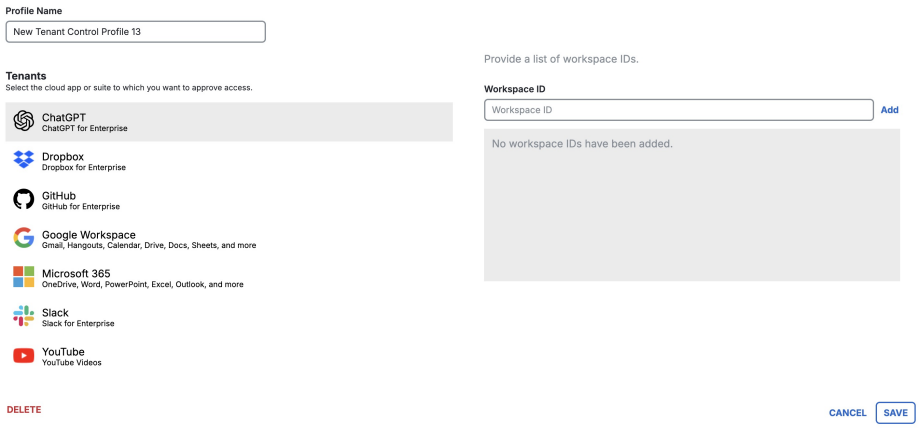
- Full admin user rule. For more information, see Manage Accounts.
- You must have your ChatGPT Workspace ID to configure tenant controls for access to ChatGPT.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources**.
2. Select **Tenant Controls**.
3. Click **Add** or expand the default **Global Tenant Controls** profile.

> **Note**
>
> Tenant controls is enabled by default for a rule. A rule uses the default global tenant controls profile if no other tenant controls profile is configured for that rule.

4. Give your configuration a good descriptive **Profile Name** and select **ChatGPT**.



5. Grant access to ChatGPT from within your organization. Enter a **Workspace ID** and click **Add**.

   You may enter multiple workspace IDs.

6. Click **Save**.

   The new Tenant Controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Control Cloud Access to GitHub

This procedure describes how to restrict access to the cloud-based application, GitHub using corporate proxy.

The Cisco Secure Access tenant controls profile manages access to the cloud-based application GitHub. After you add the profile, you can select this profile in an internet access rule (access policy) to restrict access to unsanctioned GitHub tenants.

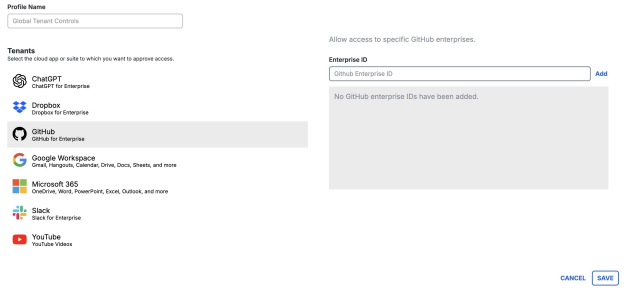
Before you begin

- Full admin user role. For more information, see Manage Accounts.
- Your GitHub enterprise must use managed users on GitHub.com.
- Secure Access requires **Enterprise ID** to configure tenant controls for access to the cloud-based application, GitHub.

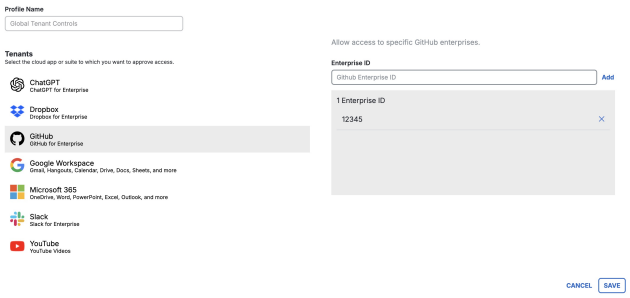
  For more information, refer to the Find the header section in Enterprise administrator documentation.
- Ensure that your GitHub usernames include your enterprise shortcode to confirm that users belong to your organization. If you use a subdomain of GitHub Enterprise (GHE.com), the header is not required to distinguish traffic to your enterprise resources.
- Your GitHub enterprise owner must enable the enterprise access restriction feature.

Procedure

1. In Cisco Secure Access, navigate to **Resources** > **Internet and SaaS Resources**.
2. Click **Tenant Controls**.
3. Click **Add**, or expand the default **Global Tenant Controls** profile.
4. Enter a descriptive profile name, and select **GitHub**.



5. In the **Enterprise ID** field, enter the **Enterprise ID** that you copied from GitHub.
6. Click **Save**.



The new tenant controls profile is now available when you add an internet access rule. For rule requirements specific to tenant controls, see Use Tenant Controls in Access Rules.

Edit or Delete a Tenant Control Profile

Provides instructions for completing the Edit or Delete a Tenant Control Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

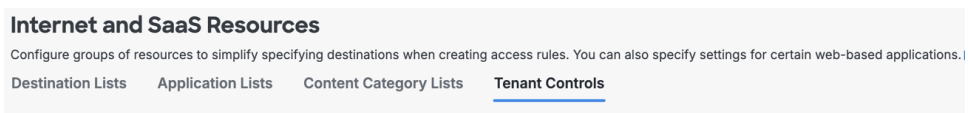
Once you add a Tenant Control profile in your organization, you can edit or remove the profile.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Internet and SaaS Resources**, and then click **Tenant Controls**.

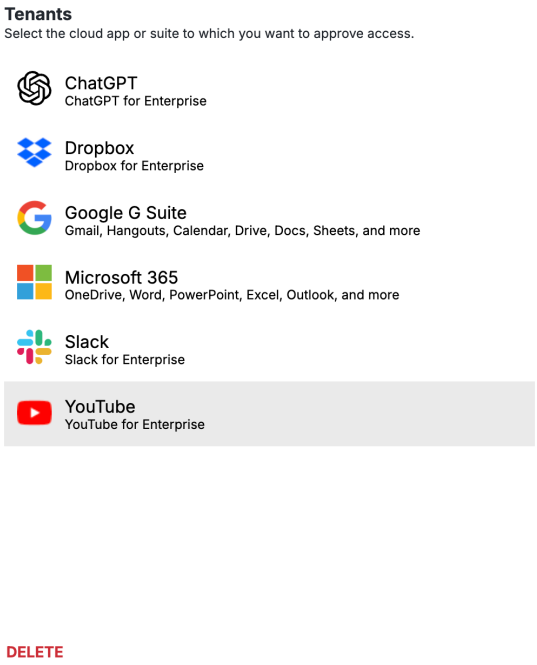


2. Expand a Tenant Control profile.
3. (Optional) Edit the Tenant Control profile and then click **Save**.

For more information, see one of the guides that describe how to add a Tenant Control profile.

- Control Cloud Access to Microsoft 365
- Control Cloud Access to Google G Suite
- Control Cloud Access to Slack
- Control Cloud Access to DropBox
- Control Cloud Access to YouTube
- Control Cloud Access to ChatGPT
- Control Cloud Access to GitHub

4. To remove the Tenant Control profile, click **Delete**.



Use Tenant Controls in Access Rules

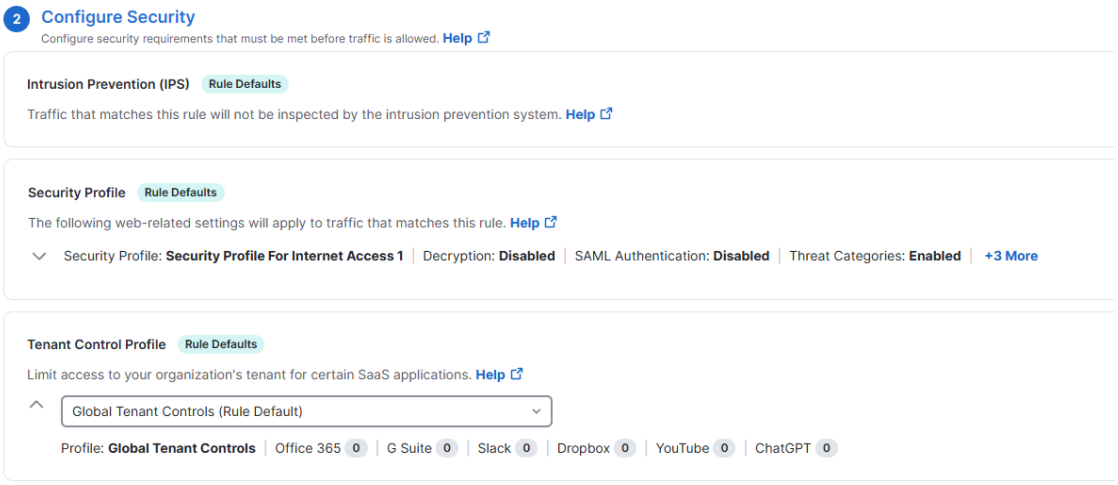
Describes Use Tenant Controls in Access Rules in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To use tenant controls in internet-access rules:

- Add tenant control profiles for the applications that require such controls.
- Decryption must be enabled for the rule. Make sure it is enabled in the security profile selected in the rule.
- The option to select a tenant control profile appears in the Security Controls section of the rule (after you choose destinations and then click Next.)
- If you enable Microsoft 365 Compatibility in Global Settings:

  Microsoft 365 Compatibility is compatible with Tenant Controls. However, when Tenant Controls are configured for Microsoft 365, Secure Access decrypts three Microsoft login domains (login.microsoftonline.com, login.microsoft.com, and login.windows.net) for the purpose of tenant enforcement. The domain is detected by analyzing the SNI (Server

Name Indication) TLS extension. Some applications may not send SNI information in which case the exclusion does not apply. For more information about Microsoft 365 Compatibility, see Global Settings for Access Rules.



Review Tenant Controls Through Reports

Provides instructions for completing the Review Tenant Controls Through Reports workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the Activity Search report to view identity activity when you're tracking attempts to access cloud-based applications that are controlled by the tenant-controls profile.

Before you begin

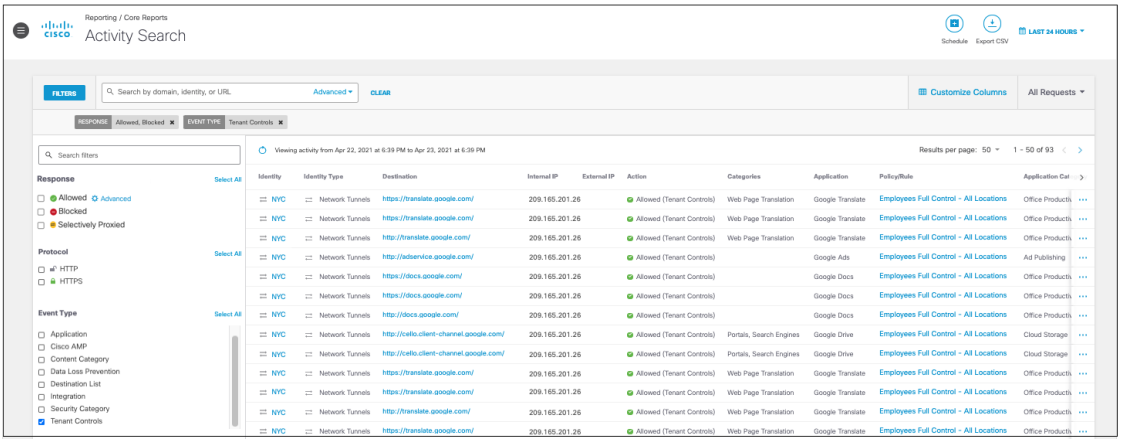
- A minimum role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. In the **Response** filter, select **Allowed** or **Blocked**.



3. Under **Event Type**, select **Tenant Controls**.



Note

Since the blocking of tenants occurs at the vendor level, Secure Access displays tenant controls as Allowed in Activity Search.

4. To access detailed information about a tenant-control event, from the **Action** menu, choose **View Further Details**.

29 Private Access Rules

Topics:

- Get Started With Private Access Rules
- Add a Private Access Rule
- Geolocation Sources and Private Access Rules
- Edit a Private Access Rule
- About ZTA Private Access Enforcement
- Allowing Traffic from Users and Devices on the Network
- Blocking Access to Private Destinations
- Troubleshoot Private Access Rules

Provides an overview of Private Access Rules in Cisco Secure Access, including Get Started With Private Access Rules, Add a Private Access Rule, and Geolocation Sources and Private Rules. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started With Private Access Rules

Describes Get Started With Private Access Rules in Cisco Secure Access. Private access rules control and secure access to internal resources and applications that are private and should not be accessed by the general public.

Private access rules control and secure access to internal resources and applications that are private and should not be accessed by the general public.

Traffic to private destinations is blocked by default. You must create rules to allow traffic to private destinations.

1. **Plan your private access rules**

   Plan your rules so that you get the results you expect. For example, factors such as rule order impact traffic handling.

2. **Create rule components.**

   Assemble rules largely from components, including but not limited to source, destination, endpoint posture, and security control components. See Components for Private Access Rules for more information.

3. **Specify rule defaults.**

   New rules will use the default security controls and other settings that you specify on the Rule Defaults page. See Default Settings for Private Access Rules for more information.

4. **Add private access rules**

   Generally, you will create rules to allow access to private resources. See Add a Private Access Rule for more information.

5. **Configure logging for the default private access rule**

   Traffic to private destinations that does not match any other private access rule in the policy will be handled by the default private access rule. Traffic that matches this rule is **blocked**. For more information, see View or Edit the Default Access Rules for more information.

6. **Edit the global settings**

   See Global Settings for Private Access Rules for more information.

7. **Review the rule order**

   Make sure the order of the rules on the Policy page will have the results you expect. See Edit the Order of the Rules on the Policy Page for more information.

8. **Distribute dummy access URLs to end users**

   For rules allowing access to private resources using browser-based connections, distribute the remotely accessible dummy URL to the users who will use it to connect to the resource. You configure a URL for each resource when configuring the resource. For more information, see Add a Private Resource for more information.

Externally Hosted Private Resources

To control access to specific SaaS internet destinations outside your network that are hosted by another company for exclusive use by your company, such as *YourCompany.OtherCompany.com*, use a private access rule to ensure specific egress IP addresses. For more information, see Zero Trust Access to Internet Destinations.

Default Settings for Private Access Rules

Describes Default Settings for Private Access Rules in Cisco Secure Access. You can choose default settings that will automatically populate newly created access rules by default.

You can choose default settings that will automatically populate newly created access rules by default.

Configure these settings on the Rule Defaults page: Navigate to **Secure > Access Policy**, click **Global Settings and Rule Defaults**, then click the **Rule Defaults** tab.

The following settings apply to private access rules:

- **Zero Trust Connection Endpoint Posture Profiles** - Posture profiles specify end-user device requirements when connecting to private resources using zero-trust access. Specify default requirements for connections from devices on which the Cisco Secure Client is installed and from devices on which the client is not installed.

  When choosing default posture profiles, keep in mind that if endpoints do not meet the requirements specified in the profile selected in a rule, the rule will not match the traffic. For more information about these posture profiles, see Manage Zero Trust Access Posture Profiles.

- **Zero Trust Access: User Authentication Interval** - Specify the frequency with which end user must sign in to the network, in order to connect to any private resource using client-based zero trust access. When disabled, users are not prompted to re-authenticate to the network. For details, see Network Authentication for Zero Trust Access.

- **Intrusion Prevention (IPS) Profile** - Specify the traffic-inspection behavior to use by default in new access rules.

  Important

  This setting applies to both private access rules and internet access rules. For more information about IPS Profiles, see Manage IPS Profiles.

- **Security Profile** - Specify default file inspection and file type blocking behavior for private traffic by choosing the default security profile for private access. You may need to create this profile before you can select it. For more information, see Security Profiles for Private Access.

The other settings on the Rule Defaults page apply only to internet access rules.

To edit default settings, see See Edit Rule Defaults and Global Settings.

Important

Choose rule defaults carefully; changing these settings later may impact existing rules. See Important Information About Changing Rule Defaults.

Global Settings for Private Access Rules

Describes Global Settings for Private Access Rules in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Global settings generally apply to all rules. However, some settings apply only to internet access rules, not to private access rules.

The following global settings apply to private access rules:

- **Decryption** - Intrusion prevention, file inspection, and file type blocking require decryption in order to be effective. For troubleshooting purposes, you can temporarily disable decryption for all access rules. This setting applies to both private access rules and internet access rules, but the functionality to which it applies is different in each case.

- **Decryption Logging** - Determine whether to enable or disable logging of decryption events for private access rules.

For more information about these settings, see Global Settings for Access Rules.

To change default rule settings, see Edit Rule Defaults and Global Settings.

Components for Private Access Rules

Describes Components for Private Access Rules in Cisco Secure Access. You can create access rules by adding rule components that you or others have configured to a rule.

You can create access rules by adding rule components that you or others have configured to a rule. Components described in this topic are reusable. You can use the same component (such as a source) in multiple rules, speeding and simplifying rule creation. For example, you can define a set of users as a source, then use the same source in an internet access rule and in a private access rule for the same set of users. Some components are profiles, or groups of settings bundled together that you choose as a unit when configuring a rule.

Sources

Describes Sources in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Sources on private access rules are either pre-configured or composite components. Pre-configured source components such as Registered Networks and Network Tunnel Groups acquire and manage the web traffic in your organization.

Composite sources may include IP addresses, CIDR blocks, and wildcard masks, and ports and port ranges.

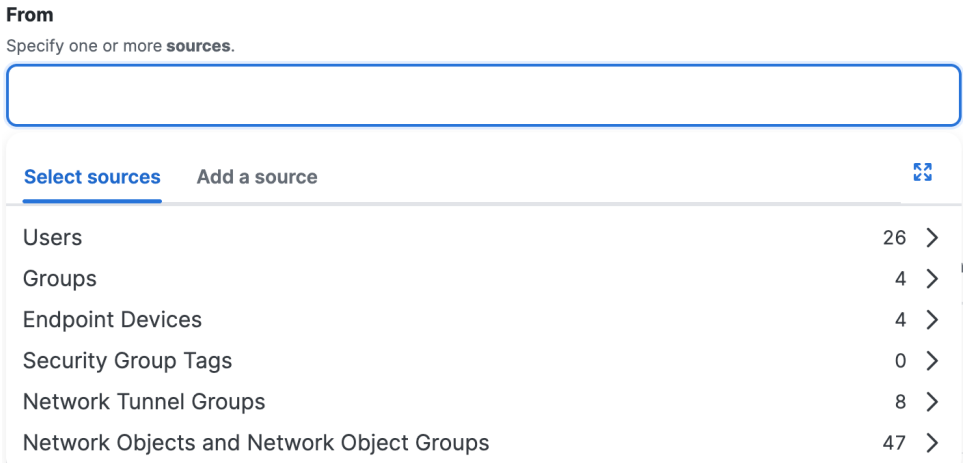
If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in the future.

Reusable Sources in Private Access Rules

Describes Reusable Sources in Private Access Rules in Cisco Secure Access. You can configure private access rules for specific source-destination pairs.

You can configure private access rules for specific source-destination pairs. Sources are the users, groups of users, and other entities that comprise the **From** end of traffic where Secure Access applies an access rule.

In a rule, you can also specify sources by typing in IP addresses and subnets, and ports and port ranges, but these network entities are not reusable source components. For more information, see Composite Sources for Private Access Rules on page 1003



You can use these reusable sources in your private access rules:

- Users

  You can apply rules to the traffic for the users in the organization.

- Groups

You can apply rules to the traffic for the groups of users in the organization.

- Endpoint Devices

  You can apply security controls on private access rules to any endpoint device in Secure Access. Endpoint devices in Secure Access include the following:

  - Any user device provisioned from an on-premise Active Directory (AD) domain controller (DC) integrated with Secure Access.
  - Any user device that has enrolled with Zero Trust Access on the Cisco Secure Client.
  - Be aware that rule-level security features (Intrusion Prevention (IPS) or Security Profile) are not compatible with access rules that have ZTA-enrolled devices as a source. We do not recommend configuring access rules with this combination.
  - Once enrolled or provisioned, user devices are available as sources in private access rules. You can select all endpoint devices in the organization, any AD device, any ZTA enrolled device, ZTA enrolled devices with specific host operating systems (macOS, Windows, iOS, or Android), or individual endpoint devices identified by device name.

  For information about the Cisco Secure Client and enrolling in Zero Trust Access, see Manage Zero Trust Access using Cisco Secure Client on Windows and macOS Devices.

  For information about AD device provisioning, see Manage Users, Groups, and Endpoints Devices.

- Security Group Tags

  You can apply rules to traffic originating from IP addresses in network segments that include Security Group Tags. Note that RA-VPNs do not receive SGT mappings directly through RADIUS.

  If you integrated Secure Access with ISE, you can use SGTs configured in the ISE application as a source in a access rule.

- Network Tunnel Groups

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Tunnel Groups.

  When you select Network Tunnel Groups, Secure Access secures and controls traffic from IPsec tunnels established by your supported network devices. If you need to know what tunnels are included in a group, navigate to **Connect > Network Connections > Network Tunnel Groups** and look at the group configuration.

- Network Objects

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Objects.

- Network Object Groups

  You can apply rules to the traffic originating from IP addresses in network segments defined by Network Objects in Network Object Groups.

Combining Multiple Sources in a Rule with Boolean Logic

Describes Combining Multiple Sources in a Rule with Boolean Logic in Cisco Secure Access. If a private access rule includes multiple sources, Secure Access combines all types of sources and all sources within a type using the boolean OR operator.

If a private access rule includes multiple sources, Secure Access combines all types of sources and all sources within a type using the boolean OR operator. Traffic to each source that you specify in a rule matches the rule. For example, if you specify a user group and a network tunnel group as sources, traffic from any member of either group matches the rule.

Supported Combinations of Reusable Sources with Composite Sources

You can select pre-configured sources and enter composite sources on the private access rules in your Access policy. Secure Access uses the logical OR operator to combine the pre-configured sources with the composite sources.

You can enter these composite sources on a private access rule:

- IP/CIDR Blocks/Wildcard Mask

For more information about composite sources, see Composite Sources in Private Access Rules.

Composite Sources for Private Access Rules

Describes Composite Sources for Private Access Rules in Cisco Secure Access. You can define a source using multiple network address components.

You can define a source using multiple network address components. A composite source accepts IP addresses, CIDR blocks, and wildcard masks directly in a private access rule.

> **Note**
>
> If you will allow access from a branch network, and you specify users or user groups, you must also configure SAML authentication for those users.

Limitations of Composite Sources

- Private Access rules with composite sources only support the **Allow** and **Block** actions.
- Composite sources do not include ports or protocols.

IP Addresses, CIDR Blocks, and Wildcard Masks

- Sources accept public IPv4 addresses and private non-routable IPs (RFC-1918 compliant). You may add public IPs for Registered Networks in Secure Access.
- Sources accept CIDR blocks.
- Sources do not require a deployed IPsec tunnel for the source IP addresses.
- Sources only accept valid IPv4 addresses.

For information about wildcard masks, see Using Wildcard Masks on Access Rules.

Adding Composite Sources

You can enter a single IPv4 address, CIDR block, or wildcard mask on a private access rule.

> **Note**
>
> Secure Access does not support a comma-separated list of wildcard masks.

For more information, see Add a Private Access Rule–Composite Sources.

Combining IPs, CIDRs, or Wildcard Masks on a Source

When you add various network address components for a source on a rule, Secure Access creates a single source entry. You can add multiple composite sources on a rule.

- The IPs, CIDR blocks, and wildcard masks that you add to the source are OR'ed together.

For example:

```
<IP address One> OR <CIDR block ONE> OR <IP address Three>
```

Destinations

Describes Destinations in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Destinations on private access rules are either pre-configured or composite components. For information about pre-configured destination components, see Reusable Destinations in Private Access Rules.

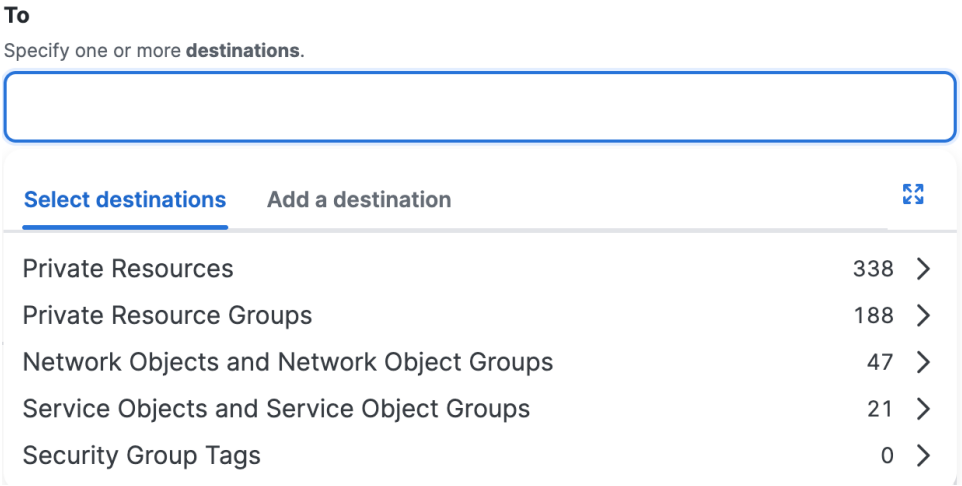
Composite destinations may include IP addresses, CIDR blocks, wildcard masks, fully-qualified domain names (FQDNs), ports and port ranges, and transport protocols. For information about composite destination components, see Composite Destinations in Private Access Rules.

Reusable Destinations in Private Access Rules

Describes Reusable Destinations in Private Access Rules in Cisco Secure Access. You can configure private access rules in the Access policy for specific source-destination pairs.

You can configure private access rules in the Access policy for specific source-destination pairs. Destinations are the private applications, application categories, or other private destinations that comprise the "To" end of traffic where Secure Access applies an access rule.

In an access rule, you can also enter destination IP addresses and subnets, and ports and protocols. For more information, see Composite Destinations in Private Access Rules



You can use these reusable destinations in your private access rules:

Private Resources

Secure Workload routes traffic securely to applications and other resources on your network, based on Private Resource configurations.

Define connection requirements for applications in your data center, including resources on private clouds. You will also specify the types of connections permitted for each resource, including Zero Trust Network Access with and without installed client, and VPN. For more information, see Manage Private Resources.

Private Resource Groups

After you add private resources, you can create groups of them for convenience and consistency, to easily apply an access rule to a collection of resources. For more information, see Add a Private Resource Group.

Network Objects

Network Objects represent IPv4 and IPv6 addresses, CIDR blocks, ranges of IPv4 addresses, or wildcard masks. Select the Network Objects on the access rules to apply security controls to the traffic on the networks. For more information, see Add a Network Object.

Network Object Groups

Select the Network Object Groups on the access rules to apply security controls to the traffic on the networks in groups. For more information, see Add a Network Object Group.

Service Objects

Service Objects represent a port, range of ports, protocol, or traffic on any protocols. Select the Service Objects on the access rules to apply security controls to the services. For more information, see Add a Service Object.

Service Object Groups

Select the Service Object Groups on the access rules to apply security controls to the traffic on the services in groups. For more information, see Add a Service Object Group.

Security Group Tags

A Securitygroup tag (SGT) is a label used to facilitate classification, propagation and enforcement by associating the SGT with an IP, VLAN, or port-profile as a source or destination.

For more information, see Security Group Tags.

Composite Destinations for Private Access Rules

Describes Composite Destinations for Private Access Rules in Cisco Secure Access. You can define a destination using multiple network address components.

You can define a destination using multiple network address components. All destinations allow connections from authenticated users on the network, including branch networks.

Composite destinations are useful if you need to quickly address a specific issue that arises, for example to immediately allow access to a destination that is being blocked by another rule, or to immediately block access to a problem destination.

Zero-trust connections are not available for destinations that are not configured as private resources.

Private access rules with composite destinations only support the **Allow** and **Block** actions.

These security controls do not apply to traffic for destinations added directly into a rule:

- Endpoint posture requirements
- Intrusion prevention (IPS)

If destinations include both configured private resources or groups and destinations typed directly into a rule, security controls are applied only to the configured private resources or groups.

IP Addresses, CIDR Blocks, and Wildcard Masks

- Destinations accept valid IPv4 addresses, CIDR blocks, and wildcard masks.

For information about wildcard masks, see Using Wildcard Masks on Access Rules.

Ports

- Destinations accept all ports or port ranges for traffic to private destinations.

Protocols

- Destinations accept the TCP, UDP or ICMP protocols.
- For the protocol on the destination, you can choose **ANY**. If you select **ANY**, the rule applies to traffic on the TCP, UDP, and ICMP protocols.

Adding Composite Destinations

You can enter a single IPv4 address, CIDR block, or wildcard mask on a private access rule.

Secure Access does not support a comma-separated list of wildcard masks.

Combining Destination Components as a Single Destination

When you add individual network address components on a destination, Secure Access combines the values to create a single destination entry. You can add multiple composite destinations on a rule.

- The ports added to the destination are OR'ed together.
- The protocols added to the destination are OR'ed together. The rule applies to traffic on the selected protocols.
- The individual network component field values that you enter for **Ports**, **Protocols**, and **IPs** or **CIDRs** are AND'ed together to create a single destination. The rule applies to the traffic on the composite destination.

You are not required to choose an IP, protocols, or ports to add a composite destination. Instead, you can choose the **ANY** protocol to define a destination that matches traffic on any IP or CIDR, with any port, on the available destination protocols.

Combining Multiple Destinations in a Rule with Boolean Logic

Describes Combining Multiple Destinations in a Rule with Boolean Logic in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

If a private access rule includes multiple destinations, the following boolean logic applies:

- Secure Access combines all types of destinations and all destinations within a type using the boolean OR operator. Traffic to each destination that you specify in a rule matches the rule. For example, if you specify a content category and an application list as destinations in a single rule, traffic to any destination that is a member of either group will match the rule.
- If you specify **ANY** for the protocol, then all traffic on the protocols (**TCP**, **UDP**, **ICMP**) supported by the private access rule matches the rule, regardless of any other destinations that you specify.

Endpoint Posture Profiles (for Endpoint Requirements)

Describes Endpoint Posture Profiles (for Endpoint Requirements) in Cisco Secure Access. You can require endpoints to meet requirements such as operating system version, firewall, and disk encryption before connecting to a network or resource.

You can require endpoints to meet requirements such as operating system version, firewall, and disk encryption before connecting to a network or resource. _These requirements are rule-matching criteria that determine whether a rule matches the traffic. _

Endpoint requirements are defined in posture profiles. There are several types of posture profile, depending on the type of connection and characteristics of the end-user device:

- **Client-based zero-trust posture profiles**: For end-user devices on which the Cisco Secure Client is installed
- **Browser-based zero-trust posture profiles**: For end-user devices on which the Cisco Secure Client is NOT installed
- **VPN posture profiles**: For end-user devices that are connected to the network using remote access VPN.

When you configure a private resource, you will specify which of the above types of connections are allowed for that resource.

When you create a private access rule, you will specify a posture profile with device requirements for each type of connection allowed by the private resources specified as destinations in the rule.

You can create different posture profiles, each with a different set of requirements, then choose appropriate profiles for each rule.

You can specify default posture profiles for zero-trust access connections (client-based and browser-based.) Create a profile with the desired default endpoint requirements for each connection type, then specify the default profiles on the Rule Defaults page. See Rule Defaults and Edit Rule Defaults and Global Settings.

Posture profile options apply only to User and User Group sources.

VPN posture is evaluated when the user connects to the network, which occurs before access rules evaluate the traffic.

Endpoint posture is not evaluated for branch connections.

See Manage Endpoint Security.

Security Controls

Describes Security Controls in Cisco Secure Access. Private access rules have (and need) less varied security controls than internet access rules.

Private access rules have (and need) less varied security controls than internet access rules.

Intrusion Prevention (IPS)

Describes Intrusion Prevention (IPS) in Cisco Secure Access. Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics.

Intrusion Prevention protects your network and assets by inspecting traffic for specified threat characteristics. Threat signatures are collected into collections called IPS Profiles.

When you configure an access rule, you can choose a predefined IPS profile such as Balanced Security and Connectivity or Maximum Security, or create a custom profile using Snort signatures that you choose. You can also choose whether to block or just monitor traffic that matches an IPS profile.

You can specify a default IPS profile on the Rule Defaults page that is automatically selected in each new rule. Default settings apply to both private access rules and internet access rules. See Rule Defaults and See Edit Rule Defaults and Global Settings.

See Manage IPS Profiles.

Security Profile, for File Inspection and File Type Controls

Describes Security Profile, for File Inspection and File Type Controls in Cisco Secure Access. Prevent upload and download of malicious files or file types such as executables in traffic to private resources by configuring at least one security profile for private access and selecting that profile in private access rules.

Prevent upload and download of malicious files or file types such as executables in traffic to private resources by configuring at least one security profile for private access and selecting that profile in private access rules.

See Security Profiles for Private Access.

About Endpoint Requirements in Access Rules

Describes About Endpoint Requirements in Access Rules in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Important

Important note about traffic handling

If endpoints do not meet the requirements specified in posture profiles, traffic is handled differently for zero trust connections and VPN connections:

- **For zero trust connections**, if endpoints do not meet the requirements in the posture profile specified in a private access rule, the rule will not match the traffic.

  If no other rule matches the traffic, Secure Access applies the default private access rule, which will block the traffic. The default private access rule appears at the bottom of the list of rules on the Access Policy listing page.

- **For VPN connections**, posture is evaluated at the time the device connects to the network. If endpoints do not meet the requirements specified in the VPN posture profile, the device cannot connect to the network.

For more information about posture profiles, see Manage Endpoint Security.

Add a Private Access Rule

Describes Add a Private Access Rule in Cisco Secure Access. Cisco Secure Access connects users, devices, both public and branch networks, and network tunnels to private resources in your enterprise.

Cisco Secure Access connects users, devices, both public and branch networks, and network tunnels to private resources in your enterprise. Private resources are applications and services that you deploy on your enterprise's infrastructure or private cloud. When you add a private resource to your organization, Secure Access enables Branch network connections to the resource.

Once you add your sources and private resources to Secure Access, you can create private access rules with these source and destination components. For more information, see Components for Private Access Rules.

In a private access rule, add the source or destination components that you configured for your organization. You can also enter sources and destinations directly into your rules. These single-use source and destination components are only available on an access rule, not shared by your policy.

The access rule defines the **Action**, **Source**, **Security Controls**, and **Destinations** for the rule. In your private access rule's **Security Controls**, Secure Access provides a default Intrusion Prevention System (IPS) profile. You can configure and apply other IPS profiles for your Branch networks to Private Resources rules. For more information, see Get Started With Private Access Rules.

Geolocation Sources and Private Access Rules

Describes Geolocation Sources and Private Access Rules in Cisco Secure Access. Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions.

Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions. The Geolocation source component is available on the internet and private access rules in the Access policy.

The Geolocation source component is a list of continents and the countries in these continents where Secure Access can manage the network traffic sent from these geographic locations.

You can select the Geolocation sources with the AD Users or AD Groups or only add the Geolocations on the access rules. Administrators of the organization are responsible for provisioning the AD Users and AD Groups. For more information, see Provision Users, Groups, and Endpoint Devices from Active Directory.

When you select the Geolocations on an access rule, Secure Access shows the AND option and the AD Users or AD Groups. When you select the AD Users and AD Groups for the source on an access rule, Secure Access shows the AND option and the list of continents and countries. Secure Access combines the selected AD Users or AD Groups and the geolocations with the boolean AND operator. You can only combine the Geolocation source component with the AD Users or AD Groups.

Monitoring Private Traffic from Geolocations

Set up the attributes and conditions on the access rules in the Access policy to monitor and protect the network traffic from the end users located in specific geographic regions. To enforce the security controls on a rule, the network traffic must match the selected sources.

For private access rules, choose to allow or block all traffic from the geolocations or all traffic from the selected AD Users or AD Groups located in the countries and continents.

- The Secure Web Gateway (SWG) detects and enforces the web traffic (TCP/80, TCP/443) sent from the end users located in the selected continents and countries.
- The Secure Access cloud-delivered firewall detects and enforces the network traffic on non-standard web ports sent from the end users located in the selected continents and countries.
- For Zero Trust Access (ZTA) connections, the Secure Access cloud-delivered firewall detects and enforces the network traffic and the SWG proxies the traffic to the private destinations.

You can view the events and logs recorded by Secure Access for the traffic sent from the end users in the organization in certain geolocations. Secure Access reports on the traffic on standard web ports and non-web ports. For more information, see:

- View the Events Report
- Activity Search Reports: Filter by Firewall Requests
- Activity Search Reports: Filter by Web Requests

About Geolocation Sources

Describes About Geolocation Sources in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Sources on private access rules are either pre-configured or composite components. Pre-configured source components such as Registered Networks and Network Tunnel Groups acquire and manage the web traffic in your organization. You can select Geolocations sources on the access rules combined with any AD Users or AD Groups.

> **Note**
>
> DNS resolution does not is not supported in source based geolocation policies. The geolocation source of a DNS lookup is not an indicator of where content is being delivered and as such source based geolocation checks and matches are enforced at other enforcement layers as part of unified policy based on your policy configuration.

Composite sources may include IP addresses, CIDR blocks, and wildcard masks, and ports and port ranges.

If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in the future.

Add Geolocation Sources on Private Access Rules

Provides instructions for completing the Add Geolocation Sources on Private Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select Geolocation sources only on access rules or combine the Geolocation sources with AD Users or AD Groups using the boolean AND operator.

- Add the Geolocation sources on the access rule, select the AND button, and then choose the AD Users and Groups.
- Add pre-configured AD Users and Groups on the access rule, select the AND button, and then choose the Geolocation sources.

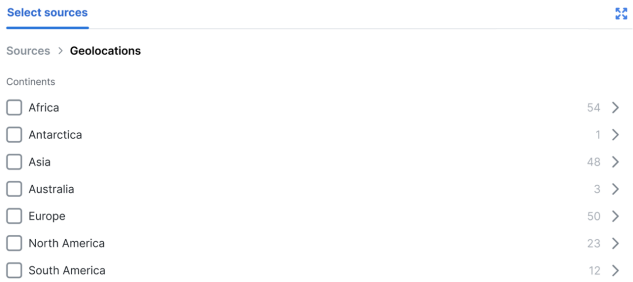
For information about Geolocation sources, see Geolocation Sources and Private Access Rules. For information about AD Users and AD Groups, see Manage Users, Groups, and Endpoint Devices on page 581.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Navigate to the rules table and choose an existing access rule to edit, or add a new access rule in the Access policy.
3. Navigate to **Specify Access** and then navigate to **From**.
4. Navigate to **Select sources** > **Geolocations**, choose a continent, which selects all countries in the continent, or choose the countries in each continent.



5. (Optional) Click **+ AND** and then add the AD Users or AD Groups.
   a) Navigate to **Select sources**, and then expand **Users** or **Groups**.
   b) Expand **Users**, and then select **AD Users** or select **Any AD Users**.



   c) Expand **Groups**, and then select **AD Groups** or select **Any AD Groups**.

View Events Report

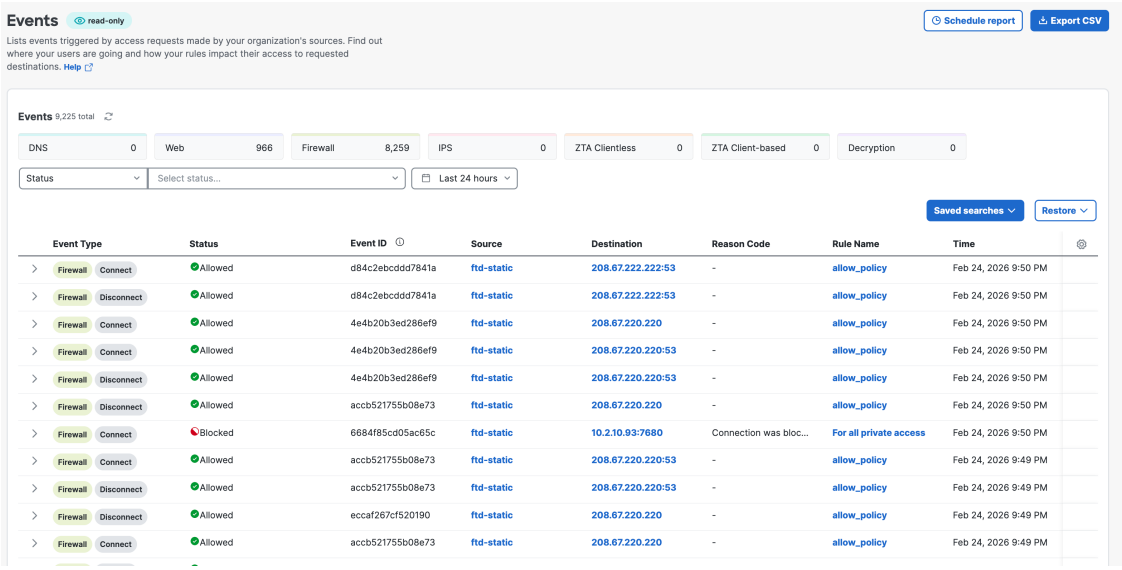
Provides instructions for completing the View Events Report workflow in Cisco Secure Access. Use the Events report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment.

Use the **Events** report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment. The Events report is a comprehensive record of event types, statuses, source and destination details, rule information, and reasons for actions. The Events reports helps you troubleshoot issues, verify policy enforcement, and adhere to compliance requirements.

Procedure

1. Navigate to **Monitor** > **Reports** > **Events**.
2. Choose a time frame.

   You can view events over the **Last 15 minutes**, **Last 30 minutes**, **Last 1 hour**, **Last 4 hours**, **Last 12 hours**, **Last 24 hours** (default), **Last 7 Days**, **Last 30 Days**, or a **Custom range**.



   For firewall events, the report displays both **Connect** and **Disconnect** actions. A **Connect** event indicates the start of a connection, recorded at the TCP handshake, where application details are typically not yet known by the Firewall. A **Disconnect** event signifies the close of the session, often containing more comprehensive, application-specific information.

   Specifically for Firewall Disconnect events, the Destination section of the Event Details Card includes the **Session Bytes Sent** and **Session Bytes Received** fields. These fields show the total amount of data sent and received during the firewall session, providing clear visibility into overall data transfer for each connection. This allows you to quickly assess the volume of data exchanged in a session and supports investigations into unusual or suspicious network activity.

   The Events Report table displays key information for each event. For a detailed understanding of each event type, including their unique characteristics, specific status values, and relevant behaviors, see Event Type Specific Details.

   - **Event Type**: Category of the event, for example, DNS, Web, Firewall.
   - **Status**: Action taken (Allowed, Blocked, or Isolated).
   - **Event ID**: A unique correlation ID generated for each request received by the policy broker, which is propagated downstream to maintain request tracking across network services.
   - The Event ID is linked to the 5-tuple (source IP address, source port, destination IP address, destination port, and protocol) of each flow. This ensures that all the packets in the same flow share the same Event ID. However,

if two different flows use the same 5-tuple within a short time, they too could get the same Event ID. This usually happens if a client quickly reuses the same source port for requests to the same destination.

- **Source**: Displays the originating identity for the event. This can be:
  - Source IP address (for network-based traffic).
  - User Identity (for authenticated users).
  - Device IP address (for client-based connections, typically representing the public IP address of the client device).
  - Public IP address of the client device (for ZTNA client-based connections). The ZTNA service also logs a specific ZTNA Device ID (a globally unique identifier) for the client, which is distinct from any IP address and helps identify the specific device regardless of its network location.
- **Destination**: The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and decryption requests.
- **Reason Code**: Cause of a particular event, for example, policy match, threat detected.
- **Rule Name**: The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
- Click a rule name to view the access policy in which the rule is configured. For more information, see Manage the Access Policy.
- **Time**: Date and time at which the event occurred.
- **Settings**: Gear icon to access table display settings, including options to adjust table density and to show or hide columns in the table.

  Column Behavior:

  - **Sorting**: Most columns can be sorted in ascending or descending order by clicking their header. Columns that are sortable will display an arrow icon (or similar visual indicator) in their header. Some columns, such as **Destination** and **Reason Code**, are currently not sortable to ensure optimal performance.
  - **Resizing**: Column widths can be adjusted by dragging the dividers between column headers.

> **Note**
>
> Note that the resize functionality is active across the entire column header area.

> **Note**
>
> If you have a block rule, for example, to block social media, and a user tries to access a blocked site such as facebook.com, the Events report will only display a Web block event. The Firewall does not log an event in this scenario because logging both a Firewall allow and a Web block could be confusing. This is intentional. When the Firewall allows the traffic, but the Secure Web Gateway (SWG) blocks it, only the Web block action is shown in the report.
>
> As a result, if you are looking to correlate events between the Firewall and Web layers for this type of traffic, you will not see a corresponding Firewall event. This is expected behavior and does not indicate a system issue.

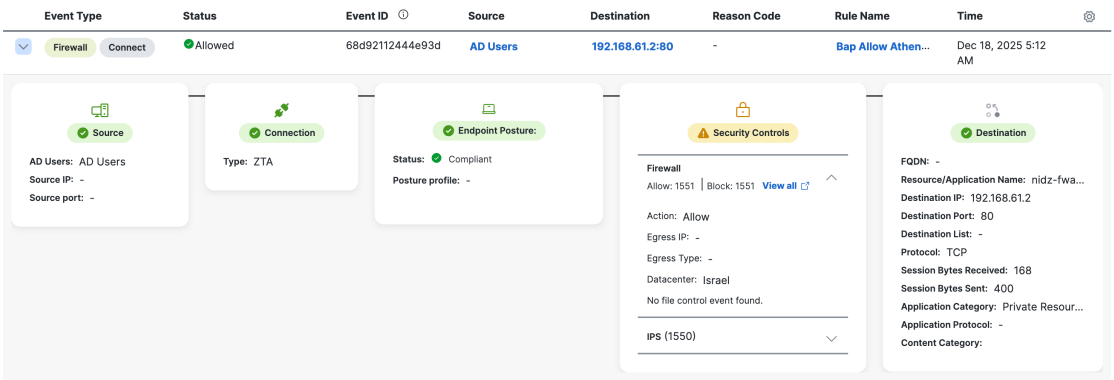
3. Select which security event types you want to view in the report. By default, all event types are selected to display activity for all event types.

   The Events report supports partial results if one or more event type queries (such as Proxy, Firewall, IP, Intrusion, or Decryption) fail due to an internal error. The report displays all available results from the successful queries, rather than showing an error for the entire request. Any unavailable event types will be clearly indicated in a message displayed on the screen.

   > **Note**
   >
   > This feature update ensures continued visibility into available security data, even when certain backend services encounter issues. All retrieved data remains accessible for review and export.

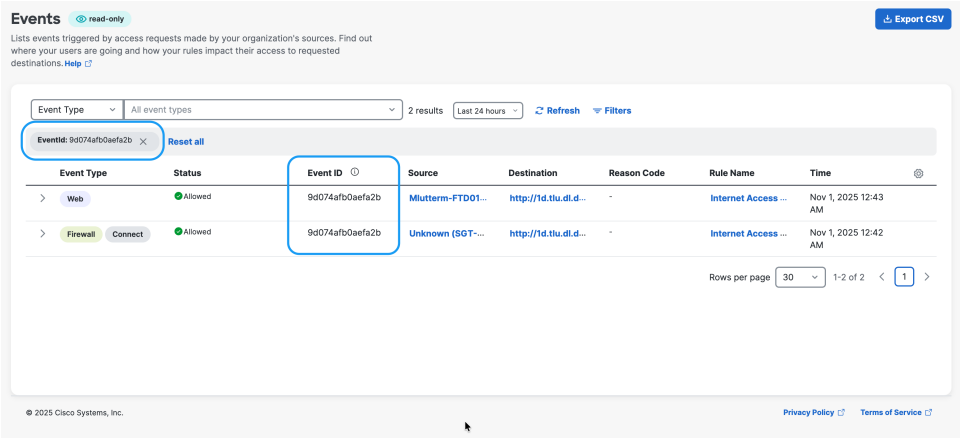
4. Click the **>** icon next to an event to view its Event Details Card.

   This card provides a comprehensive, correlated view of the event, grouped by Source, Connection, Security Controls, and Destination. The card also details applied security controls and the final rule action (e.g., blocked or allowed) for the specific event.



> **Note**
>
> Interactive elements within the Event Details Card may display additional information upon hover or click.

Click on an Event ID within the table to automatically filter the report and display all correlated events.



5. (Optional) Refine your search using advanced filters. For detailed information on all available filtering and search options, see Filtering and Search Options.
6. (Optional) To export the events report, click the **Export CSV** button at the top-right corner of the table. This downloads the current view of the report in CSV format for further analysis or record-keeping. For detailed instructions on exporting report data, see Export Report Data to CSV.

Filter the Report by Firewall Requests

Provides instructions for completing the Filter the Report by Firewall Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

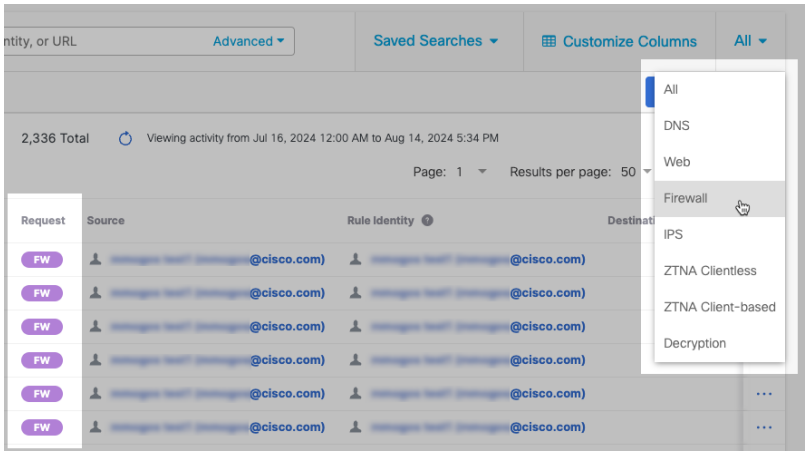
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view events from the **last 24 hours** (default), **Yesterday** , **Last 7 Days**, **Last 30 Days**, or a **Custom range**.

   The label **FW** in the **Request** column indicates a Firewall event.
3. Select the **Firewall** option from the dropdown menu at the top right to filter the report for Firewall events. Columns and Filter options update to those that are relevant to Firewall events.



4. Click the row to view Event Details.

   The Activity Search Report displays Event Details for each search result in a navigation drawer on the right. For more information, see View Activity Search Report Actions.

   Firewall event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see View and Customize the Activity Search Report.

   - **Action**
   - **Time**
   - **Rule Name**
   - **Source Geolocation**
   - **Source**
   - **Destination IP**
   - **Categories**
   - **File Name**
   - **Protocol**
   - **Application Protocol**

   Firewall event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Source IP	The source IPv4 or IPv6 address. Supports both compressed and long-form IPv6 address formats.
Source Port	The network port number on the source host from which the request originated.
Destination Port	The TCP or UDP port number on the destination host to which the request was sent. This field identifies the specific service or application targeted by the connection (for example, port 80 for HTTP or port 443 for HTTPS).
Resource/Application	The name of the resource or application.
Session Bytes Sent	The total number of bytes sent during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data sent from the source to the destination for the event session.

Field Name	Description
Session Bytes Received	The total number of bytes received during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data received from the destination by the source for the event session.
File Status (Disposition)	The file's Cisco AMP disposition: • **Clean**: Indicates that the AMP cloud categorized the file as clean. • **Malware**: Indicates that the AMP cloud categorized the file as malware, or local malware analysis identified malware. • **Unknown**: Indicates that the system queried the AMP cloud, but the AMP cloud has not assigned the file a disposition.
SHA256 Hash	The checksum of the file, if available and the event matched rules with File Type Control or File Inspection enabled.
File Transfer Direction	**DOWNLOAD**, **UPLOAD**, or **UNKNOWN**, if the event matched rules with File Type Control or File Inspection enabled.
Identified Threat	The name of the detected malware.
Malware Analysis Detected	If the event matched rules with File Inspection enabled, this field shows one of the following values as a result of file analysis by Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics. • **UNKNOWN** • **NOT ANALYZED** • **ANALYSIS COMPLETE NO VIRUS** • **ANALYSIS FAILED** • **ANALYSIS COMPLETE MALWARE DETECTED**
Threat Severity Score	The threat score most recently associated with this file. This is a value from 0 to 100.
File Type Identifiers	The type of file. For example, PDF or MSEXE.
File Size (bytes)	The size of the file in bytes, if the event matched rules with File Type Control or File Inspection enabled.
Archive File Name	The name of the archive file involved with the activity, if the event matched rules with File Type Control or File Inspection enabled.
Archive Extraction Depth	The level (if any) at which the file was nested in an archive file.

Field Name	Description
Archive SHA-256 Hash	The checksum of the archive file, if the event matched rules with File Type Control or File Inspection enabled.

Filter the Report by Web Requests

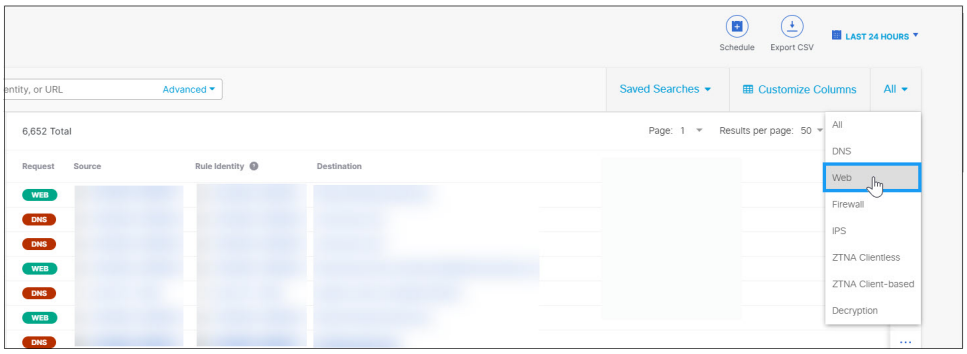
Provides instructions for completing the Filter the Report by Web Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

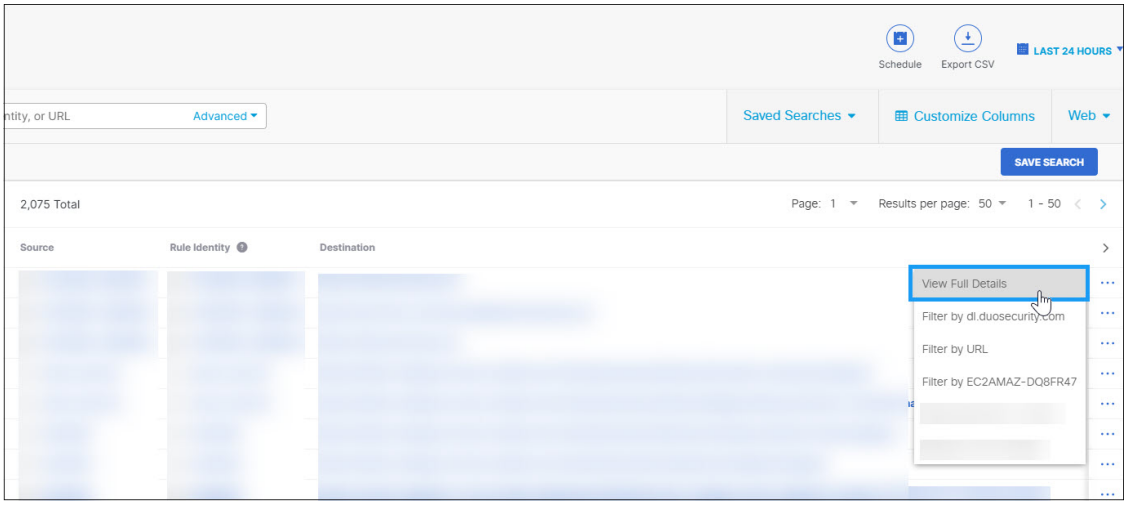
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **last 24 hours** (default), **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**.
3. From the drop-down menu at the top-right of the table, choose the **Web** option to filter the report for web events.



4. Click the ellipsis (**...**) and choose the **View Full Details** option to view web event details in the side panel.



5. The event details are displayed in the side panel. For more information, see View Activity Search Report Actions.

Web event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see Customize the Activity Search Report.

- **Action**
- **Time**
- **Rule Name**
- **Source Geolocation**
- **Source**
- **Rule Identity**
- **Internal IP Address**
- **External IP Address**
- **Destination**
- **Categories**
- **Resource/Application**
- **Application Category**
- **Content Type**
- **Request Method**
- **Referrer**
- **Status Code**

Web event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Hostname	Fully Qualified Domain Name (FQDN) of the machine or container from which the event originated.
File Action (Remote Browser Isolation)	Action taken on a file, such as Viewed, Original File Downloaded, Sanitized PDF File Downloaded.
Total Size, in Bytes	The number of bytes sent from the client for all the requests, including HTTP headers, for example, 234.
User Agent	The user agent string as captured by the proxy, for example, Mozilla 5.0 (X11; Linux x86_64; rv:12.0) Gecko 20100101 Firefox 21.0.
SHA256 Hash	This represents the SHA-256 hash of the response body.
Egress IP Address	The IP address is used by the proxy to communicate with the origin server. Dot notation is used for IPv4 and RFC 5952 is used for IPv6 , for example, 1.2.3.4, 2001:db8::1.
Egress Data Center	The data center that processed the request.
YouTube Channels	The YouTube channel name, such as @Cisco in the Cisco YouTube channel (https://www.youtube.com/@Cisco).

Field Name	Description
YouTube Categories	The set of YouTube categories, such as Education, Entertainment, Animation.

Set Up the Private Access Rule

Provides instructions for completing the Set Up the Private Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

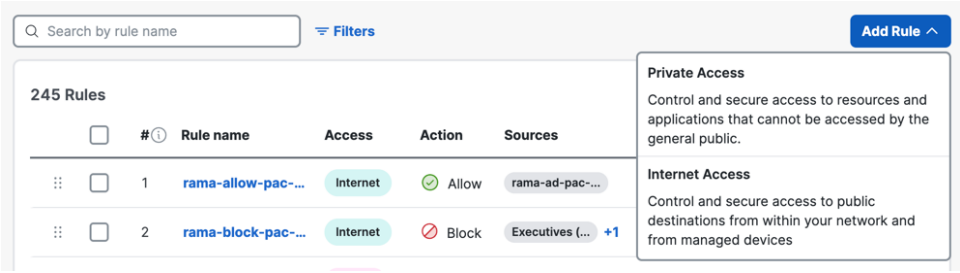
Add a private access rule in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Add sources to your organization. For more information, see Components for Private Access Rules.
- Add Private Resources to your organization. For more information, see Add a Private Resource.
- Edit Default Settings for Private Access Rules.

Procedure

1. Navigate to **Secure** > **Access Policy**.



2. Click **Add Rule**, and then choose **Private Access**.

Enable the Rule and Edit Your Logging Settings

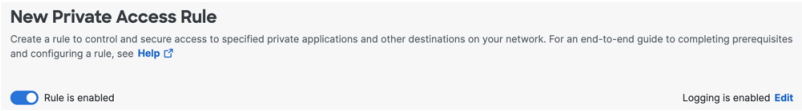
Provides instructions for completing the Enable the Rule and Edit Your Logging Settings workflow in Cisco Secure Access. Enable your private access rule and edit the logging settings for the rule.

Enable your private access rule and edit the logging settings for the rule.

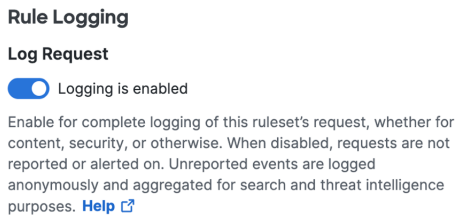
Procedure

1. Toggle on **Rule is enabled** to enable the access rule.

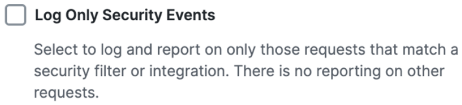
   After you configure and save the rule to your policy, the rule is enabled. You can toggle off the rule at any time to disable it.



2. Click **Edit** to manage your logging settings on the access rule.
   a) For **Log Request**, toggle **Logging is enabled** off or on to choose whether Secure Access logs the events for the traffic managed by the access rule.



   b) For **Log Only Security Events**, select whether Secure Access logs the events that match the security filters. For more information, see Manage Logging.



Add a Rule Name

Describes Add a Rule Name in Cisco Secure Access. For Rule name, add a meaningful name for your access rule.

For **Rule name**, add a meaningful name for your access rule. The **Rule name** is required. You must give your rule a name before you can continue to configure the **Security Controls** on the access rule.

> **Note**
>
> The **Next** button on the access rule is not available until you enter a name for the rule.



Guidelines for Creating a Rule Name

Secure Access enforces the number and type of characters supported in a rule name. You can add a rule name with these constraints:

- A rule name is a sequence of 2–50 alphanumeric, hyphen, underscore, and space characters.
- A rule name must be unique across all access rules in the organization's Access policy.

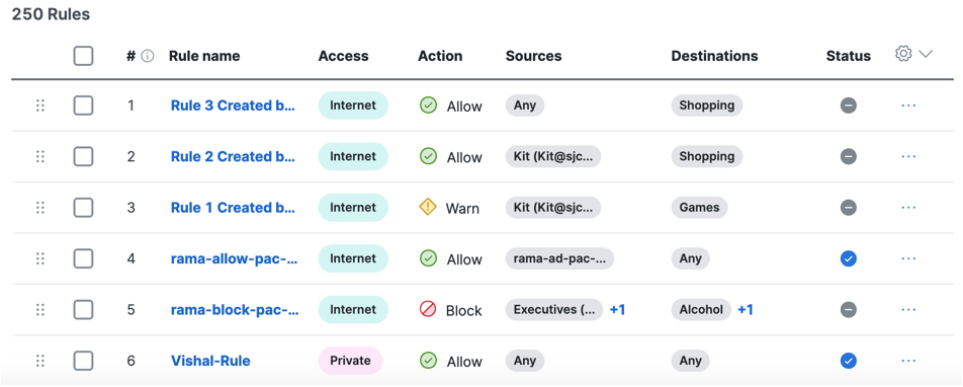
Summary

Describes Summary in Cisco Secure Access. After you add a rule to your policy, you can edit the rule and then view the rule summary.

After you add a rule to your policy, you can edit the rule and then view the rule summary.

1. Navigate to **Secure > Access Policy**.

2. Navigate to a rule, and then click on the horizontal ellipsis (**...**) to expand the rule menu.



3. Click **Edit** to open the rule and view the rule summary.



The summary contains the components that you configured on the access rule:

- **Sources**
- **Action**
- **Security Controls**
- **Destinations**

If you see an **Upgrade** button, this means that your organization has an opportunity to upgrade to a subscription that offers additional functionality. For more information, see Welcome to Cisco Secure Access.

Choose a Rule Order

Describes Choose a Rule Order in Cisco Secure Access. For Rule order, choose a new priority for the rule, or keep the rule order assigned to the rule by Secure Access.

1. For **Rule order**, choose a new priority for the rule, or keep the rule order assigned to the rule by Secure Access.

   When you add a new rule, Secure Access assigns the next lowest priority to the rule. Secure Access applies the first rule in the list on the Access Policy page that matches the traffic. Order your rules so that more specific rules that might apply to the traffic are above more general rules. For more information, see Edit the Order of Rules on the Access Policy Page.



Rule Action

Describes Rule Action in Cisco Secure Access. Choose Allow or Block to assign how Secure Access applies the configured components in the access rule.

1. Choose **Allow** or **Block** to assign how Secure Access applies the configured components in the access rule.

> **Note**
>
> Secure Access blocks the traffic in your organization to private destinations unless an access rule allows the connections.

> **Note**
>
> When the action is **Allow** and the traffic does not pass the security controls defined in the rule, Secure Access blocks the traffic.

If you assign **Block** to a rule that is destine for a private application and there is an HTTPS “Get” request for a downloadable file, the rule blocks matching traffic and actions appropriately but the event appears in Activity Search twice: one entry as the action is “blocked” and one entry as the action is “allow”. Activity Search does not currently condense events that generate multiple entries and thusly increases the hit counter as “2”.

Enable a Schedule on a Private Access Rule

Provides instructions for completing the Enable a Schedule on a Private Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

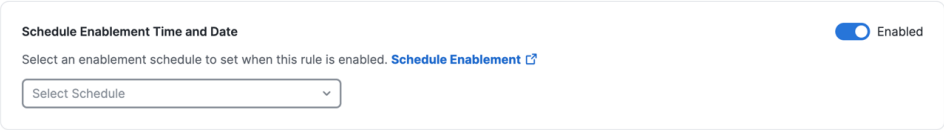
Configure the **Schedule Enablement Time and Date** setting and add a Schedule for the private access rule. For information about configuring Schedules in Secure Access, see Manage Schedules.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. On a private access rule in the Access policy, navigate to **Specify Access**, and then navigate to **Schedule Enablement Time and Date**.



2. Click **Enabled** to activate a Schedule on the private access rule.
   a) (Optional) To disable a Schedule on the private access rule, toggle off the **Schedule Enablement Time and Date** setting.
3. Click the **Select Schedule** drop-down menu and then choose a schedule to enable on the private access rule.
4. Click **Save**.

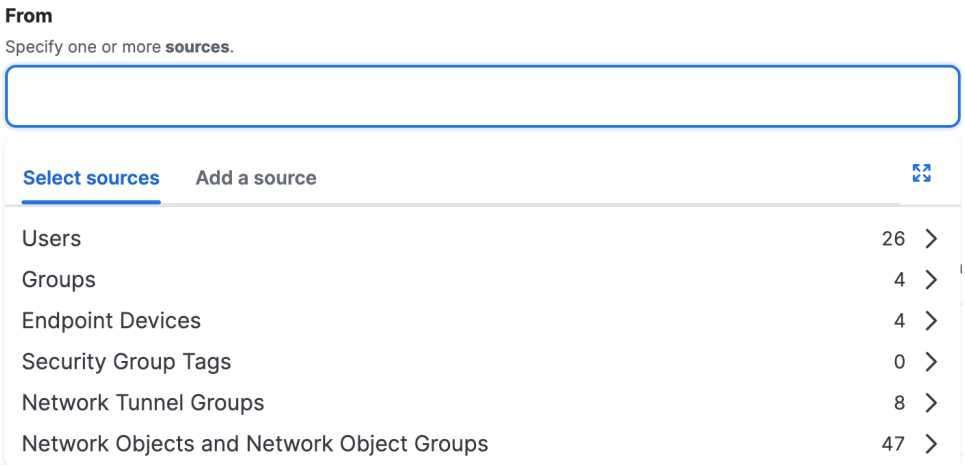
Pre-Configured Sources

Describes Pre-Configured Sources in Cisco Secure Access. We recommend that you use your organization's reusable source components in your access rules.

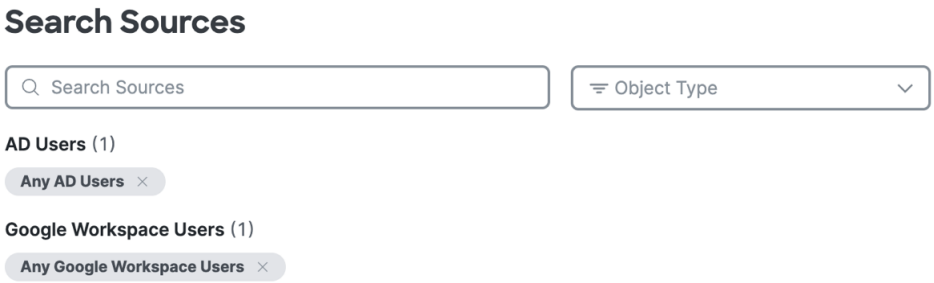
We recommend that you use your organization's reusable source components in your access rules. If you select Users or User Groups, you can choose destinations enabled for virtual private networks (VPNs) and Zero Trust Access connections, not Branch connections.

> **Note**
>
> The connection methods for a destination depend on the type of sources that you choose.

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Private Access**.
2. Navigate to **Specify Access** and then click on the search bar under **From**.
3. For **Select sources**, click in the white space beside the default value ("Any") and choose the configured source components in your organization. When you finish choosing your sources, click **Done**. For descriptions of the different types of sources, see Components for Private Access Rules: Sources.



4. After you add a source component, click **+More** to view the list of sources that you added to the rule.



Add Composite Sources

Provides instructions for completing the Add Composite Sources workflow in Cisco Secure Access. Add a network address as a source on a private access rule.

Add a network address as a source on a private access rule.

The connection methods for a destination depend on the type of sources that you choose.

Procedure

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Private Access**.

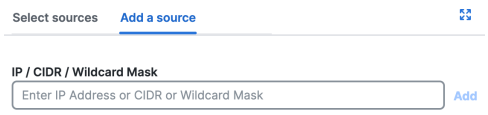
2. Navigate to **Specify Access** and then click on the search bar under **From**.
3. For **Add a source**, enter an IPv4 address, CIDR block, or IPv4 address with a wildcard mask

   This option is useful if you need to quickly address a specific issue that arises, for example to immediately block a particular user's access to an internet destination. For more information, see About Configuring Sources in Private Access Rules.

   For Example:

   - IPv4 address–**1.2.3.4**
   - CIDR block–**1.2.3.4/24**
   - Wildcard mask–**1.2.3.4/255.255.255.255**

     For **Wildcard Mask**, use the format: `<IP address>/<Wildcard Mask>`.



4. Click **Add**.
5. After you add a composite source, click **+More** to view the list of sources that you added to the rule.



Pre-Configured Destinations

Describes Pre-Configured Destinations in Cisco Secure Access. We recommend that you use your organization's configured destination components in your private access rules.

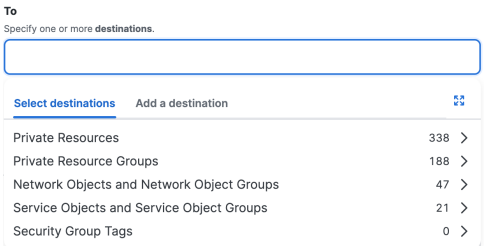
We recommend that you use your organization's configured destination components in your private access rules. For more information, see Reusable Destinations in Private Access Rules.

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Private Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. For **Select destinations**, click in the white space beside the default value ("Any") and choose the configured **Private Resource Groups** and **Private Resources** in your organization. When you finish choosing your private resources, click **Done**.

   > **Note**
   >
   > The arrows out icon opens a window to configure the destinations in your rule.

   a. For each **Private Resource**, hover over the network connections icons.

      Secure Access describes the type of network connections supported by the private destination.



4. After you add a destination component, click **+More** to view the list of destinations that you added to the rule.
   a. Click on the **X** to remove a previously added destination, then click **Done**.



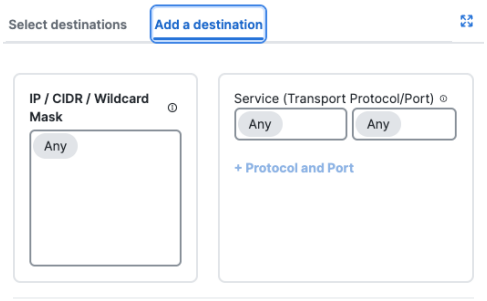
For more information, see About Configuring Destinations in Private Access Rules.

Add Composite Destinations

Describes Add Composite Destinations in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

You can add destinations directly on a private access rule. For more information, see About Configuring Destinations in Private Access Rules.

1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Private Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.
3. For **Add a destination**, enter or select the network components, then click **Add**.



   a. For **IP, CIDR, or Wildcard Mask**, enter an IPv4 or IPv6 address, CIDR block, or IPv4 address with a wildcard mask.

      For example:

      - IPv4 address–**1.2.3.4**
      - IPv6 address–**2001:DB8::/32**
      - CIDR block–**1.2.3.4/24**
      - Wildcard mask–**1.2.3.4/255.255.255.255**

      For **Wildcard Mask**, use the format: `<IP address>/<Wildcard Mask>`.

   b. For **Protocol**, choose from one of the supported protocols: **ANY**, **TCP**, **UDP**, or **ICMP**.

   c. For **Port/Port Range**, enter a port or range of ports.

4. After you add a composite destination, click **+More** to view the list of destinations that you added to the rule.
   a. Click on the **X** to remove a previously added destination, then click **Done**.



To allow VPN access to a private resource, specify its IP, CIDR, or Wildcard mask, port, or protocol with the **Add a destination** option.

> **Note**
>
> You might use this option to allow users from one branch to access private applications in another branch. Destinations that you enter manually are not reusable in another access rule.

For more information, see About Configuring Destinations in Private Access Rules.

Select Network and Service Objects on Private Access Rules

Provides instructions for completing the Select Network and Service Objects on Private Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select pre-configured Network Objects and Groups and Service Objects and Groups as destinations on private access rules. When you choose the objects and groups, you have the option to combine the objects and groups with the logical AND operator. For more information, see Combine Destinations with Boolean Logic.

> **Note**
>
> If you do not add the logical AND operator with the selected destinations, Secure Access combines the destinations with the logical OR operator. For more information, see Combining Multiple Destinations in a Rule (Boolean Logic).

Before you begin

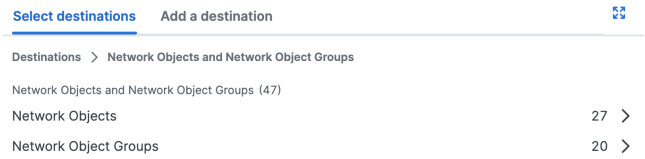
- Full Admin user role. For more information, see Manage Accounts.

Procedure

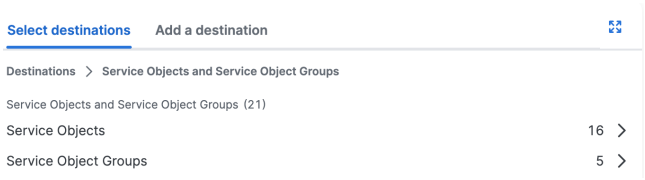
1. Navigate to **Secure** > **Access Policy** > **Add Rule** > **Private Access**.
2. Navigate to **Specify Access** and then click on the search bar under **To**.



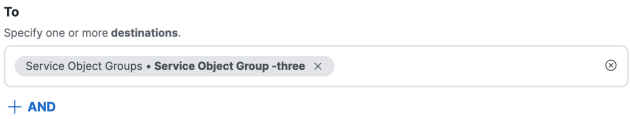
3. Select the Network Objects and Groups or Service Objects and Groups.
   a) Click **Select destinations**, and then choose the Network Objects and Groups to add to the internet rule.



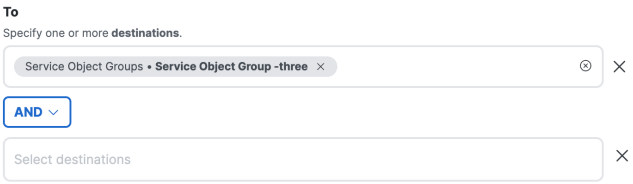
b) Click **Select destinations**, and then choose the Service Objects and Groups to add to the internet rule.



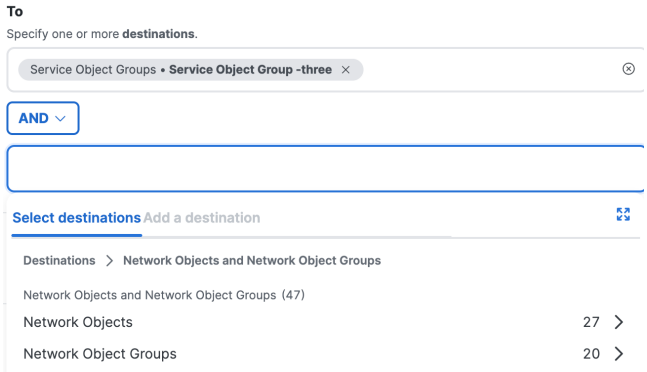
4. (Optional) Click **+AND**.



a) Click on the **Select destinations** text area.

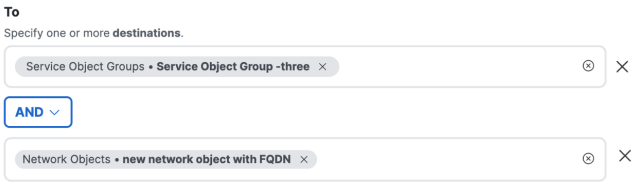


b) Choose a destination to combine with the other selected destinations using the logical AND operator. For more information, see Combine Destinations With Boolean Logic.



After you select the objects and groups to use with the AND operator, you can remove the destinations and then add new destinations.

> **Note**
>
> You have to select all destinations at the same time for each side of the **AND** option. Once selected, you can not go back and add more destinations.



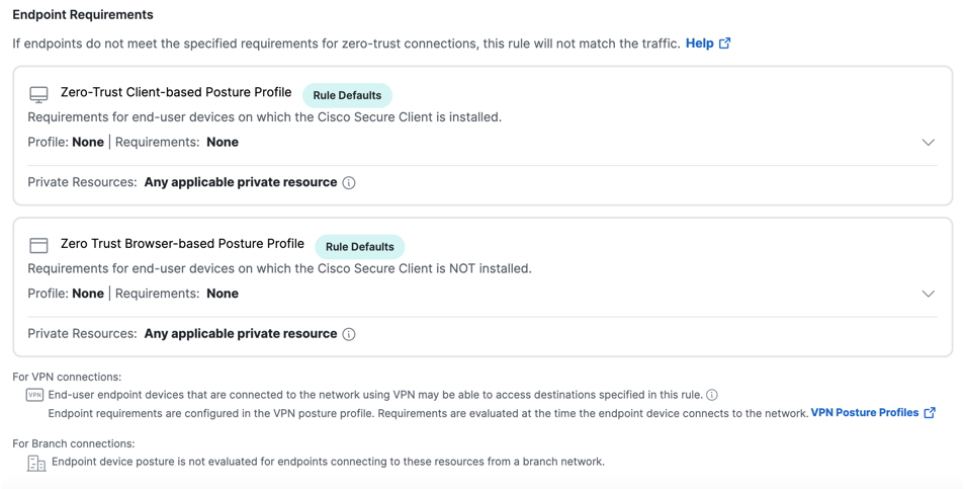
5. Click **Next**.

Endpoint Requirements

Describes Endpoint Requirements in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Branch connections to private destinations do not require additional configuration. For important information about endpoint requirements and traffic handling, see About Endpoint Requirements in Access Rules.

For general information about posture profiles, see Manage Endpoint Security.



User Authentication Requirements

Describes User Authentication Requirements in Cisco Secure Access. For Zero Trust Access: User Authentication Interval, toggle on or off whether Secure Access prompts users to authenticate before connecting to private destinations.

For **Zero Trust Access: User Authentication Interval**, toggle on or off whether Secure Access prompts users to authenticate before connecting to private destinations. When **Zero Trust Access: User Authentication Interval** is enabled, you can set the interval when Secure Access requests that you authenticate.

This setting determines how often users must sign in to the network in order to make a Zero Trust connection to a private resource specified as a destination in this rule. Users are prompted to sign in only once per interval if they try to connect to a resource during that time, regardless of the private resources they access.

This option appears only if destinations include at least one private resource.

In access rules that apply to iOS devices, User Authentication Interval must be disabled or iOS device users will be unable to access resources that are enabled for zero trust access.

You can use the default interval as configured on the Rule Defaults page or specify a different interval.

For more information, see Network Authentication for Zero Trust Access.

Configure Security Control Options

Describes Configure Security Control Options in Cisco Secure Access and outlines Intrusion Prevention (IPS) and Security Profile. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Security control options for traffic to private destinations include the following:

Intrusion Prevention (IPS)

1. Use the default IPS profile as specified on the Rule Defaults page, or choose a different IPS profile that includes the threat detection settings that you want applied to traffic that matches this rule.
2. Click **Save**.

We recommend that you do not disable your IPS Profiles. For more information, see Manage IPS Profiles.

Security Profile

The security profile for private access specifies file inspection and file type controls for uploaded and downloaded files in private traffic.

Use the default security profile for private access as specified on the Rule Defaults page, or choose a different security profile to apply to traffic that matches this rule.

For details, see Security Profiles for Private Access.

Geolocation Sources and Private Access Rules

Describes Geolocation Sources and Private Access Rules in Cisco Secure Access. Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions.

Geolocation sources enable organizations to monitor and control the traffic from end users in specific geographic regions. The Geolocation source component is available on the internet and private access rules in the Access policy.

The Geolocation source component is a list of continents and the countries in these continents where Secure Access can manage the network traffic sent from these geographic locations.

You can select the Geolocation sources with the AD Users or AD Groups or only add the Geolocations on the access rules. Administrators of the organization are responsible for provisioning the AD Users and AD Groups. For more information, see Provision Users, Groups, and Endpoint Devices from Active Directory.

When you select the Geolocations on an access rule, Secure Access shows the AND option and the AD Users or AD Groups. When you select the AD Users and AD Groups for the source on an access rule, Secure Access shows the AND option and the list of continents and countries. Secure Access combines the selected AD Users or AD Groups and the geolocations with the boolean AND operator. You can only combine the Geolocation source component with the AD Users or AD Groups.

Monitoring Private Traffic from Geolocations

Set up the attributes and conditions on the access rules in the Access policy to monitor and protect the network traffic from the end users located in specific geographic regions. To enforce the security controls on a rule, the network traffic must match the selected sources.

For private access rules, choose to allow or block all traffic from the geolocations or all traffic from the selected AD Users or AD Groups located in the countries and continents.

- The Secure Web Gateway (SWG) detects and enforces the web traffic (TCP/80, TCP/443) sent from the end users located in the selected continents and countries.
- The Secure Access cloud-delivered firewall detects and enforces the network traffic on non-standard web ports sent from the end users located in the selected continents and countries.
- For Zero Trust Access (ZTA) connections, the Secure Access cloud-delivered firewall detects and enforces the network traffic and the SWG proxies the traffic to the private destinations.

You can view the events and logs recorded by Secure Access for the traffic sent from the end users in the organization in certain geolocations. Secure Access reports on the traffic on standard web ports and non-web ports. For more information, see:

- View the Events Report
- Activity Search Reports: Filter by Firewall Requests
- Activity Search Reports: Filter by Web Requests

About Geolocation Sources

Describes About Geolocation Sources in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Sources on private access rules are either pre-configured or composite components. Pre-configured source components such as Registered Networks and Network Tunnel Groups acquire and manage the web traffic in your organization. You can select Geolocations sources on the access rules combined with any AD Users or AD Groups.

> **Note**
>
> DNS resolution does not is not supported in source based geolocation policies. The geolocation source of a DNS lookup is not an indicator of where content is being delivered and as such source based geolocation checks and matches are enforced at other enforcement layers as part of unified policy based on your policy configuration.

Composite sources may include IP addresses, CIDR blocks, and wildcard masks, and ports and port ranges.

If you see an option to **Select All**, this selects all existing items in the group at the time you select it, but the rule will not include items added to the group in the future.

Add Geolocation Sources on Private Access Rules

Provides instructions for completing the Add Geolocation Sources on Private Access Rules workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can select Geolocation sources only on access rules or combine the Geolocation sources with AD Users or AD Groups using the boolean AND operator.

- Add the Geolocation sources on the access rule, select the AND button, and then choose the AD Users and Groups.
- Add pre-configured AD Users and Groups on the access rule, select the AND button, and then choose the Geolocation sources.

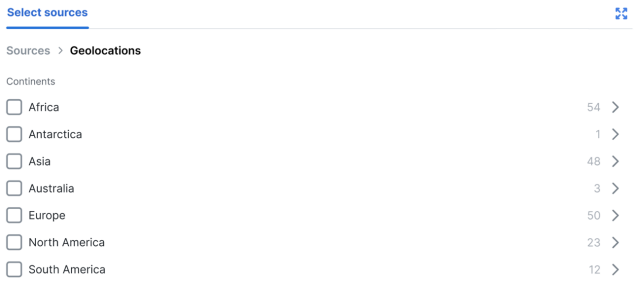
For information about Geolocation sources, see Geolocation Sources and Private Access Rules. For information about AD Users and AD Groups, see Manage Users, Groups, and Endpoint Devices on page 581.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Navigate to the rules table and choose an existing access rule to edit, or add a new access rule in the Access policy.
3. Navigate to **Specify Access** and then navigate to **From**.
4. Navigate to **Select sources** > **Geolocations**, choose a continent, which selects all countries in the continent, or choose the countries in each continent.



5. (Optional) Click **+ AND** and then add the AD Users or AD Groups.
   a) Navigate to **Select sources**, and then expand **Users** or **Groups**.
   b) Expand **Users**, and then select **AD Users** or select **Any AD Users**.



   c) Expand **Groups**, and then select **AD Groups** or select **Any AD Groups**.

View Events Report

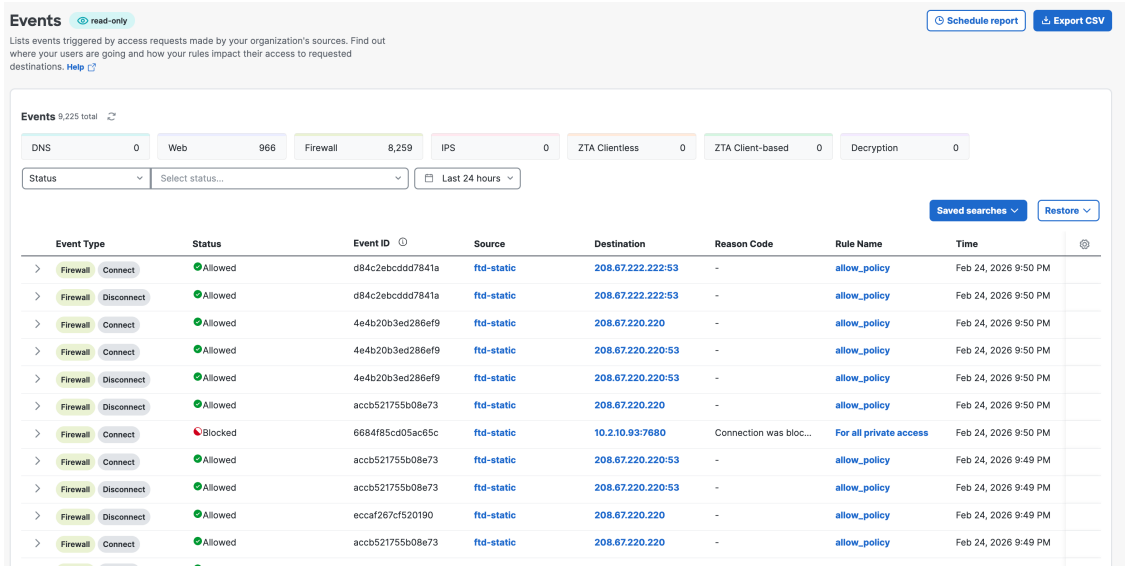
Provides instructions for completing the View Events Report workflow in Cisco Secure Access. Use the Events report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment.

Use the **Events** report to view, filter, and analyze the security and network activities across your Cisco Secure Access deployment. The Events report is a comprehensive record of event types, statuses, source and destination details, rule information, and reasons for actions. The Events reports helps you troubleshoot issues, verify policy enforcement, and adhere to compliance requirements.

Procedure

1. Navigate to **Monitor** > **Reports** > **Events**.
2. Choose a time frame.

   You can view events over the **Last 15 minutes**, **Last 30 minutes**, **Last 1 hour**, **Last 4 hours**, **Last 12 hours**, **Last 24 hours** (default), **Last 7 Days**, **Last 30 Days**, or a **Custom range**.



For firewall events, the report displays both **Connect** and **Disconnect** actions. A **Connect** event indicates the start of a connection, recorded at the TCP handshake, where application details are typically not yet known by the Firewall. A **Disconnect** event signifies the close of the session, often containing more comprehensive, application-specific information.

Specifically for Firewall Disconnect events, the Destination section of the Event Details Card includes the **Session Bytes Sent** and **Session Bytes Received** fields. These fields show the total amount of data sent and received during the firewall session, providing clear visibility into overall data transfer for each connection. This allows you to quickly assess the volume of data exchanged in a session and supports investigations into unusual or suspicious network activity.

The Events Report table displays key information for each event. For a detailed understanding of each event type, including their unique characteristics, specific status values, and relevant behaviors, see Event Type Specific Details.

- **Event Type**: Category of the event, for example, DNS, Web, Firewall.
- **Status**: Action taken (Allowed, Blocked, or Isolated).
- **Event ID**: A unique correlation ID generated for each request received by the policy broker, which is propagated downstream to maintain request tracking across network services.
- The Event ID is linked to the 5-tuple (source IP address, source port, destination IP address, destination port, and protocol) of each flow. This ensures that all the packets in the same flow share the same Event ID. However, if two different flows use the same 5-tuple within a short time, they too could get the same Event ID. This usually happens if a client quickly reuses the same source port for requests to the same destination.
- **Source**: Displays the originating identity for the event. This can be:
  - Source IP address (for network-based traffic).
  - User Identity (for authenticated users).
  - Device IP address (for client-based connections, typically representing the public IP address of the client device).
  - Public IP address of the client device (for ZTNA client-based connections). The ZTNA service also logs a specific ZTNA Device ID (a globally unique identifier) for the client, which is distinct from any IP address and helps identify the specific device regardless of its network location.
- **Destination**: The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and decryption requests.
- **Reason Code**: Cause of a particular event, for example, policy match, threat detected.

- **Rule Name**: The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
- Click a rule name to view the access policy in which the rule is configured. For more information, see Manage the Access Policy.
- **Time**: Date and time at which the event occurred.
- **Settings**: Gear icon to access table display settings, including options to adjust table density and to show or hide columns in the table.

  Column Behavior:

  - **Sorting**: Most columns can be sorted in ascending or descending order by clicking their header. Columns that are sortable will display an arrow icon (or similar visual indicator) in their header. Some columns, such as **Destination** and **Reason Code**, are currently not sortable to ensure optimal performance.
  - **Resizing**: Column widths can be adjusted by dragging the dividers between column headers.

> **Note**
>
> Note that the resize functionality is active across the entire column header area.

> **Note**
>
> If you have a block rule, for example, to block social media, and a user tries to access a blocked site such as facebook.com, the Events report will only display a Web block event. The Firewall does not log an event in this scenario because logging both a Firewall allow and a Web block could be confusing. This is intentional. When the Firewall allows the traffic, but the Secure Web Gateway (SWG) blocks it, only the Web block action is shown in the report.
>
> As a result, if you are looking to correlate events between the Firewall and Web layers for this type of traffic, you will not see a corresponding Firewall event. This is expected behavior and does not indicate a system issue.

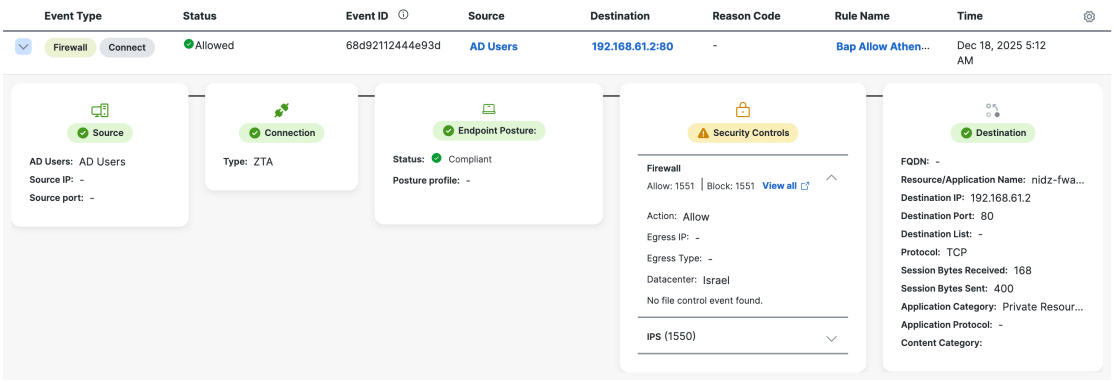
3. Select which security event types you want to view in the report. By default, all event types are selected to display activity for all event types.

   The Events report supports partial results if one or more event type queries (such as Proxy, Firewall, IP, Intrusion, or Decryption) fail due to an internal error. The report displays all available results from the successful queries, rather than showing an error for the entire request. Any unavailable event types will be clearly indicated in a message displayed on the screen.

   > **Note**
   >
   > This feature update ensures continued visibility into available security data, even when certain backend services encounter issues. All retrieved data remains accessible for review and export.

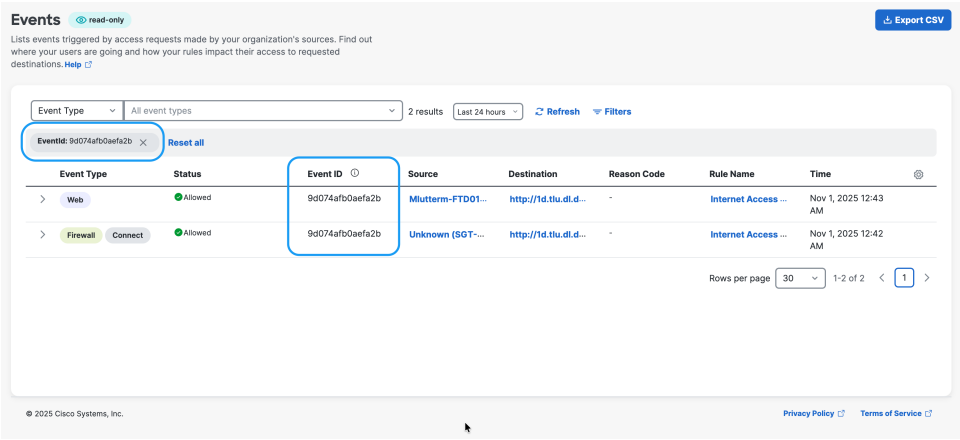
4. Click the **>** icon next to an event to view its Event Details Card.

This card provides a comprehensive, correlated view of the event, grouped by Source, Connection, Security Controls, and Destination. The card also details applied security controls and the final rule action (e.g., blocked or allowed) for the specific event.



> **Note**
>
> Interactive elements within the Event Details Card may display additional information upon hover or click.

Click on an Event ID within the table to automatically filter the report and display all correlated events.



5. (Optional) Refine your search using advanced filters. For detailed information on all available filtering and search options, see Filtering and Search Options.
6. (Optional) To export the events report, click the **Export CSV** button at the top-right corner of the table. This downloads the current view of the report in CSV format for further analysis or record-keeping. For detailed instructions on exporting report data, see Export Report Data to CSV.

Filter the Report by Firewall Requests

Provides instructions for completing the Filter the Report by Firewall Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

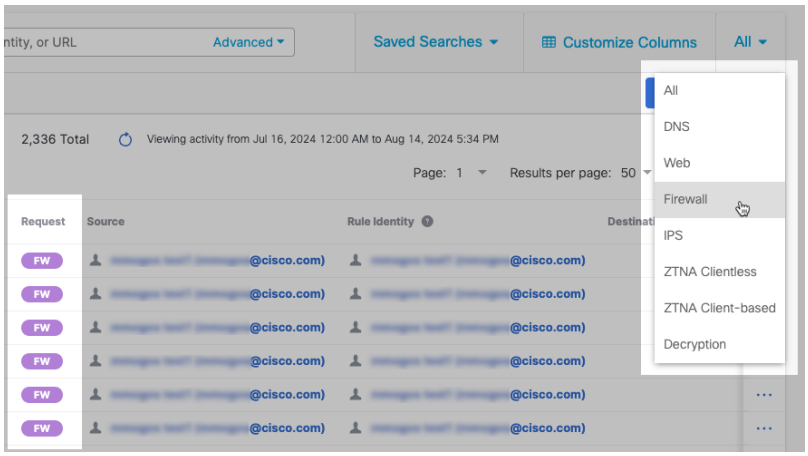
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view events from the **last 24 hours** (default), **Yesterday** , **Last 7 Days**, **Last 30 Days**, or a **Custom range**.

   The label **FW** in the **Request** column indicates a Firewall event.
3. Select the **Firewall** option from the dropdown menu at the top right to filter the report for Firewall events. Columns and Filter options update to those that are relevant to Firewall events.



4. Click the row to view Event Details.

   The Activity Search Report displays Event Details for each search result in a navigation drawer on the right. For more information, see View Activity Search Report Actions.

   Firewall event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see View and Customize the Activity Search Report.

   - **Action**
   - **Time**
   - **Rule Name**
   - **Source Geolocation**
   - **Source**
   - **Destination IP**
   - **Categories**
   - **File Name**
   - **Protocol**
   - **Application Protocol**

   Firewall event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Source IP	The source IPv4 or IPv6 address. Supports both compressed and long-form IPv6 address formats.
Source Port	The network port number on the source host from which the request originated.

Field Name	Description
Destination Port	The TCP or UDP port number on the destination host to which the request was sent. This field identifies the specific service or application targeted by the connection (for example, port 80 for HTTP or port 443 for HTTPS).
Resource/Application	The name of the resource or application.
Session Bytes Sent	The total number of bytes sent during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data sent from the source to the destination for the event session.
Session Bytes Received	The total number of bytes received during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data received from the destination by the source for the event session.
File Status (Disposition)	The file's Cisco AMP disposition: • **Clean**: Indicates that the AMP cloud categorized the file as clean. • **Malware**: Indicates that the AMP cloud categorized the file as malware, or local malware analysis identified malware. • **Unknown**: Indicates that the system queried the AMP cloud, but the AMP cloud has not assigned the file a disposition.
SHA256 Hash	The checksum of the file, if available and the event matched rules with File Type Control or File Inspection enabled.
File Transfer Direction	**DOWNLOAD**, **UPLOAD**, or **UNKNOWN**, if the event matched rules with File Type Control or File Inspection enabled.
Identified Threat	The name of the detected malware.
Malware Analysis Detected	If the event matched rules with File Inspection enabled, this field shows one of the following values as a result of file analysis by Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics. • **UNKNOWN** • **NOT ANALYZED** • **ANALYSIS COMPLETE NO VIRUS** • **ANALYSIS FAILED** • **ANALYSIS COMPLETE MALWARE DETECTED**
Threat Severity Score	The threat score most recently associated with this file. This is a value from 0 to 100.
File Type Identifiers	The type of file. For example, PDF or MSEXE.

Field Name	Description
File Size (bytes)	The size of the file in bytes, if the event matched rules with File Type Control or File Inspection enabled.
Archive File Name	The name of the archive file involved with the activity, if the event matched rules with File Type Control or File Inspection enabled.
Archive Extraction Depth	The level (if any) at which the file was nested in an archive file.
Archive SHA-256 Hash	The checksum of the archive file, if the event matched rules with File Type Control or File Inspection enabled.

Filter the Report by Web Requests

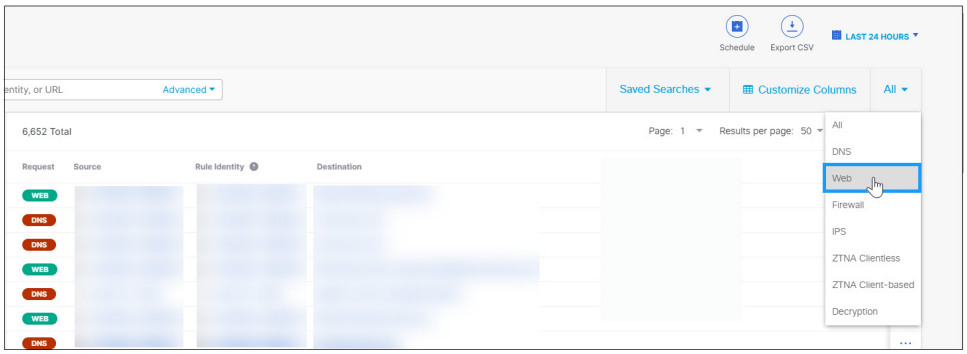
Provides instructions for completing the Filter the Report by Web Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

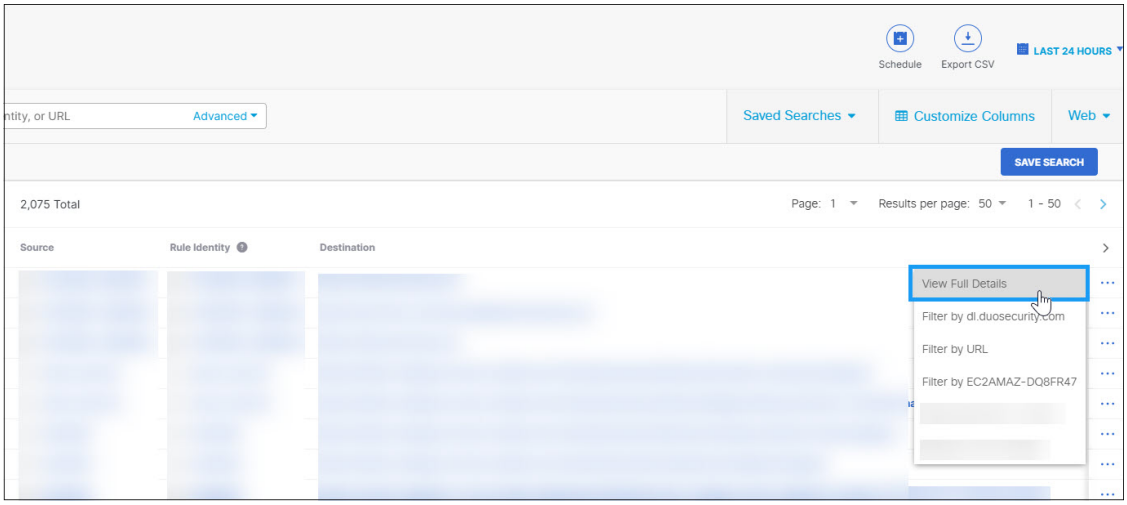
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **last 24 hours** (default), **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**.
3. From the drop-down menu at the top-right of the table, choose the **Web** option to filter the report for web events.



4. Click the ellipsis (**...**) and choose the **View Full Details** option to view web event details in the side panel.



5. The event details are displayed in the side panel. For more information, see View Activity Search Report Actions.

Web event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see Customize the Activity Search Report.

- **Action**
- **Time**
- **Rule Name**
- **Source Geolocation**
- **Source**
- **Rule Identity**
- **Internal IP Address**
- **External IP Address**
- **Destination**
- **Categories**
- **Resource/Application**
- **Application Category**
- **Content Type**
- **Request Method**
- **Referrer**
- **Status Code**

Web event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Hostname	Fully Qualified Domain Name (FQDN) of the machine or container from which the event originated.
File Action (Remote Browser Isolation)	Action taken on a file, such as Viewed, Original File Downloaded, Sanitized PDF File Downloaded.
Total Size, in Bytes	The number of bytes sent from the client for all the requests, including HTTP headers, for example, 234.
User Agent	The user agent string as captured by the proxy, for example, Mozilla 5.0 (X11; Linux x86_64; rv:12.0) Gecko 20100101 Firefox 21.0.
SHA256 Hash	This represents the SHA-256 hash of the response body.
Egress IP Address	The IP address is used by the proxy to communicate with the origin server. Dot notation is used for IPv4 and RFC 5952 is used for IPv6 , for example, 1.2.3.4, 2001:db8::1.
Egress Data Center	The data center that processed the request.
YouTube Channels	The YouTube channel name, such as @Cisco in the Cisco YouTube channel (https://www.youtube.com/@Cisco).

Field Name	Description
YouTube Categories	The set of YouTube categories, such as Education, Entertainment, Animation.

Edit a Private Access Rule

Provides instructions for completing the Edit a Private Access Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

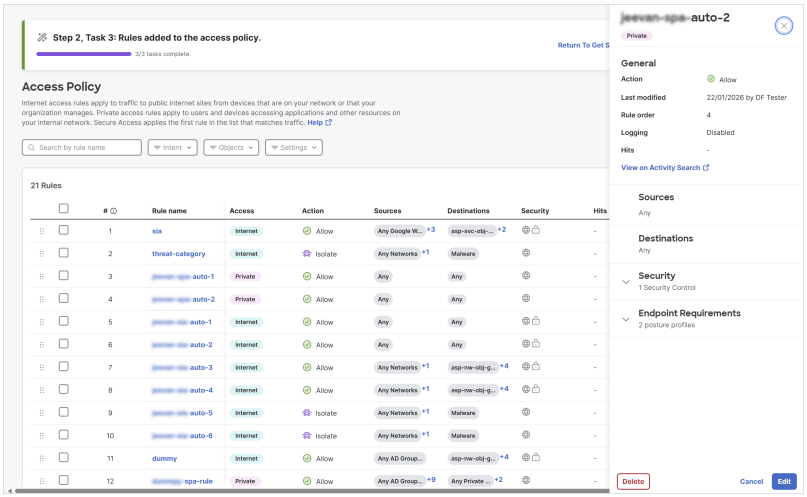
After a private access rule is created in Secure Access, you can modify the access rule's criteria and security control options.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy**.
2. In the access rules table, click the name of a private rule that you want to edit.
3. In the rule details section, click **Edit** to modify the access rule.



4. Edit the name and priority of the access rule, and other criteria.

   For more information about private access rules, see Add a Private Access Rule.

5. Click **Save**.

About ZTA Private Access Enforcement

Describes About ZTA Private Access Enforcement in Cisco Secure Access. Secure Access has a single Access policy, which consists of policy rules and settings.

Secure Access has a single Access policy, which consists of policy rules and settings. There are two types of access rules:

- Private access rules, which controls access to applications hosted from your data center and private clouds.
- Internet access rules, which controls access to resources on the internet from managed devices.

Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization. Before you start adding rules to your policy, we recommend that you read through the topics in Manage the Access Policy.

Secure Access supports Zero Trust Access (ZTA) for secure remote access connections to configured private resources. We recommend that you read through the topics in Manage Private Resources and Manage Connections to Private Destinations for a thorough understanding of ZTA private access.

You configure private access rules to control the access and security of your private resources and protect the traffic in your organization. By default, traffic is handled by the first rule in the list that matches the traffic. Rules lower in the list have no effect on traffic that matches a rule higher in the list.

Secure Access provides several enforcement modes which provide a flexible approach to policy evaluation by allowing IT administrators to apply rules based on a broader set of criteria. The following topics describe the enforcement modes for ZTA private access:

- Most specific match enforcement mode – This is the **default** enforcement mode for ZTA private access.
- Multi-app match enforcement mode – This enforcement mode option considers all possible private resources matches (including duplicates) for a given access request during policy evaluation, rather than narrowing down to only one most-specific resource match.
- Multi-app with resolved IP match enforcement mode – This enforcement mode option identifies all the possible private resources that would be matched to resolved IP addresses following DNS resolution, and considers all possible private resources (across both FQDN and resolved IPs) during policy evaluation equally.

Note

For information about changing your organization's enforcement mode, contact Cisco Secure Access Support. For more information, see the contact support section in the Welcome to Secure Access topic.

Tip

Secure Access Packages and Feature Availability

Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. See also, Cisco Secure Access Packages.

Most Specific Match Enforcement Mode

Describes Most Specific Match Enforcement Mode in Cisco Secure Access. The default enforcement mode for ZTA private access follows a top-down approach to private access rule processing.

The default enforcement mode for ZTA private access follows a top-down approach to private access rule processing. Each request is evaluated against the defined list of rules in order of priority until it finds a rule that matches its criteria. Once a match is found, the access policy applies the specified action (allow or block).

> **Note**
>
> Traffic to private destinations is blocked by default. You must create rules to allow traffic to private destinations.

For each ZTA private access request, the **default** mode for policy evaluation functions as follows:

- Prior to policy evaluation, the ZTA proxy selects the one most-specific private resource to move ahead for the request.
- Only this one single resource is considered during policy evaluation, and only rules that include that resource in its destination can possibly be matched to.
- In order for a rule to match a request, along with defined source and destination, endpoint posture profile requirements associated with the rule must also be met.
- In the case of exactly duplicated private resources (identical IP/FQDN, port and protocol), this approach would have multiple equally specific matches, in which case ZTA would pick an arbitrary one of the matching resources.

Multi-App Match Enforcement Mode

Describes Multi-App Match Enforcement Mode in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

This enforcement mode for ZTA private access considers all possible private resources matches (including duplicates) for a given access request during policy evaluation, rather than narrowing down to only one most-specific resource match, while still matching to rules based on the top-down rule priority ordering.

The ZTA private access enforcement evaluation functions as follows:

1. Identify all possible private resources that apply to the access request destination.
   a. In the case of IPs, match all resources that have IPs or CIDRs that contain the requested destination IP.
   b. In the case of FQDNs, match all resources that have exact domains or wildcards that contain the requested FQDN.
2. Evaluate for rules that would apply to the requesting user/source and ANY of the identified possible resource matches.
3. Still prioritize the rule priority/definition order to decide which rule to match to:
   a. Evaluation will be done top-down, with rule #1 being checked before rule #2, and so on.
   b. Each rule is evaluated and moved past if there is no perfect match (including posture requirements), but in case it is a rule match then evaluation stops with that rule as the selection and the proxy moves past the evaluation phase.
4. In the case of a “tie-breaker” scenario the most-specific match resource will be considered.

Scenario 1: Multiple matching IP/CIDR destinations in different resources

Describes Scenario 1: Multiple matching IP/CIDR destinations in different resources in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Resource A -> 10.10.10.10.

Resource B -> 10.10.10.10 (same port and protocol as Resource A)

Resource C -> 10.10.10.0/24

Resource D -> 10.0.0.0/8

Access policy rules:

1. UserGroupA has access to Resource A
2. UserGroupB has access to Resource B
3. UserGroupC has access to Resource C
4. UserGroupD has access to Resource D

Behavior:

- When a request comes in for "10.10.10.10" as the destination, all resources (A to D) are identified and taken forward for policy evaluation.
- At policy evaluation, a request for "10.10.10.10" can match to any of rules #1 to #4 from a destination point of view (logical equivalent is that – rule destination should be contained within the set of all possible resource matches that were identified).
- But, since each rule has an explicitly different source, the rule would only be matched to if the source also aligns (i.e. user from UserGroupA would only ever match to rule #1, and so on).

Scenario 2: Multiple matching FQDN destinations in different resources

Describes Scenario 2: Multiple matching FQDN destinations in different resources in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Resource A -> "test.acme.com".

Resource B -> "*.acme.com".

Resource C -> "test.acme.com".

Access policy rules:

1. UserGroupA has access to Resource A
2. UserGroupB has access to Resource B
3. UserGroupC has access to Resource C

Behavior:

- Exactly like the IP/CIDR Scenario 1, all resources (A to C) would be identified for a request to "test.acme.com".
- Exactly like Scenario 1, while such a request can be matched to any of rules #1 to #3 in terms of destination, matching to a rule also requires matching to the source and so access would be segregated based on user identity; i.e. user from UserGroupA would only ever match to rule #1, and so on.

Scenario 3: Multiple matching rules by source and destination – rule ordering priority in effect

Describes Scenario 3: Multiple matching rules by source and destination – rule ordering priority in effect in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Resource A -> 10.10.10.0/24.

Resource B -> 10.10.10.10.

Access policy rules:

1. UserGroupA has access to Resource A.

2. UserGroupA has access to Resource B.

Behavior:

- Like the earlier scenarios, a request to “10.10.10.10” would match to both resources A and B.
- Unlike earlier scenarios, both rules can now apply to the same user (from UserGroupA) and both rules can provide access but to 2 different resources.
- But, ZTA top-down rule enforcement based on rule priority is maintained, and because a request from UserGroupA to "10.10.10.10" would match to rule #1, rule #2 would never even be checked; the rule providing access to Resource B would never be hit, even though it is the most specific resource.

Scenario 4: Tie-breaker scenarios for multiple valid resource destinations in matched rule

Describes Scenario 4: Tie-breaker scenarios for multiple valid resource destinations in matched rule in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Resource A -> 10.10.10.10.

Resource B -> 10.10.10.10 (same port and protocol as Resource A).

Resource C -> 10.10.10.0/24.

Access policy rules:

1. UserGroupA has access to Resource A OR Resource C.
2. UserGroupB has access to Resource A OR Resource. The resulting behavior is:

- Like the earlier scenarios, a request to "10.10.10.10" would match to all resource (A to C).
- Like the earlier scenarios, a request from user in UserGroupA would match to rule #1, and for UserGroupB would match to rule #2, for the same "10.10.10.10" destination.
- Unlike earlier scenarios, both rules have multiple destination resources that all map to the "10.10.10.10" destination.
- For rule #1, since Resource A (10.10.10.10) is more specific than Resource C (10.10.10.0/24), access will be provided to Resource A.
- For rule #2, since Resource A and B are identical in all sense (10.10.10.10 with same port and protocol), we will arbitrarily pick one to provide access.

Multi-App with Resolved IP Match Enforcement Mode

Describes Multi-App with Resolved IP Match Enforcement Mode in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

This enforcement mode for ZTA private access combines the multi-app enforcement mode with additional identification of all possible private resources that would match to the resolved IP addresses of any domain-based resources found during the initial multi-app identification:

- For each domain-based private resource that is identified, DNS resolution is performed at the ZTA proxy and all possible resolved IP addresses for the requested FQDN, ZTA enforcement will additionally identify all the possible private resources that would be matched to the resolved IP addresses.
- ZTA enforcement next considers all possible private resources (across both FQDN and resolved IPs) during policy evaluation equally, while still matching to rules based on the top-down rule priority ordering.

The ZTA private access enforcement evaluation functions as follows:

1. Identify all possible private resources that apply to the access request destination.

2. For FQDN-based resources only, complete DNS resolution for all destinations even before it is known whether we will proceed with this resource at the end of policy evaluation.

   Note

   DNS resolution for this step would continue to happen at the ZTA proxy as in any other domain-based flow:

   a. In the case of a resource behind an IPSec tunnel, the "internal DNS server" specified in the private resource definition would have to be accessible behind the same IPSec tunnel. The proxy would reach out to the DNS server for resolution in the same way as it would reach out to the destination resource itself.

   b. In the case of a resource behind an Resource Connector Gateway (RCG), the resource DNS server would also be hosted behind the RCG. The proxy would reach out to the RCG for DNS resolution, and the RCG would complete DNS resolution and return the results to ZTA.

3. Use the resolved IPs from DNS to re-identify all possible resources that apply to the entire subset of DNS-resolved IPs.
4. Evaluate for rules that would apply to the requesting user/source and ANY of the identified possible resource matches. This includes both initially found FQDN-based resources, and IP-based resources that were identified after DNS resolution.
5. Still prioritize the rule priority/definition order to decide which rule to match to.
6. In case of a "tie-breaker" scenario (access requests matches to rule with multiple destinations that are all "valid" in multi-match approach), the most-specific match resource will be considered, with respect to the original requested destination.
   a. So, if the original request was to an FQDN, we would select the destination in the matched rule that corresponds to the most-specific FQDN over IP-based resources, if available.
   b. If there are no FQDN destinations in the matched rule for a FQDN-based request, we would match to the most specific IP-based resource (based on the DNS resolved IP).

Scenario 1: FQDN resource-based rule at higher priority than IP resource-based rule

Describes Scenario 1: FQDN resource-based rule at higher priority than IP resource-based rule in Cisco Secure Access. Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource B -> defined with destination "10.10.10.0/24".

Access policy rules:

1. UserGroupA has access to Resource A
2. UserGroupA has access to Resource B
3. UserGroupB has access to Resource A
4. UserGroupB has access to Resource B

Behavior:

- When a user in either group A or B accesses the "acme.com" destination, they would be matched to both Resource A and B; however, due to rule priority ordering, they would match to rules #1 and #3 respectively for all accesses. They would never match to the resolved-IP based resource.

- When a user in either group A or B accesses an IP within the "10.10.10.0/24" CIDR, they would be matched to only Resource B. As a result, they would only ever match to rules #2 and #4 respectively for all accesses.

Scenario 2: IP resource-based rule at higher priority than FQDN resource-based rule

Describes Scenario 2: IP resource-based rule at higher priority than FQDN resource-based rule in Cisco Secure Access. Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource B -> defined with destination "10.10.10.0/24"

Access policy rules:

1. UserGroupA has access to Resource B
2. UserGroupA has access to Resource A
3. UserGroupB has access to Resource B
4. UserGroupB has access to Resource A

Behavior:

- When a user in either group A or B accesses "acme.com" destination, they would be matched to both Resource A and B. But due to rule priority ordering, they would match to rules #1 and #3 respectively for all accesses. They would never match to the original FQDN-based resource.
- When a user in either group A or B accesses an IP within the "10.10.10.0/24" CIDR, they would be matched to only Resource B. As a result, they would only ever match to rules #2 and #4 respectively for all accesses.

Scenario 3: Tie-breaker scenario for FQDN-IP overlap within the same rule

Describes Scenario 3: Tie-breaker scenario for FQDN-IP overlap within the same rule in Cisco Secure Access. Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource A -> defined with destination "acme.com", which resolves to 10.10.10.10.

Resource B -> defined with destination "10.10.10.0/24".

Access policy rules:

1. UserGroupA has access to Resource A OR Resource B

Behavior:

- Like earlier scenarios, a request to "acme.com" would match to both resource A and B.
- But unlike earlier Scenarios, a request from a user in UserGroupA would match to rule #1 that has two valid destinations.
- In this case, because the original request was to FQDN ("acme.com"), Resource A is the most specific match to the access request, and so access will be provided to Resource A.

Allowing Traffic from Users and Devices on the Network

Describes Allowing Traffic from Users and Devices on the Network in Cisco Secure Access. In addition to creating access rules for remote users accessing private resources, you must create rules to allow traffic from users and devices on the network, including those in branch offices.

In addition to creating access rules for remote users accessing private resources, you must create rules to allow traffic from users and devices on the network, including those in branch offices.

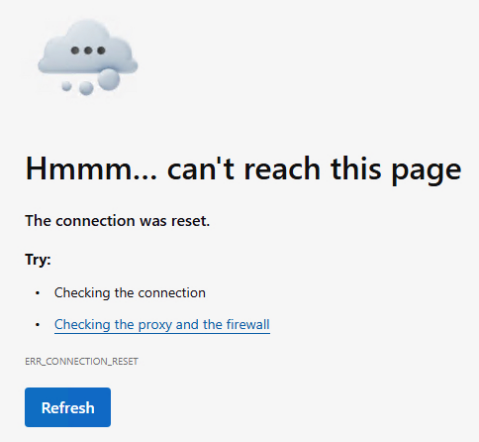
Devices that might require such a rule include kiosks, Internet of Things (IOT) devices, and printers.

When you create the rule, you can create one or more private resources to use as sources and destinations, or you can add sources and destinations directly in the rule. For more information, see Manage Branch Connections.

Blocking Access to Private Destinations

Describes Blocking Access to Private Destinations in Cisco Secure Access. When users request a private destination that is blocked by the organization's Access policy, Secure Access presents a page indicating that the destination is not reachable.

When users request a private destination that is blocked by the organization's Access policy, Secure Access presents a page indicating that the destination is not reachable. You cannot customize this page.



The user's access is blocked by a private access rule with the **Block** action and the default private access rule.

To block a private resource, the organization must meet these requirements:

- The user's device has the Cisco Secure Client installed.
- Decryption is enabled on the private resource configuration page.
- VPN connections are not enabled on the private resource configuration page.
- Zero Trust connections are enabled for the resource.

Troubleshoot Private Access Rules

Describes Troubleshoot Private Access Rules in Cisco Secure Access and outlines General Troubleshooting Tips, Guidelines for When a Rule Does Not Match Traffic as Expected, and Guidelines for When Traffic Is Unexpectedly Allowed. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

To troubleshoot your private access rules, review these guidelines.

General Troubleshooting Tips

- Navigate to the Overview page for possible status notifications.
- Use Activity Search to look for logged events. Use Events to investigate browser-based ZTA connections.
- While creating a private access rule, the **Next** button is not available until you give the rule a name and then click out of the Rule name field.

Guidelines for When a Rule Does Not Match Traffic as Expected

Try these suggestions, either to temporarily suspend problematic blocks and allow end users to access a needed resource, or to narrow down the cause of the problem.

- Check the private resource configuration.
- Make sure that the internal address for the private resource does not duplicate or overlap with any other private resource or IP address or CIDR block typed directly into the destination in an access rule. For example, if Private Resource A is defined with a CIDR block as the internal address, and Private Resource B is defined with an IP address that is included in the same CIDR block.
- Check the sources and destinations configured in the rule to be sure they include the problematic source and destination.
- Endpoint requirements as specified in posture profiles are matching criteria, not security criteria. Try specifying posture profiles that have no requirements and see if the traffic matches.
- Check other rules in the rule order; traffic may be hitting a different rule than the one you expect.
- If you deployed the client on iOS devices, see unique matching information in the "Guidelines and Limitations" section of the Set up the Zero Trust Access App for iOS Devices topic.
- If you configured a Private Resource, then modified the automatically created entry on the Traffic Steering page (for example, to exclude subdomains from zero-trust access), then modified addresses on the Private Resource configuration page, the resource addresses are not updated for traffic steering purposes. You must manually update the address(es) on the Traffic Steering page.

Guidelines for When Traffic Is Unexpectedly Allowed

A few things to try, either to block problematic traffic, or to narrow down the cause of the problem.

- Because traffic to private destinations is blocked by default, this means there is one or more existing rules that explicitly allows this traffic. You will need to find any such rules.
- Make sure the applicable rule is enabled (toggle at top of rule page)
- Make sure IPS is not disabled in the rule default or in the rule. Any rule tagged to use the default setting continues to use the default setting even if the default setting has changed.
- Make sure Decryption is not disabled in Global Settings.
- Check each rule component (rule action and each posture and security control) to be sure each specifies the behavior you expect.
- Check to see that an expected exception to connect to the private resource appears as expected on the Traffic Steering page (Connect > End User Connectivity > Zero Trust.)
- To immediately block access to a problem destination that is unexpectedly being allowed, you can create a new access rule (using the "Enter manually" option for source and/or destination if necessary) and put this rule at or near the top of the rule list on the Policy page so it hits before more general rules that would otherwise apply to the traffic.

Guidelines for When Traffic Is Unexpectedly Blocked

A few things to try, either to temporarily suspend problematic blocks, or to narrow down the cause of the problem.

- Verify that any existing rule allowing the traffic is enabled.
- To allow immediate access to a necessary destination that is being blocked, you can create a new access rule allowing the traffic (using the "Enter manually" option for source and/or destination if necessary).
- You can disable intrusion prevention (IPS) for a rule.

- You can disable intrusion prevention (IPS) on the Rule Defaults page, which disables it for all rules that are configured to use the default setting for IPS.
- You can disable decryption for intrusion prevention (IPS), file inspection, and file type blocking for all rules in Global Settings, which effectively disables intrusion prevention.
- If a Zero Trust connection is unsuccessful:
  - Make sure that zero trust connections are enabled for the resource.
  - Check the Traffic Steering page (Connect > End User Connectivity > Zero Trust) for absence of, exceptions to, or conflicts with the applicable Private Resource configuration.
  - Endpoint requirements as specified in the applicable zero trust posture profile.
  - Posture profiles are rule-matching criteria, not security criteria. Try specifying posture profile(s) that have no requirements and see if the traffic matches.
  - For browser-based connections, you may need to configure a custom host header for the resource in order to forward traffic correctly. For more information, see Add a Private Resource.
- If a VPN connection is unsuccessful, ensure that:
  - There is a VPN traffic steering rule for the applicable network address space
  - There is an access rule allowing the traffic (either for a configured private resource or for the applicable network address space)
  - If a Private Resource is configured for the resource, it must permit VPN connections.
  - If a private resource is configured for client-based zero trust access and the user device is enrolled for zero trust access, the device will use zero trust access to connect. Check the zero trust access connection.
- Assess whether the following situation applies: App A is dependent on App B, but App B is not included in the private resource or access rule configurations.
- If your organization is using Resource Connectors, see Troubleshoot Resource Connectors and Connector Groups.
- If all traffic is blocked, make sure you have not inadvertently blocked traffic to a destination that is required infrastructure for managing access. For example, make sure there is no Geolocation rule that blocks traffic to your identity services (IdP) provider.

30 IPS Profiles

Topics:

- Manage IPS Profiles

Provides an overview of IPS Profiles in Cisco Secure Access, including Manage IPS Profiles. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage IPS Profiles

Describes Manage IPS Profiles in Cisco Secure Access. Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats.

Secure Access's Intrusion Prevention System (IPS) protects your network and assets from known threats. You define IPS profiles with signature lists that group these threats and allow you to specify how each threat should be handled. You then specify an IPS profile in each access rule.

> **Note**
>
> IPS in Cisco Secure Access does not support traffic from the Secure Client roaming module.

How IPS Works

Describes How IPS Works in Cisco Secure Access. Secure Access IPS uses signature-based detection and provides an added layer of protection against threats such as malware, botnets, phishing, and command and control call backs.

Secure Access IPS uses signature-based detection and provides an added layer of protection against threats such as malware, botnets, phishing, and command and control call backs. When IPS is enabled, it's enabled for your entire environment, including all of your network tunnels.

IPS Signature Lists contain signatures filtered by three actions:

- **Block**–Signatures are screened for threats on your network and recorded in Activity Search.
- **Log Only**–Signatures are recorded in Activity Search, but not screened for threats.
- **Ignore**–Signatures are completely ignored and not recorded in Activity Search.

Hit Counts

Describes Hit Counts in Cisco Secure Access. Hit counts represent the amount of times signatures were detected on your network for a certain period.

Hit counts represent the amount of times signatures were detected on your network for a certain period. By default, hit count durations for all lists are set to the last 24 hours. Each list's hit count duration can be changed to the last five minutes, last hour, yesterday, or the last 30 days. Hit counts may also be reset at any time.

Cisco-Provided IPS Signature Lists

Describes Cisco-Provided IPS Signature Lists in Cisco Secure Access. The IPS signature lists provided by Cisco are constructed based on the balance between network connectivity and network security.

The IPS signature lists provided by Cisco are constructed based on the balance between network connectivity and network security. The more a list is focused on security the more signatures are set to Blocked in that list rather than Log Only or Ignored.

- **Connectivity Over Security**–This signature list places an emphasis on network connectivity and throughput at the possible expense of security. Traffic is inspected less deeply, and fewer rules are evaluated.
- **Balanced Security and Connectivity**–This signature list attempts to balance network connectivity and security to keep users secure while being less obtrusive toward normal traffic. Less strict than Connectivity Over Security.
- **Security Over Connectivity**–This signature list emphasizes security over network connectivity. Traffic is inspected more deeply and more rules are evaluated. The result is an increase in false positives and network latency.
- **Maximum Detection**–This signature list places all emphasis on security, such that network connectivity and throughput are compromised. Only select this setting when total protection is required as alerts must be monitored and validated manually.

Decryption is Required for Effective Intrusion Prevention

Describes Decryption is Required for Effective Intrusion Prevention in Cisco Secure Access. IPS requires decryption in order to effectively evaluate threats in traffic.

IPS requires decryption in order to effectively evaluate threats in traffic. Decrypting traffic requires certificates that you must provide and manage:

- Certificates required for decrypting traffic to internet destinations. See Certificates for Internet Decryption for more information.
- Certificates required for decrypting traffic to private destinations. See Manage Certificates for Private Resource Decryption for more information.

Exceptions for Traffic That Should Not be Decrypted

Describes Exceptions for Traffic That Should Not be Decrypted in Cisco Secure Access. If regulation or policy requires traffic to certain types of internet destinations to remain confidential, you can use the system-provided Do Not Decrypt List for this purpose.

If regulation or policy requires traffic to certain types of internet destinations to remain confidential, you can use the system-provided Do Not Decrypt List for this purpose. Navigate to **Secure** > **Settings** > **Do Not Decrypt Lists** and click the **System Provided Do Not Decrypt List**. (Additional lists that you create on this page do not apply to IPS.) For more information, see Important Information About Do Not Decrypt Lists.

IPS is Used in Both Types of Access Rules

Describes IPS is Used in Both Types of Access Rules in Cisco Secure Access. IPS profiles are used in both internet access rules and private access rules.

IPS profiles are used in both internet access rules and private access rules.

Settings such as the default IPS profile and the decryption setting in global settings apply to both types of access rules.

Add a Custom IPS Signature List

Describes Add a Custom IPS Signature List in Cisco Secure Access. You can use the system-provided signature lists in custom IPS profiles to build your own custom IPS signature lists that fit your organization's specific needs.

You can use the system-provided signature lists in custom IPS profiles to build your own custom IPS signature lists that fit your organization's specific needs.

Prerequisites

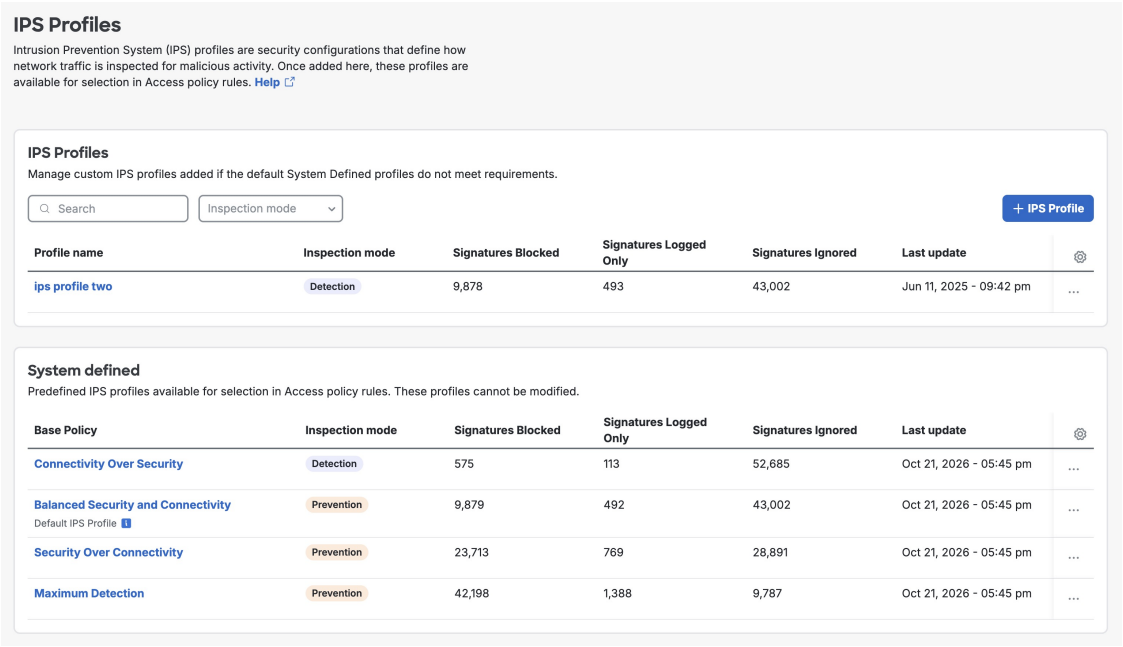
- Full admin access to the Secure Access dashboard. For more information, see Manage Accounts.

Procedure for Adding a Custom IPS Signature List

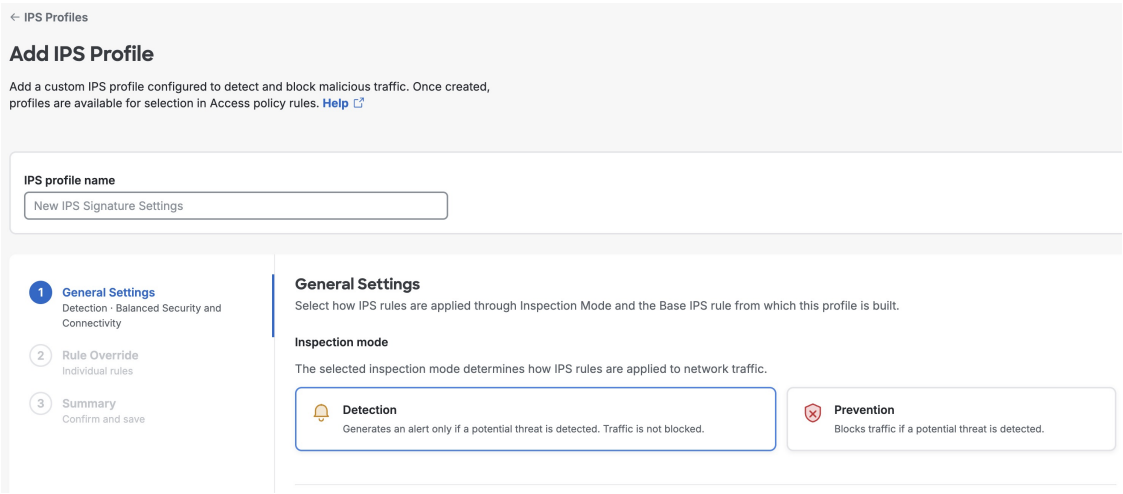
Provides instructions for completing the Procedure for Adding a Custom IPS Signature List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Profiles** > **IPS Profiles**.

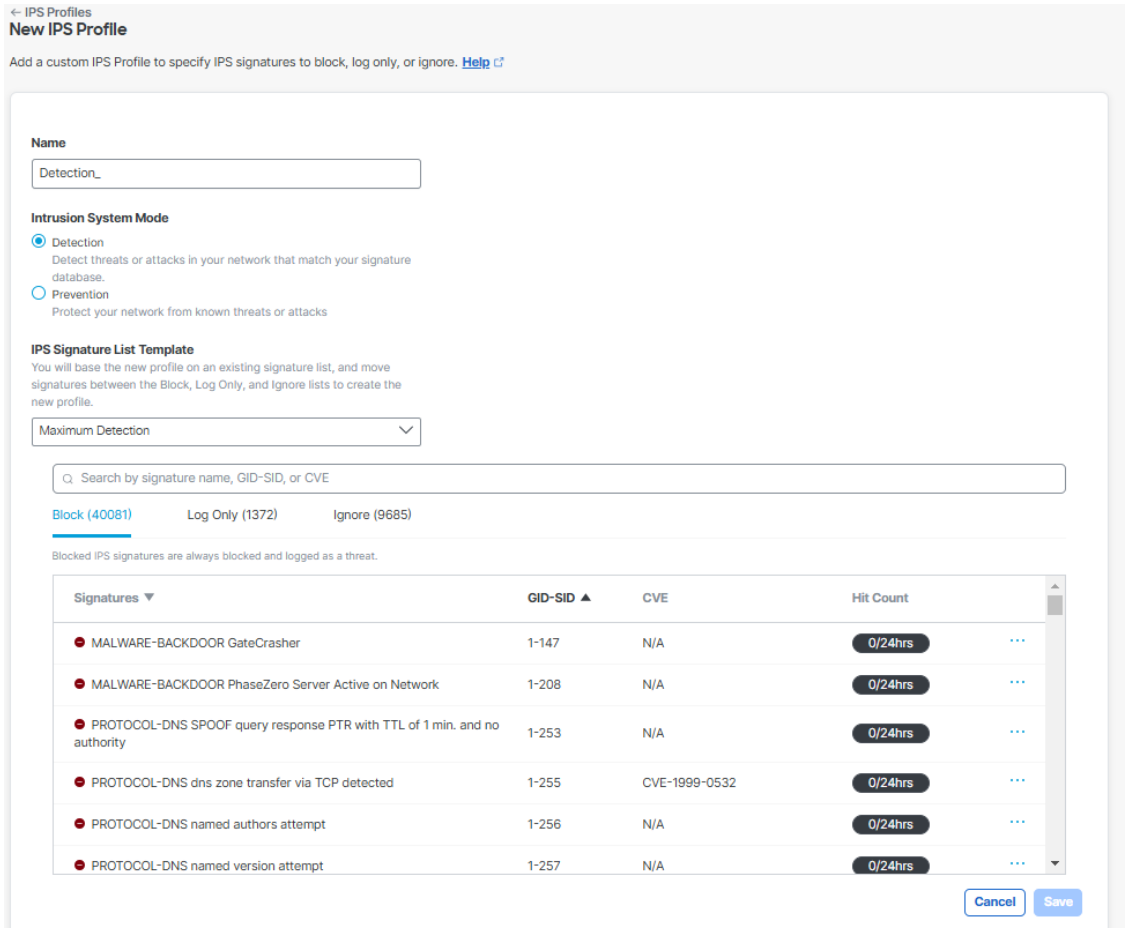


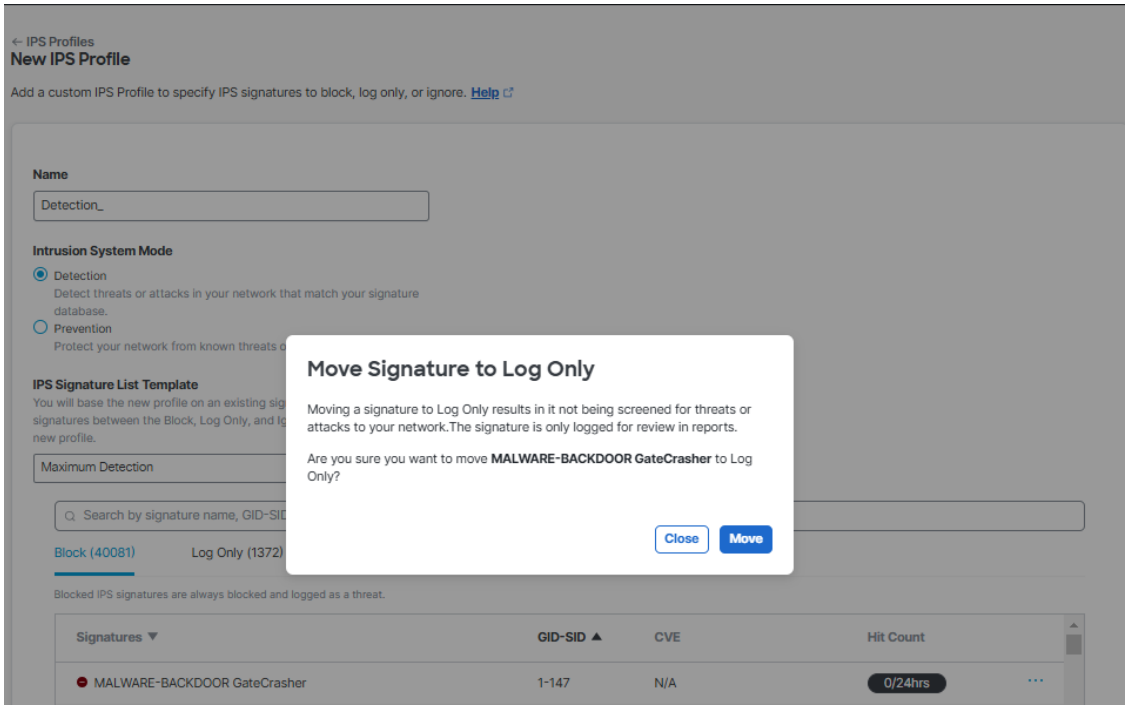
2. Click **+ IPS Profile** and enter a name for your custom signature list and choose either **Detection** or **Prevention** for **Intrusion System Mode**.



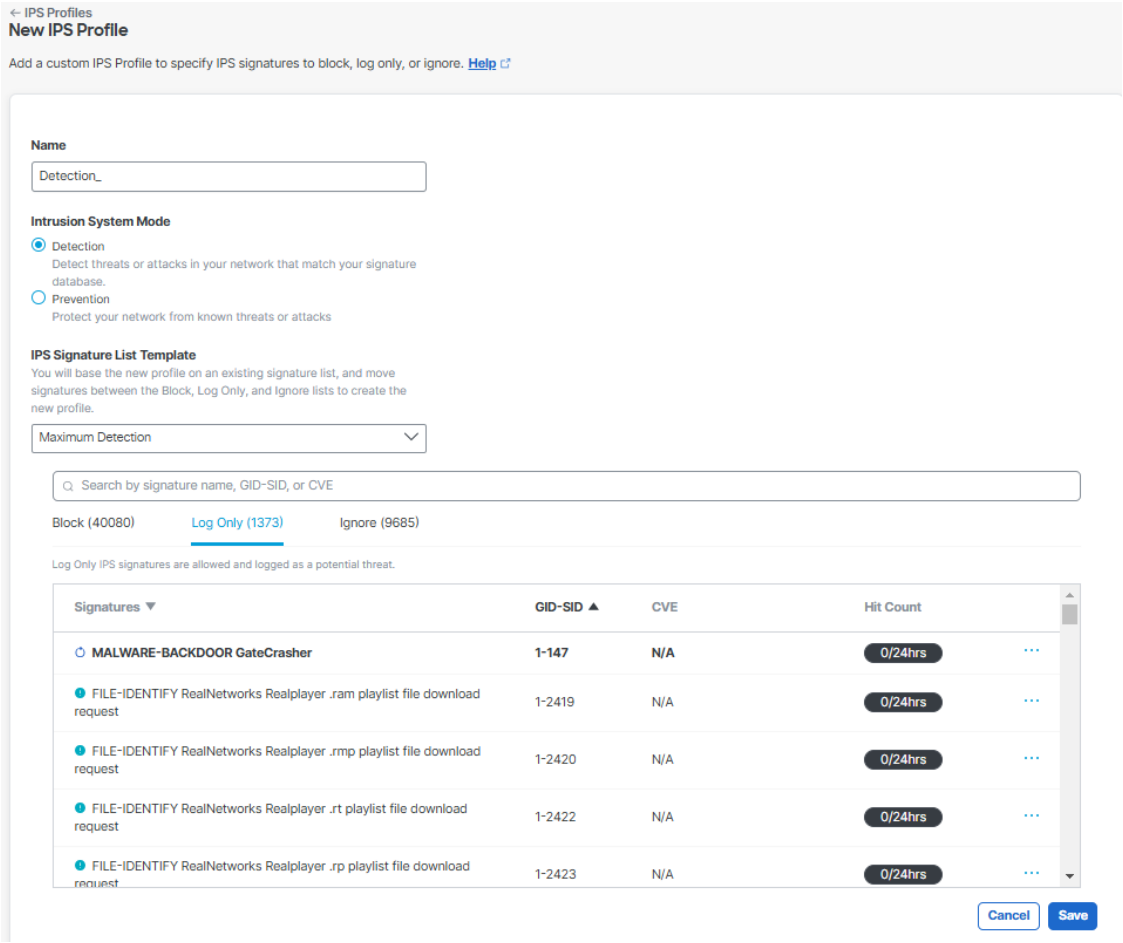
- **Detection**–Detect threats or attacks in your network that match your signature database. When Detection Only mode is used, your IPS settings can be tested on your network without affecting traffic. Signatures that would be blocked in Protection mode will be logged in Activity Search as "Allowed (Would Block)" under IPS Signatures.
- **Prevention**–Protect your network from known threats or attacks.

3. Under **IPS Signature List Template**, choose the signature list to apply these settings to.
4. Change which signatures are blocked, logged only, or ignored. Click the menu next to the signature you want to move and click **Move to Block**, **Move to Log Only**, or **Move to Ignore**. A prompt appears asking you to confirm your choice.





5. Click **Move**. The signature you moved is now within the section you chose.



6. Click **Save** to finish creating your custom signature list.

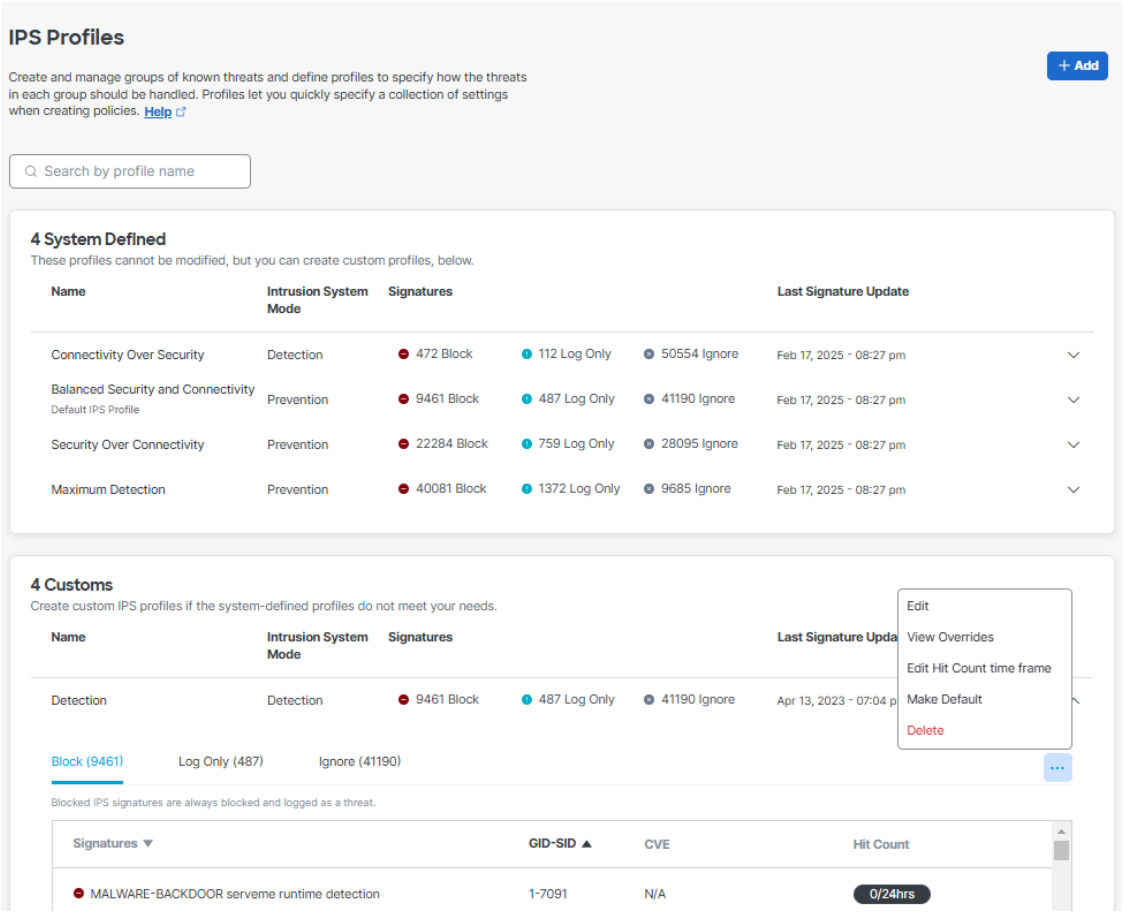
Reset a Signature's Action

Provides instructions for completing the Reset a Signature's Action workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

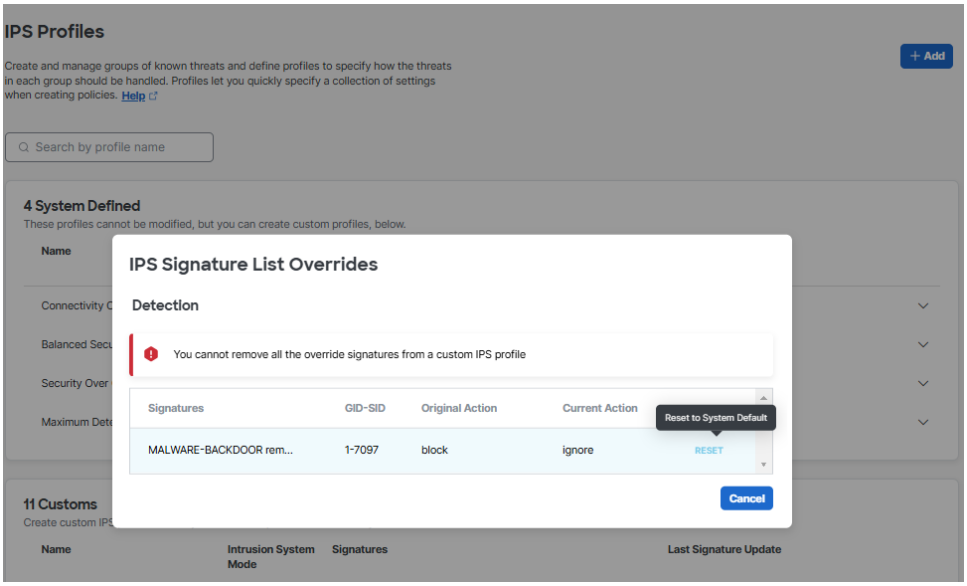
Procedure

---

1. Navigate to **Secure** > **Profiles** > **IPS Profiles**.
2. Under Custom IPS Signature Lists, click the list you want to edit. The list expands.
3. Click the More Actions menu and click **View Overrides** to view the list of signatures that have been moved.



4. Locate the signature you want to reset and click **Reset to System Default** for that signature. A prompt appears asking you to confirm your choice.



5. The signature you reset is now set back to its original action from the default list your custom list is based on.
6. Click **Save** to finish editing your custom signature list.

31 Security Profiles

Topics:

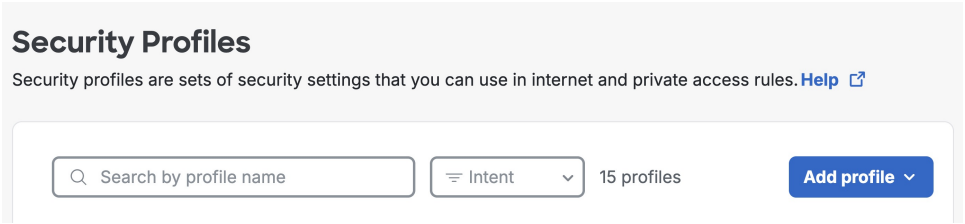
- Manage Security Profiles
- Security Profiles for Internet Access
- Enable SafeSearch
- Security Profiles for Private Access

Provides an overview of Security Profiles in Cisco Secure Access, including Manage Security Profiles, Security Profiles for Internet Access, and Enable SafeSearch. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Security Profiles

Describes Manage Security Profiles in Cisco Secure Access. A Cisco Secure Access Security profile is a reusable component that you can use in the rules on the Access policy.

A Cisco Secure Access Security profile is a reusable component that you can use in the rules on the Access policy.



There are two types of Security profiles:

- **Security Profiles for internet access rules**–For more information, see Security Profiles for Internet Access.
- **Security Profiles for private access rules**–For more information, see Security Profiles for Private Access.

> **Note**
>
> You can configure up to 100 Security profiles in Secure Access, which includes security profiles for both internet and private access rules.

Security Profiles for Internet Access

Describes Security Profiles for Internet Access in Cisco Secure Access. A Security profile for internet access includes security controls and other settings such as acceptable use controls that you configure as a set.

A Security profile for internet access includes security controls and other settings such as acceptable use controls that you configure as a set. Once you add the security profile in Secure Access, you can use this profile on one or more internet access rules in the Access policy. For example, you can use different security profiles for different sets of users, or for different types of destinations.

> **Note**
>
> Secure Access comes with a partially configured security profile for internet access; you must either configure that profile to suit your needs or create a different security profile and designate that profile as the default security profile for internet access rules.

To configure security profiles for internet access, see detailed information in Add a Security Profile for Internet Access.

Functionality Included in a Security Profile for Internet Access

Describes Functionality Included in a Security Profile for Internet Access in Cisco Secure Access. You can configure various settings and security controls on a security profile for internet access.

You can configure various settings and security controls on a security profile for internet access.

- Decryption

- SSO Authentication
- Security and Acceptable Use Controls
- End-User Notifications

Decryption

Describes Decryption in Cisco Secure Access. Decryption is necessary for proper functioning of all features enabled in the security profile, and for processing traffic to most internet destinations in general.

Decryption is necessary for proper functioning of all features enabled in the security profile, and for processing traffic to most internet destinations in general. When enabled, all internet traffic will be decrypted except as specified in the selected Do Not Decrypt list. For more information about decryption, see Manage Traffic Decryption.

Generally, you should disable decryption only if the security profile will be used in rules that:

- Have only destinations to which traffic should never be decrypted, for example for privacy or confidentiality reasons, such as medical or financial sites, for locations that regulate this traffic.
- Have sources that only include devices on which you cannot install certificates required to decrypt and inspect traffic, such as devices that are not managed by your organization, for example vendors' or contractors' devices.
- Have only sources that cannot respond to certificates required for decryption, such as IoT devices, printers, or kiosks
- Allow access to applications that will not work properly if decryption is enabled, including Microsoft 365 and applications that use certificate pinning.
- Include only known safe destinations.

  For example, use this profile for rules that control access to the sites that IoT devices access in order to update their software.

If you enable decryption, you can opt not to decrypt traffic to specific destinations. For more information, see Important Information About Do Not Decrypt Lists.

SSO Authentication

Describes SSO Authentication in Cisco Secure Access. If your organization uses SSO authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

If your organization uses SSO authentication, you should generally enable this option on the networks and tunnels configured for the rules that use this profile.

Requirements for Enabling OIDC Authentication

- Configure Open ID Connect (OIDC) authentication to authorize connections to the Secure Web Gateway (SWG) from user devices on networks and network tunnels, and connections using Zero Trust Access (ZTA). For more information, see Configure Integrations with OIDC Identity Providers.

Requirements for Enabling SAML Authentication

- Configure SAML authentication to authorize connections to the SWG from user devices on networks and network tunnels, and connections using Zero Trust Access (ZTA). For more information, see Configure Integrations with SAML Identity Providers.
- Decryption must also be enabled for network SAML enforcement.

Requirements for Disabling SAML Authentication

- Decryption is disabled in the security profile, or is enabled only for notifications.
- The security profile will be used in rules that include sources that:
  - Are not configured for SAML authentication.

- Cannot be authenticated using SAML. For example, if the rule source includes:
  - Devices that are not managed by your organization, when certificates are required for authentication but cannot be installed on the device. Such devices might be used by contractors or vendors on your guest network.
  - Devices such as IoT devices, printers, or kiosks that cannot respond to authentication requests or present certificates required for authentication.
- Should not be authenticated using SAML. For example, if users should not be identified for privacy or confidentiality reasons, such as by regulation or policy.

Security and Acceptable Use Controls

Describes Security and Acceptable Use Controls in Cisco Secure Access. Configure security and control the use of the threat categories, file inspection, file type blocking, Content Disarm and Reconstruction (CDR), SafeSearch settings, and AI supply chain blocking.

Configure security and control the use of the threat categories, file inspection, file type blocking, SafeSearch settings, and AI supply chain blocking.

Option	Description	More Information
Threat Categories	Block traffic to sites that have been categorized as risky or threatening.	Manage Threat Categories
File inspection	Block download of files known to carry threats, and analyze files for suspicious behaviors.	Manage File Inspection
File type blocking	Block files based on filename extension, such as executable files.	Manage File Type Controls
SafeSearch	Return only family-friendly search results in popular search engines.	Enable SafeSearch
AI Supply Chain Blocking	Block end user attempts to download AI model files that are developed or authored by prohibited suppliers, released under a copyleft license, or capable of executing arbitrary code.	AI Supply Chain Report

Note

For acceptable use controls on access to web sites based on categories that are not known security threats, see Manage Content Category Lists. You will specify these categories or lists in access rules.

End-User Notifications

Describes End-User Notifications in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You configure two types of end-user notifications in security profiles for internet access:

- Block notifications that end users see instead of a browser error when they attempt to access a destination that is blocked by an access rule.

- Warning notifications that end users must click through in order to access destinations in rules configured with the Warn action.

For information about configuring Block and Warn pages, see Manage Notification Pages.

Get Started: Security Profiles for Internet Access

Describes Get Started: Security Profiles for Internet Access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Add a Security Profile. For more information, see Add a Security Profile for Internet Access.
- Modify or delete a Security Profile. For more information, see Edit a Security Profile and Delete a Security Profile.
- Enable SafeSearch for the organization. For more information, see Enable SafeSearch.

Add a Security Profile for Internet Access

Describes Add a Security Profile for Internet Access in Cisco Secure Access. A Cisco Secure Access Security profile is a set of security controls and other settings that you can use in access rules.

A Cisco Secure Access Security profile is a set of security controls and other settings that you can use in access rules.

For information about each of the components or controls that you can configure in a Security profile for internet access, see Security Profiles for Internet Access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- In Secure Access, configure the components that you will select in a security profile for internet access.
  - Add a **Do Not Decrypt** list. For more information, see Add a Do Not Decrypt List for Security Profiles.
  - Create the list of threat categories. For more information, see Manage Threat Categories.
  - Carefully review the information about enabling file analysis with Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics.
  - (Optional) Create custom notification pages that Secure Access will display when rules that use this security profile match traffic that blocks access or displays a warning. Customizations can include the logo, message, and contact information of your choice. For more information, see Notification Pages.

Procedure

> **Note**
>
> You can add up to 100 security profiles in Secure Access for the organization.

Configure the settings on a Security profile and add the profile to the organization. After you add the Security profile, configure any related security settings and use the Security profile in an access rule.

For more information, see:

- Manage Internet Security
- Add a Security Profile
- Enable or Disable Decryption

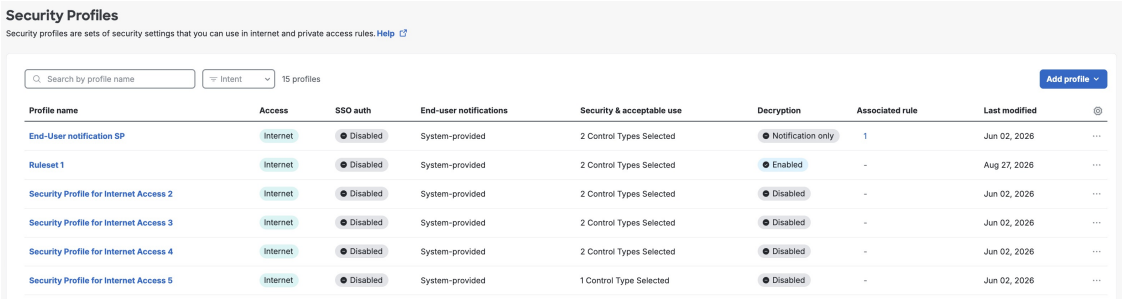
- SSO Authentication
- Security and Acceptable Use Controls
- Configure End-User Notifications

Add a Security Profile

Provides instructions for completing the Add a Security Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Security Profiles**.



2. Click **Add Profile**, and then select **Internet Access**.

Enable or Disable Decryption

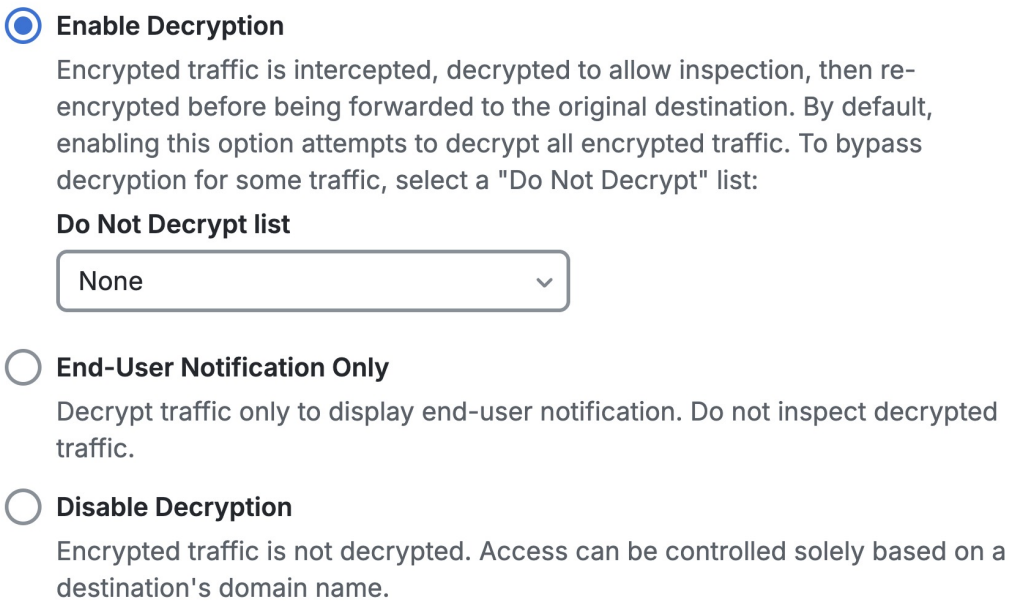
Provides instructions for completing the Enable or Disable Decryption workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Decryption**.
2. Choose a decryption option.

Note

Decryption is required for most security features to work properly. For more information about decryption, see Manage Traffic Decryption.



a. Click **Enable Decryption**

   Encrypted traffic is intercepted, decrypted to allow inspection, then re-encrypted before being forwarded to the original destination. By default, enabling this option attempts to decrypt all encrypted traffic. To bypass decryption for some traffic, select a **Do Not Decrypt** list.

b. Click **Enable Decryption for End-User Notification Only**.

   Decrypt traffic only to display end-user notification. Do not decrypt traffic for inspection.

   Note

   A root certificate is required in any situation in which the system must proxy and decrypt traffic intended for a website.

c. Click **Disable Decryption**.

   Encrypted traffic is not decrypted. Access can be controlled solely based on a destination's domain name.

3. Click **Save**.

What to do next

> **Note**
>
> If you enabled decryption, choose a **Do Not Decrypt** list. For more information, see Add a Do Not Decrypt List for Security Profiles.

SSO Authentication

Provides instructions for completing the SSO Authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

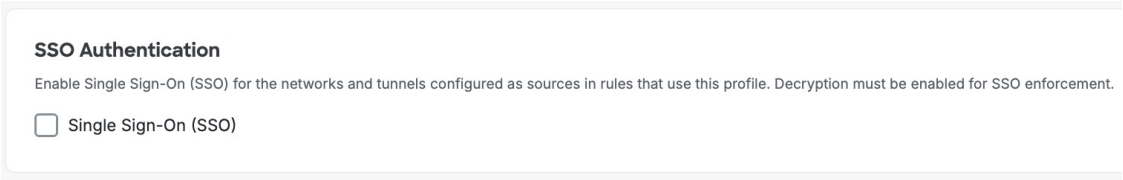
Enable or disable SSO Authentication. For information about the SSO authentication setting on the profile, see Security Profiles for Internet Access.

Procedure

---

1. Navigate to **SSO Authentication**.
2. Click **SSO enabled** to toggle the setting on.

> **Note**
>
> If you enable this option, ensure that decryption is enabled in the same security profile and in any rule in the Access policy that uses this profile.



3. Click **Save**.

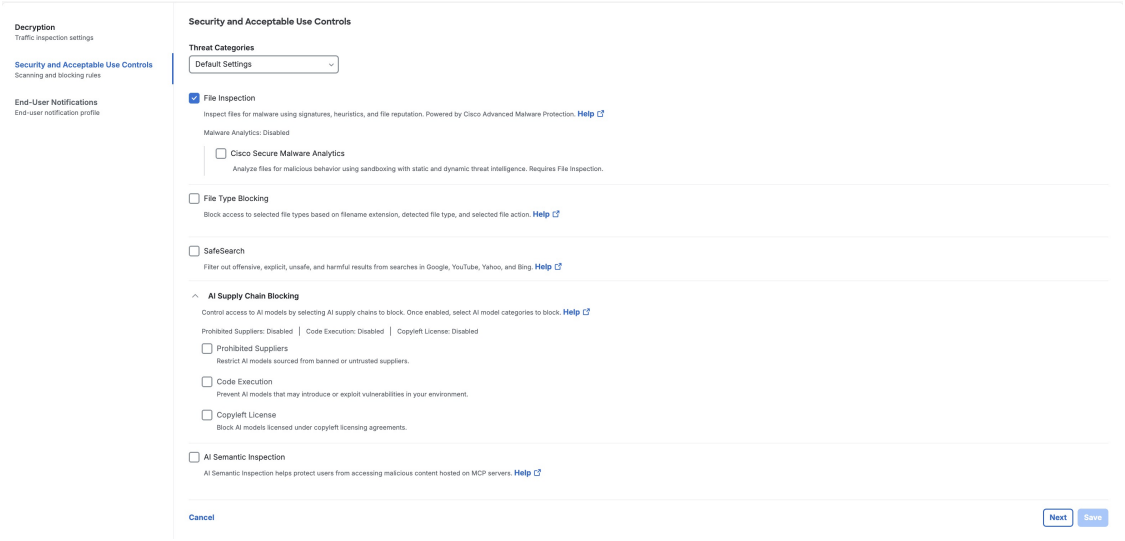
What to do next

> **Note**
>
> (Optional) Click **SSO disabled** to toggle the setting off.

Configure Security and Acceptable Use Controls

Describes Configure Security and Acceptable Use Controls in Cisco Secure Access. Configure security and acceptable use controls in the Security Profile.

Configure security and acceptable use controls in the Security Profile. Depending on your requirements, you can enable multiple kinds of scanning and blocking. For information about these settings, see Security Profiles for Internet Access.

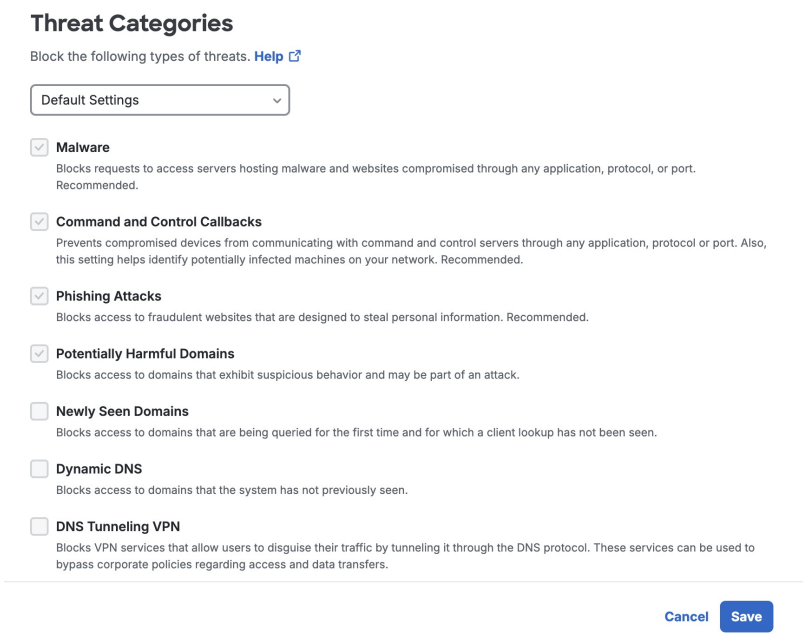


Threat Categories

Provides instructions for completing the Threat Categories workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Click the **Threat Categories** dropdown and expand your setting to open the dialog box.



2. To block access to known malicious sites and potentially risky sites based on threat category, choose from the existing lists of threat categories.
3. Click **Save**.

File Inspection

Provides instructions for completing the File Inspection workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

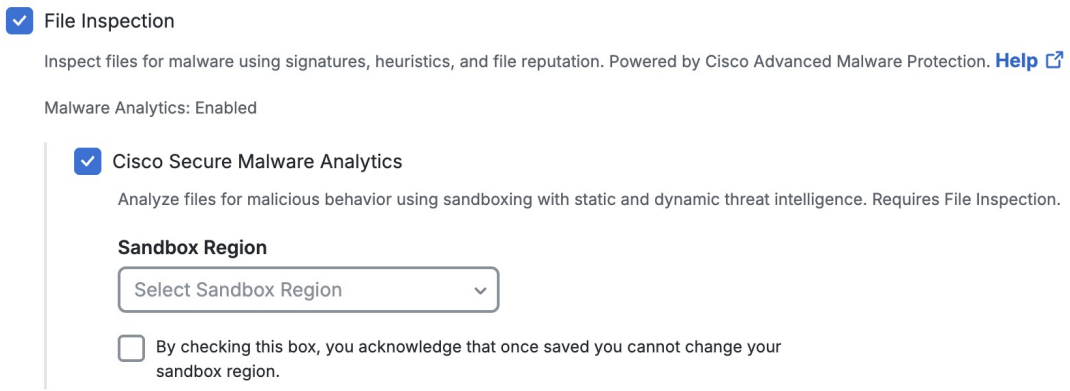
1. For **File inspection**, click **Edit**.
2. Choose the file inspection and analysis tools to use to protect traffic that matches rules that use this security profile.

   Important

   If this is the first time you enable Cisco Secure Malware Analytics, Secure Access displays the option to select a sandbox region. Before you enable Cisco Secure Malware Analytics, we recommend that you review the instructions about this option. For more information, see Enable File Analysis by Cisco Secure Malware Analytics.

   a. Click **File Inspection is Enabled**.

   b. (Optional) Click **Cisco Secure Malware Analytics is Enabled**.



3. Click **Save**.

File Type Blocking

Describes File Type Blocking in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

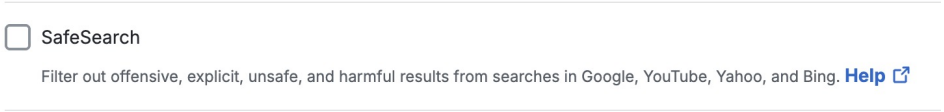
For more information, see Enable File Type Controls.

SafeSearch

Provides instructions for completing the SafeSearch workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Enable the **SafeSearch** to filter out offensive, explicit, unsafe, and harmful search results in Google, YouTube, Yahoo, and Bing.



2. Click **Save**.

AI Semantic Inspection

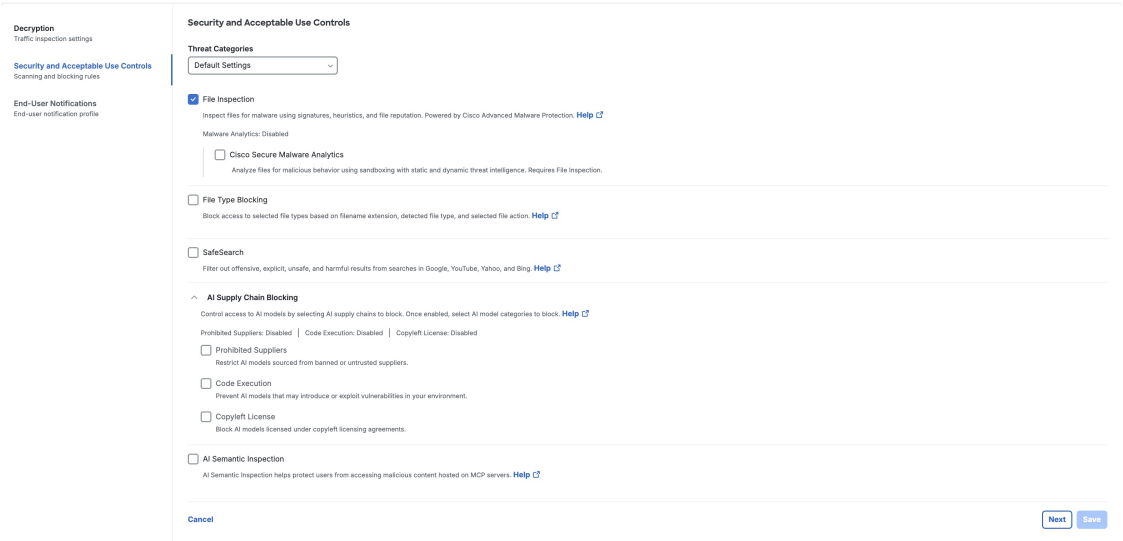
Provides instructions for completing the AI Semantic Inspection workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

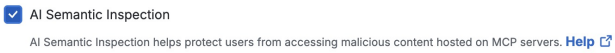
Ensure that Decryption is enabled for the profile.

Procedure

1. For **AI Semantic Inspection**, click **Edit**.



2. Enable this option to inspect the MCP traffic flowing through Secure Access.



3. Click **Save**.

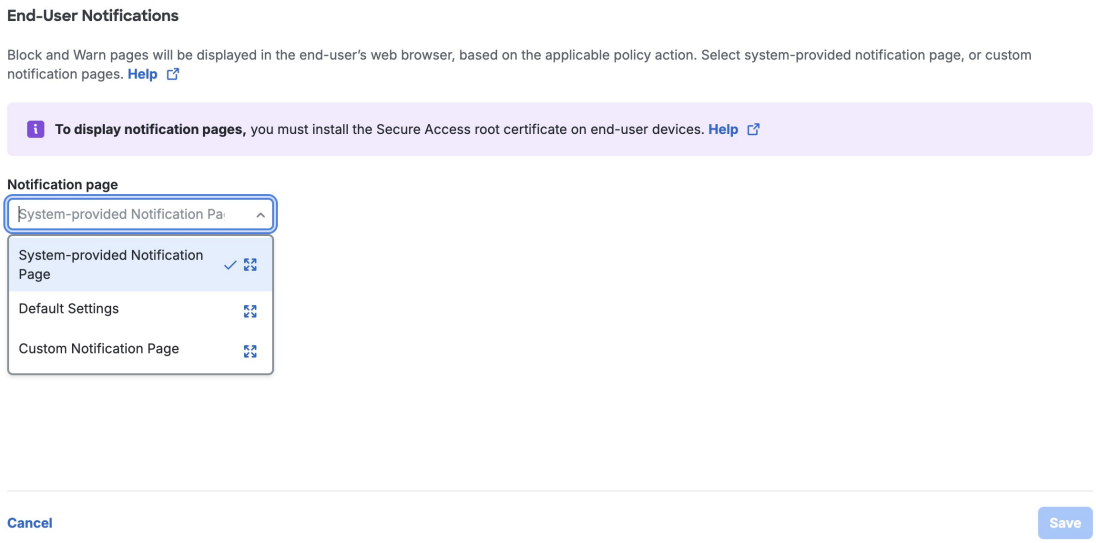
Configure End-User Notifications

Provides instructions for completing the Configure End-User Notifications workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure end-user notifications for the organization. Secure Access displays Block and Warn pages in the end-user's web browser. The display of the Block or Warn page is based on the action that you configure in each rule where the security profile is used. For more information, see Manage Notification Pages.

Procedure

1. Navigate to **Notification Pages**, and then click **Edit**.



2. Choose one of the options.

   Each option includes a Block notification and a Warn notification.

   a. Click **System-provided Notification Pages**.

   b. Click **Custom Notification Pages**.

   > **Note**
   >
   > For custom pages, choose the pages that you want to display.

3. (Optional) To preview the pages that you have selected, click the Preview links.



4. Click **Save**.

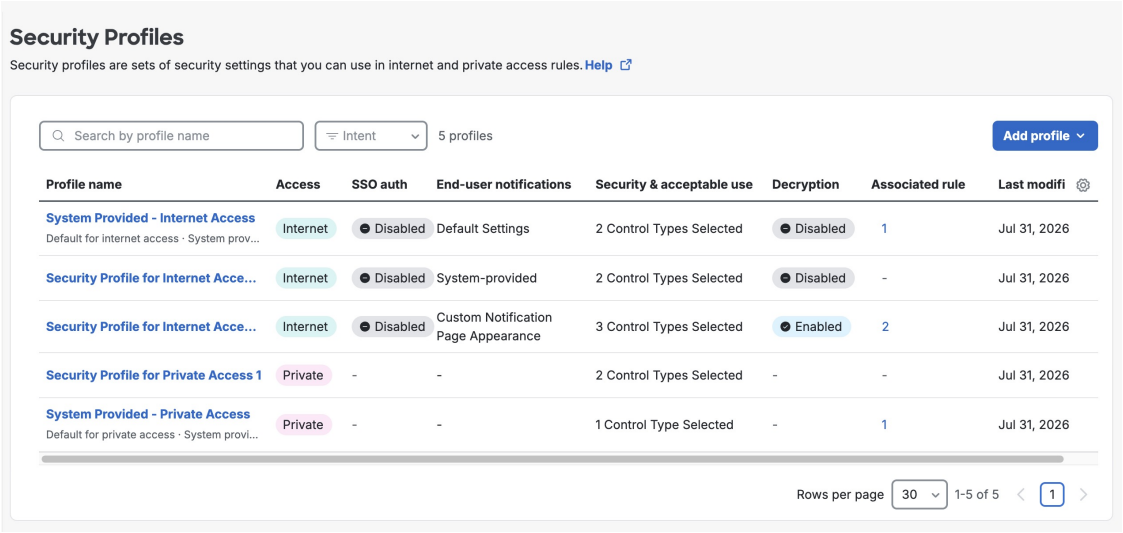
View Security Profiles

Provides instructions for completing the View Security Profiles workflow in Cisco Secure Access. View the configured security profiles in Secure Access.

View the configured security profiles in Secure Access.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Navigate to a security profile and expand the profile. A configured security profile includes these details:
   - Name of the security profile.
   - **Applied To**–The number access rules where the security profile is included.
   - **Access**–The type of the security profile.
   - **Decryption**–Specifies whether decryption is enabled on the profile.
   - **SSO Auth**–Specifies whether SSO authentication has been enabled on the profile.
   - **Security and Acceptable Use**–Lists the number of security controls that are enabled on the profile.
   - **End-User Notifications**–Lists the type of notifications that are configured on the profile.
   - **Last Modified**–The date when the security profile was last updated.



Configure Additional Security Options

Describes Configure Additional Security Options in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Configure additional functionality that is required for your selected features. For example, configure:

- **Traffic decryption** - Decryption requires certificates. For more information, see Certificates for Internet Decryption.
- **SSO authentication**- If you enable this option in a security profile, ensure that you configure SSO authentication.
  - For **SAML**, enable SAML for the Cisco Secure Client roaming security module. For more information, see Configure Integrations with SAML Identity Providers.
  - For **Open ID Connect (OIDC)**, see Configure Integrations with OIDC Identity Providers.
- **Notification pages** - To display notification pages, you must install a Secure Access root CA certificate on all end-user devices. This may not be the same certificate you use for decrypting internet traffic. For more information, see Certificates for Internet Decryption.

Add a Security Profile on Internet Access Rules

Describes Add a Security Profile on Internet Access Rules in Cisco Secure Access. Add the security profile to one or more internet access rules.

Add the security profile to one or more internet access rules. For more information, see Add an Internet Access Rule and Default Settings for Internet Access Rules.

Edit a Security Profile

Provides instructions for completing the Edit a Security Profile workflow in Cisco Secure Access. After you add a security profile in Secure Access, you can modify it.

After you add a security profile in Secure Access, you can modify it.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand a security profile, and then click **Edit**.
3. Choose any of the security controls and settings to modify. For more information, see:
   - Enable or Disable Decryption
   - SSO Authentication
   - Security and Acceptable Use Controls
   - Configure End-User Notifications

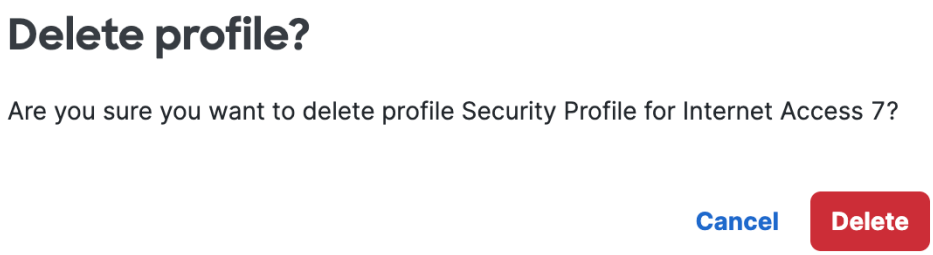
Delete a Security Profile

Provides instructions for completing the Delete a Security Profile workflow in Cisco Secure Access. After you add a security profile in Secure Access, you can remove it.

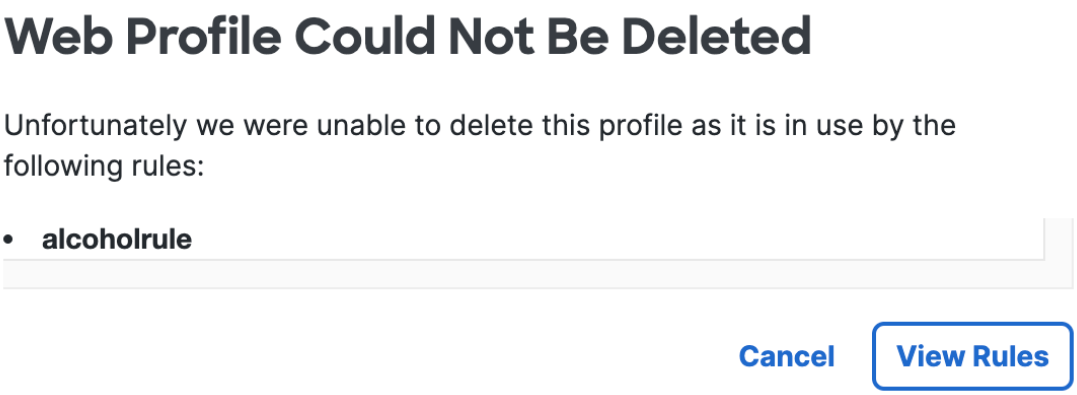
After you add a security profile in Secure Access, you can remove it.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand a security profile, and then click **Delete**.
3. Confirm the removal of the security profile.
   a. a. Click **Delete** to confirm the removal of the security profile.



   b. b. If the security profile is in use on an access rule, you can not remove the profile. First remove the security profile from the access rules where it is included, and the try to remove the security profile again.



Enable SafeSearch

Describes Enable SafeSearch in Cisco Secure Access. SafeSearch is a search engine filter for internet-bound traffic that blocks search results for explicit content such as pornography, violence, gore, and other offensive adult content.

SafeSearch is a search engine filter for internet-bound traffic that blocks search results for explicit content such as pornography, violence, gore, and other offensive adult content. When enabled, if an end user enters a potentially inappropriate or suggestive phrase into a search engine, the search engine only returns safe "family-friendly" results.

SafeSearch applies to Google, YouTube, Yahoo, and Bing. SafeSearch can not be disabled on an end-user device for any applicable search engine or site.

When you enable SafeSearch in a security profile, you must also enable decryption in the same security profile. For more information, see Manage Traffic Decryption.

To enable SafeSearch and decryption, see Add a Security Profile for Internet Access.

Confirm That SafeSearch is Working

Describes Confirm That SafeSearch is Working in Cisco Secure Access. The most reliable way to confirm that SafeSearch is enabled is to visit a search engine or site where SafeSearch settings are enforced.

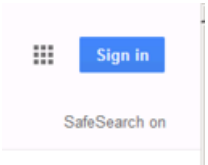
The most reliable way to confirm that SafeSearch is enabled is to visit a search engine or site where SafeSearch settings are enforced. You can also perform a search using a term that might be deemed inappropriate and review search results. Only "family friendly" results should be returned.

Tests must be done through a source that is included in an access rule that is configured to use a security profile in which SafeSearch is enabled.

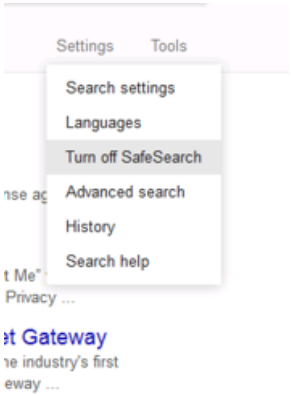
Google

Describes Google in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

After attempting a search in Google, a **SafeSearch on** indicator should be displayed.



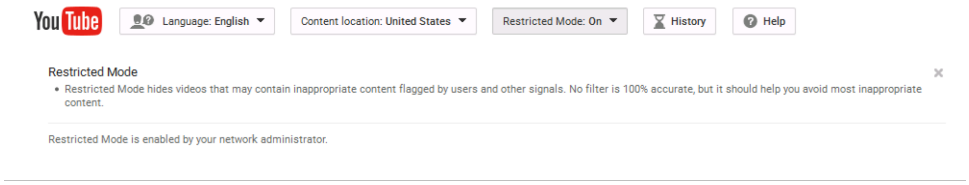
In the browser, under **Settings**, if you select **Turn off SafeSearch**, it has no effect and explicit sites are not listed in searches.



YouTube

Describes YouTube in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

Results when searching YouTube displays that “Restricted Mode” is "On". Expanding this result indicates that "Restricted Mode is enabled by your network administrator".

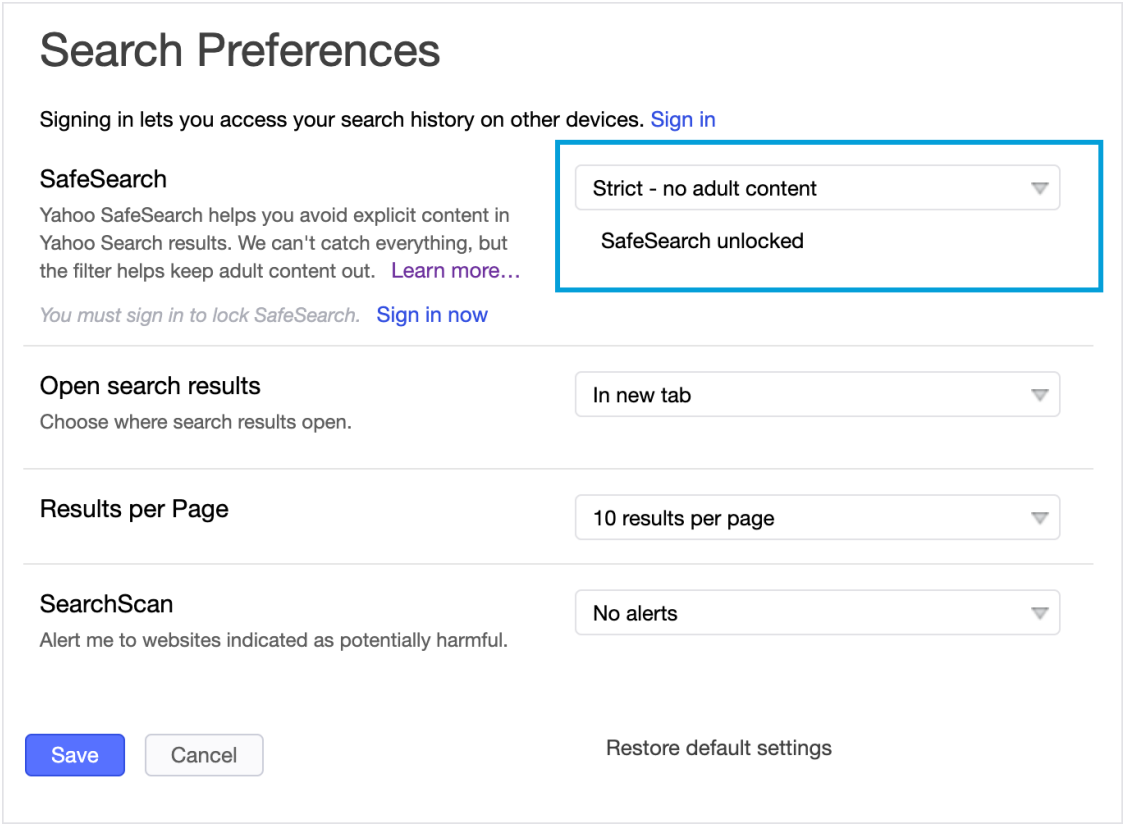


Yahoo

Describes Yahoo in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

From the Yahoo search page, click **Settings** and then **Preferences**.

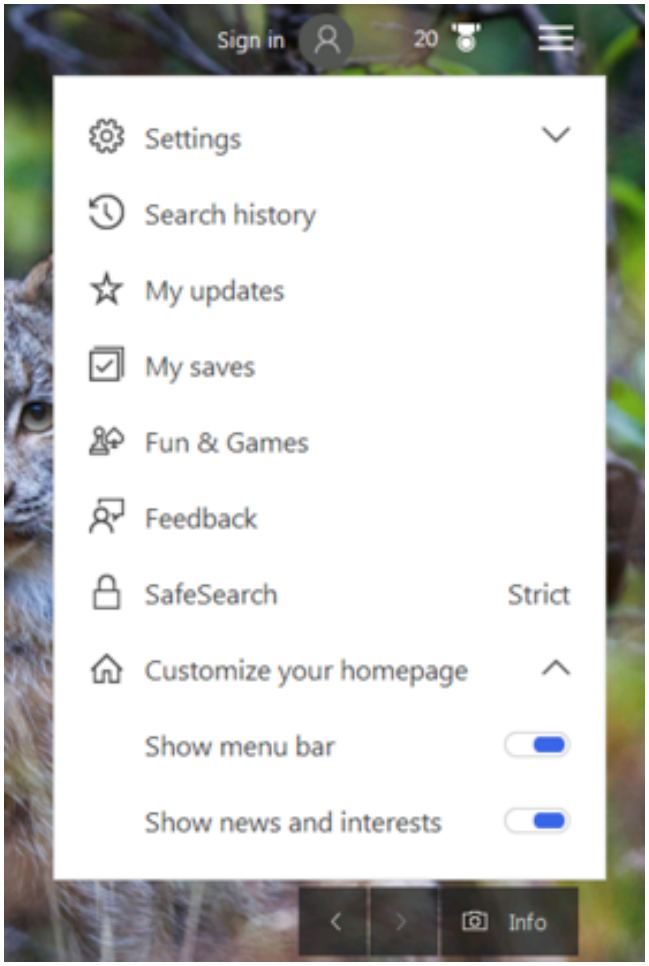
SafeSearch should be set to **Strict - no adult content**. You cannot change the setting.



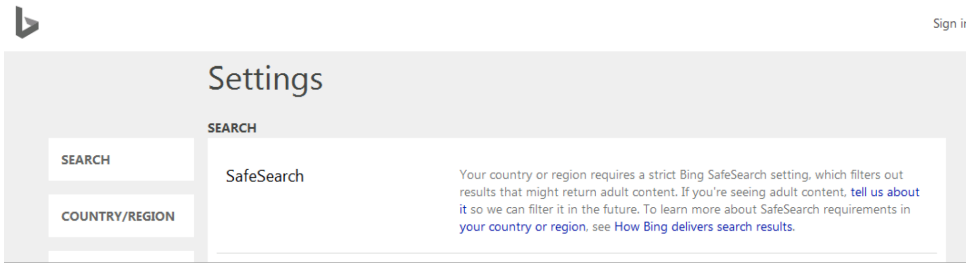
Bing

Describes Bing in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

From the menu icon, Bing displays that SafeSearch is set to “Strict”.



Clicking **SafeSearch** takes you to a page describing SafeSearch, but there is no disable option.



Security Profiles for Private Access

Describes Security Profiles for Private Access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

A security profile for private access rules lets you configure the following options to protect resources on your network from malicious files:

- File Inspection and File Type Blocking
- File Type Controls

To configure security profiles for private access, see Add a Security Profile for Private Access.

Security profile for private access blocks both downloading and uploading of file types selected in file type controls.

Add a Security Profile for Private Access

Provides instructions for completing the Add a Security Profile for Private Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

A security profile for private access rules lets you configure options to protect resources on your network from malicious files.

A security profile is a set of security controls and other settings that you can use in access rules. To add a security profile, navigate to **Secure** > **Security Profiles**.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- ⚠ **Caution**

  Certain initial settings affect all file analysis operations in your organization, for both private and internet traffic, and cannot be changed once configured. Be sure you understand these settings before you proceed. See Manage File Inspection and File Analysis.
- Understand the file-related options in the profile:
  - File Inspection and File Type Blocking
  - File Type Controls

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Click **Add Profile** > **Private Access**.
3. Configure file-related options.

What to do next

- Add the security profile to one or more private access rules.

32 App Risk Profiles

Topics:

- Manage App Risk Profiles

Provides an overview of App Risk Profiles in Cisco Secure Access, including Manage App Risk Profiles. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage App Risk Profiles

Describes Manage App Risk Profiles in Cisco Secure Access. App risk profiles define the level of risk you are willing to accept in controllable internet applications users access.

App risk profiles define the level of risk you are willing to accept in controllable internet applications users access. The risk level associated with a profile is determined by a set of risk attributes you select, joined by the OR or AND operator (which you also select).

Once you have defined an app risk profile, you can apply it in an Internet Access Rule. The controllable applications impacted by the rule will be restricted by the app risk profile attributes. So, for example, if you create a rule citing social networking applications as the destination, and apply an app risk profile that stipulates allowing only applications that are FedRamp compliant, then Secure Access will block social networking applications that are not FedRamp compliant.

Be aware that the effect of a risk profile on a given application may change as the characteristics of that application change. For instance, if an app risk profile is defined to block applications that do not comply with FedRamp, an application that is not FedRamp compliant will be blocked; but if that application becomes FedRamp compliant, Secure Access will recognize this and the app risk profile will no longer cause the application to be blocked. Similarly, if an app risk profile is defined to block applications with a particular value for Label Status or Application Risk Score, and you manually change the Label or Risk Score from the App Discovery Report, the app risk profile will no longer cause the application to be blocked.

App Risk Profile Attributes

Describes App Risk Profile Attributes in Cisco Secure Access. All app risk profile attributes are viewable in app details in the App Discovery Report.

All app risk profile attributes are viewable in app details in the App Discovery Report.

- Label Status

  The approval status of an app.

- Application Risk Score

  The application risk score could be calculated by Secure Access (based on Business risk, Usage risk, Vendor compliance, and Community risk (if available)) or assigned by you. The possible values are Very Low, Low, Medium, High, and Very High. The application risk score is displayed in the Third-Party Apps Report and the App Discovery Report.

- Business Risk Factors

  Business risks take into account factors such as usage type, web reputation, financial viability, and data storage risks.

- Attribute Categories

  Security attribute categories include compliance standards, vulnerabilities, data security attributes, email authenticity assurance techniques, access control methods, and audit features.

Add an App Risk Profile

Provides instructions for completing the Add an App Risk Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

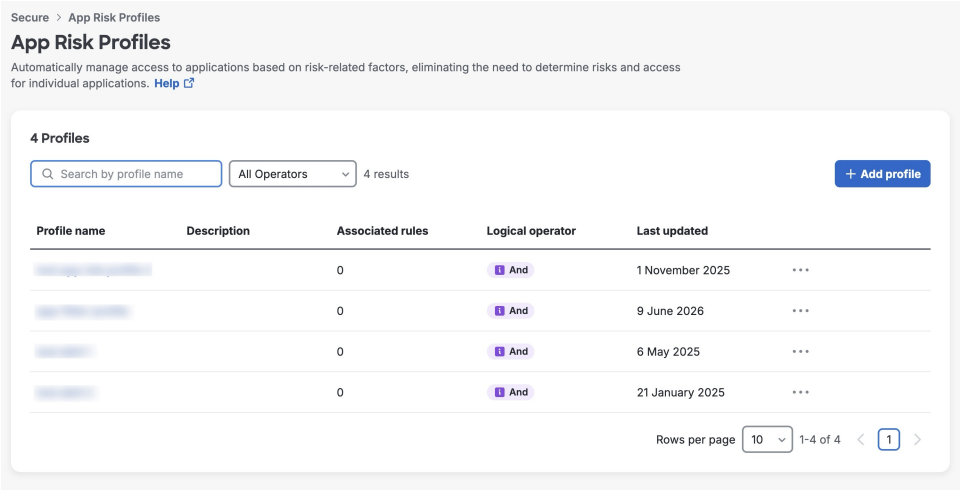
Configure an app risk profile to define acceptable risk factors for end-user devices connecting to controllable internet applications.

Before you begin

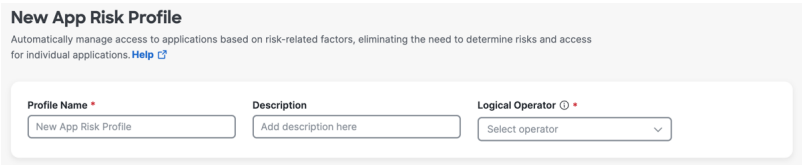
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

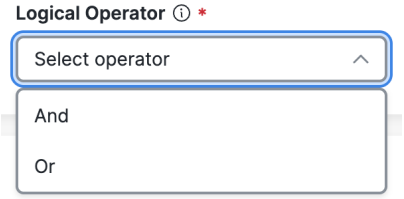
1. Navigate to **Secure > Profiles > App Risk Profiles** and click **Add profile**.



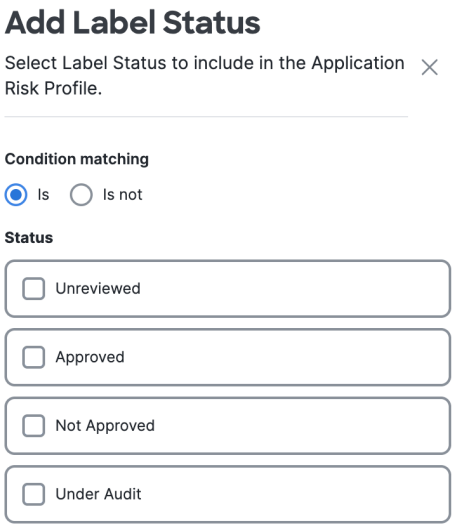
2. Give your profile a unique **Name** and a **Description**.



3. For the **Logic Operator** option, choose **And** or **Or** to indicate how the system will evaluate multiple attributes in the profile.



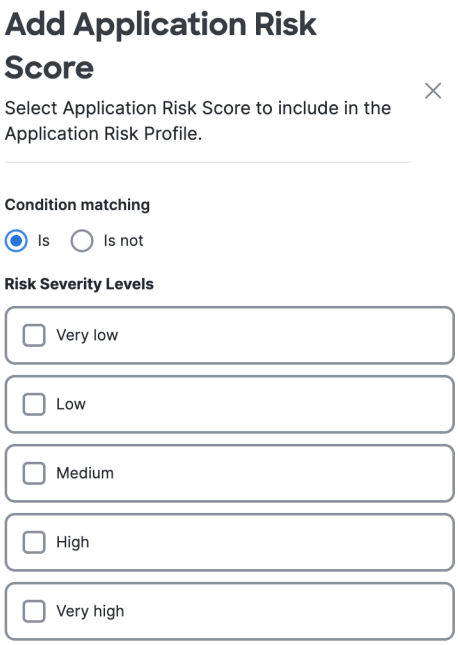
4. For **Label Status**, click **Add Label Status** and choose the matching conditions for an app's approval status from the App Discovery Report. Click **Save** when done.



5. For **Application Risk Score**, click **Add Application Risk Score** and choose application risk scores to include or exclude from the profile. Click **Save** when done.

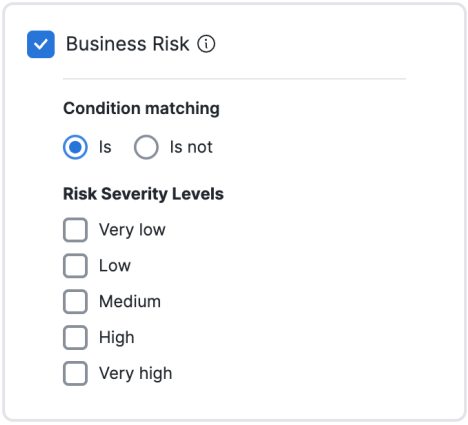
   The application risk score could be calculated by Secure Access (based on Business risk, Usage risk, Vendor compliance, and Community risk (if available)) or assigned by you.

   The possible values are Very Low, Low, Medium, High, and Very High.

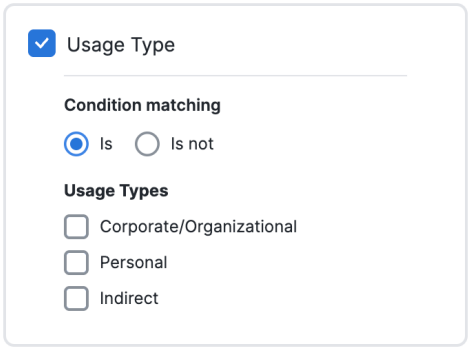


6. For **Business Risk Factors**, click **Add Business Risk Factors** and choose business risks from the following categories to include or exclude from the profile. Click **Save** when done.

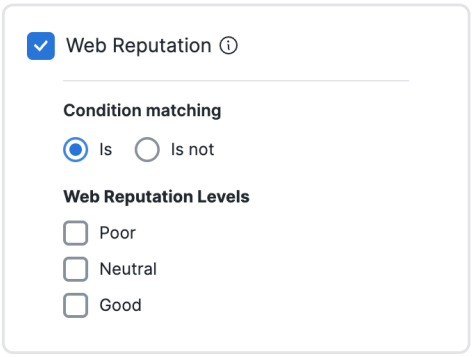
   - Business Risk



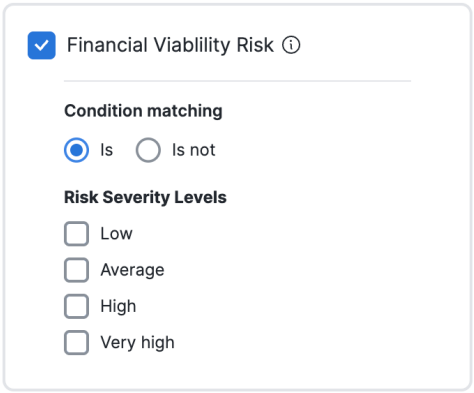
   - Usage Type



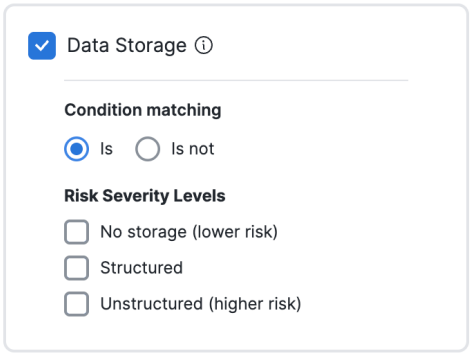
- Web Reputation



- Financial Viability Risk



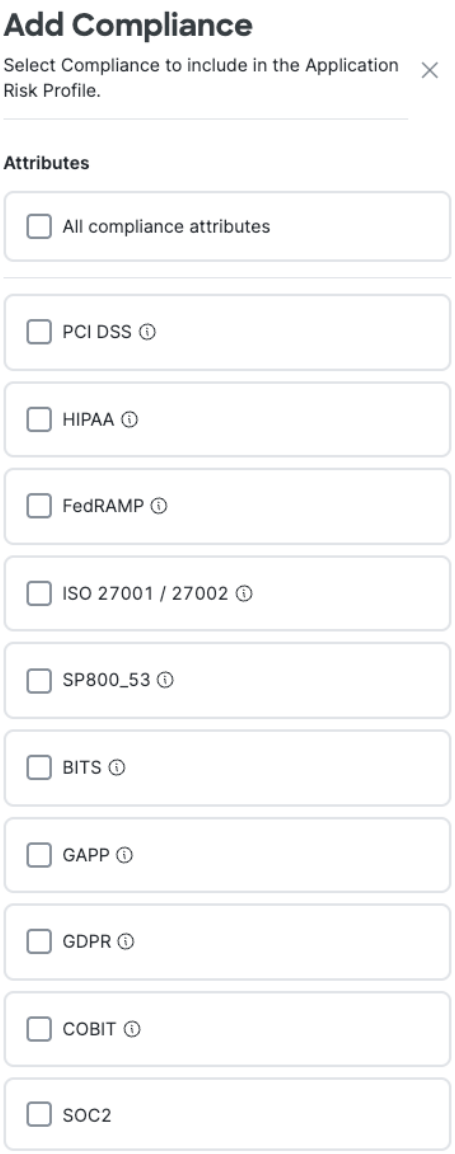
- Data Storage



7. For **Attribute Categories**, you can choose to add characteristics and properties from the following categories to add to your profile:

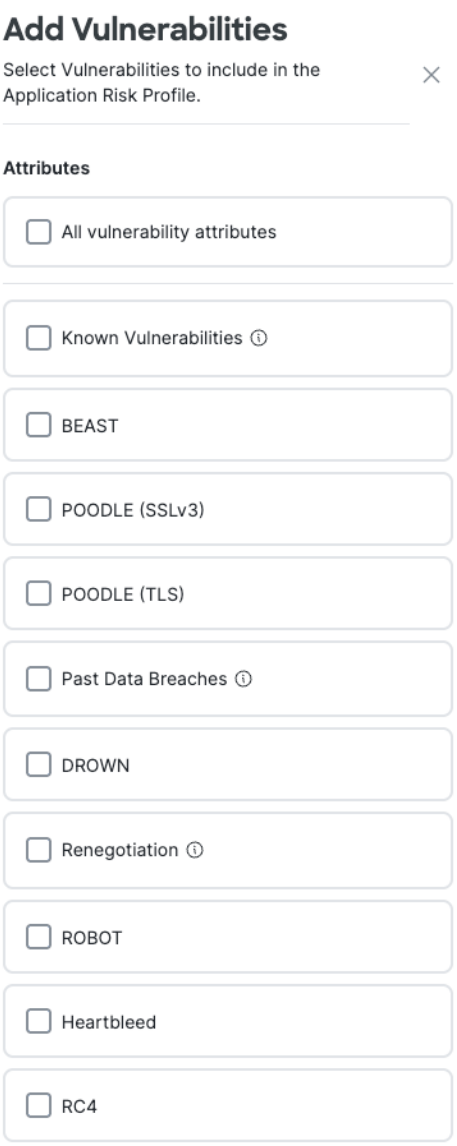
a) Click **Add Compliance** to select from a list of security standards with which an application must comply or standards with which an application need not comply.

You may select a specific security standard (such as FEDRAMP or COBIT), or all standards presented in the list.



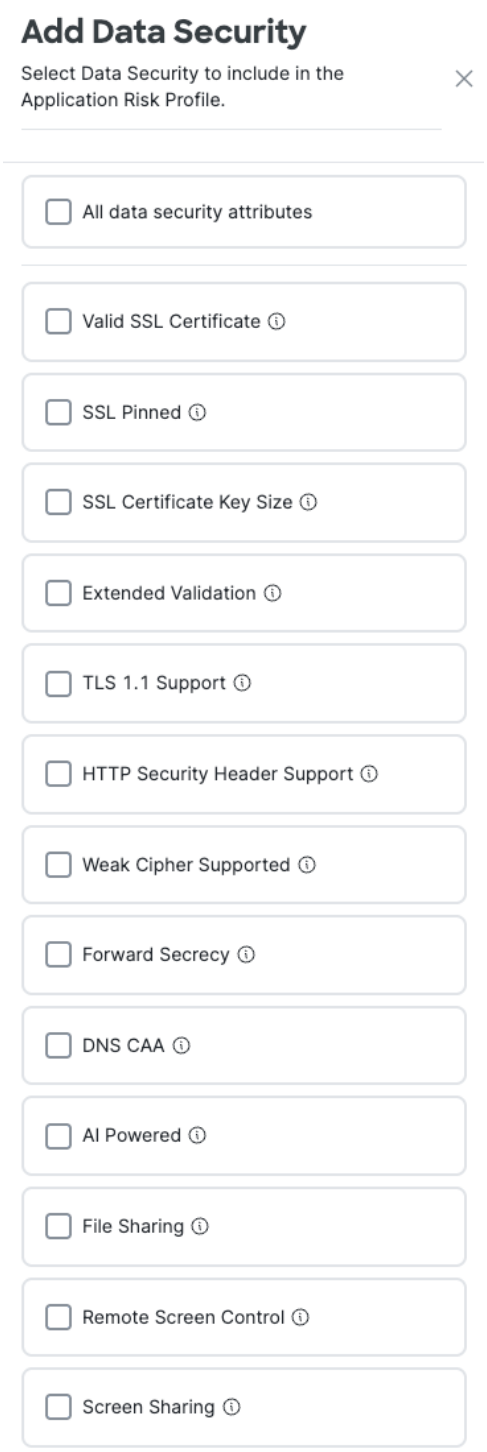
b) Click **Add Vulnerabilities** to select from list of vulnerabilities to which an application must be resistant or need not be resistant.

You may select a specific known vulnerability (such as DROWN or BEAST), or all known vulnerabilities.



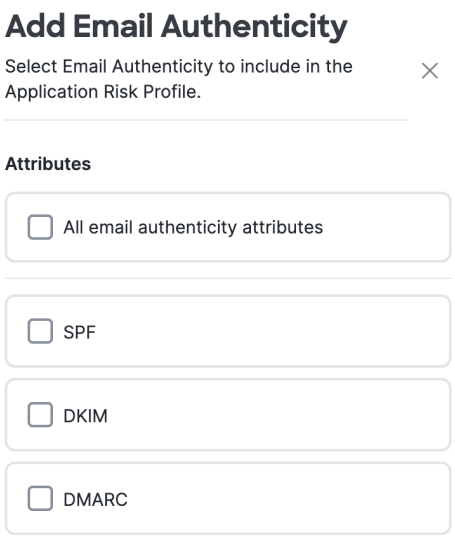
c) Click **Add Data Security** to select from a list of data security attributes an application must provide (such as HTTP Security Header Support) or exclude (such as weak ciphers).

You may select specific attributes or all attributes offered.



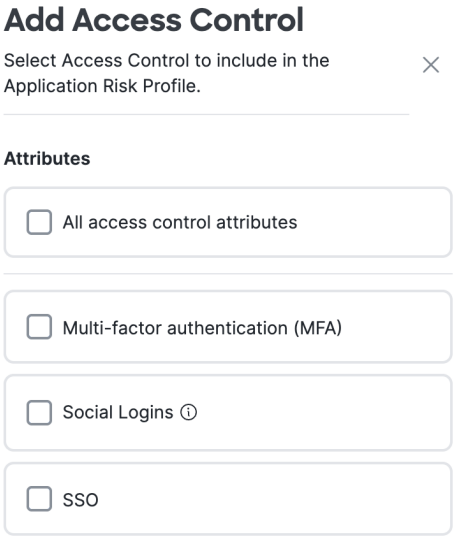
d) Click **Add Email Authenticity** to select from a list of email security attributes an application must support or exclude (DPF or DKIM).

You may select specific attributes or all attributes offered.

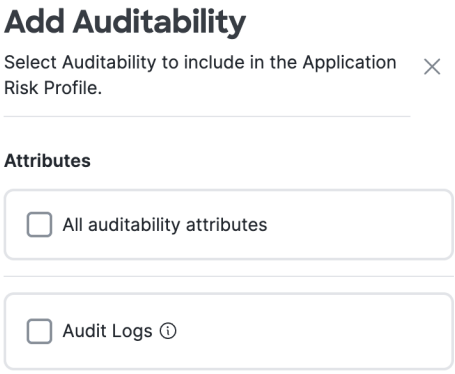


e) Click **Add Access Control** to select from a list of access methods an application must support or exclude (MFA or SSO).

You may select specific methods or all methods offered.



f) Click **Add Auditability** to select from a list of auditing features an application must support or exclude.



8. Click **Save** to save the app risk profile and make it available for use in Internet Access Rules.

33 Threat Categories

Topics:

- Manage Threat Categories

Provides an overview of Threat Categories in Cisco Secure Access, including Manage Threat Categories. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Threat Categories

Describes Manage Threat Categories in Cisco Secure Access. Secure Access groups harmful destinations into categories based on the type of threat they present, and allows you to control access to those destinations.

Secure Access groups harmful destinations into categories based on the type of threat they present, and allows you to control access to those destinations. You create lists of threat categories to block access to, then specify a threat category list in each security profile for internet access, then specify one of these security profiles in each internet access rule.

For a list of all threat categories and a description of each, see Threat Category Descriptions.

Default Threat Category List

A default threat category list ships with Secure Access. This default list is included in the default security profile for internet access and by default in all security profiles for internet access that you create.

You can change the enabled threat categories in the default list, and you can create different threat category lists to use in different security profiles.

The following threat categories are enabled in the threat categories list that is included by default in security profiles for internet access: Malware, Command Control Callbacks, and Phishing.

Reporting on Threat Category Access Attempts

When traffic is blocked based on one of these categories, Secure Access generates a reporting event.

If a domain matches a threat category but is not set to be blocked by a web security setting in the security profile selected for your rule, it is still reported as an allowed visit to a destination that matches one of the threat categories.

Threat Category Descriptions

Describes Threat Category Descriptions in Cisco Secure Access. Malware—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port.

- **Malware**—Blocks requests to access servers hosting malware and websites compromised through any application, protocol, or port. Recommended.
- **Command Control Callbacks**—Prevents compromised devices from communicating with command and control servers through any application, protocol or port. Also, this setting helps identify potentially infected machines on your network. Recommended.
- **Phishing Attacks**—Blocks access to fraudulent websites that are designed to steal personal information. Recommended.
- **Potentially Harmful Domains**—Blocks access to domains that exhibit suspicious behavior and may be part of an attack.
- **Newly Seen Domains**—Blocks access to domains that are being queried through Secure Access for the first time and for which Secure Access has not yet seen a client lookup. Not all new domains are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **Dynamic DNS**—Blocks access to sites that host dynamic DNS content. Not all sites in this category are necessarily harmful; blocking access to this category may block access to legitimate sites.
- **DNS Tunneling VPN**—Blocks VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These services can be used to bypass corporate policies regarding access and data transfers.
- **Cryptomining**—Blocks access to crypto mining pools where "miners" group together and share resources—processing power—to better gather and share cryptocurrencies. Also blocks known web crypto mining source code repositories.

Add a Threat Category List

Provides instructions for completing the Add a Threat Category List workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can create different threat category lists to use in different security profiles for internet access, which you can then use in different internet access rules.

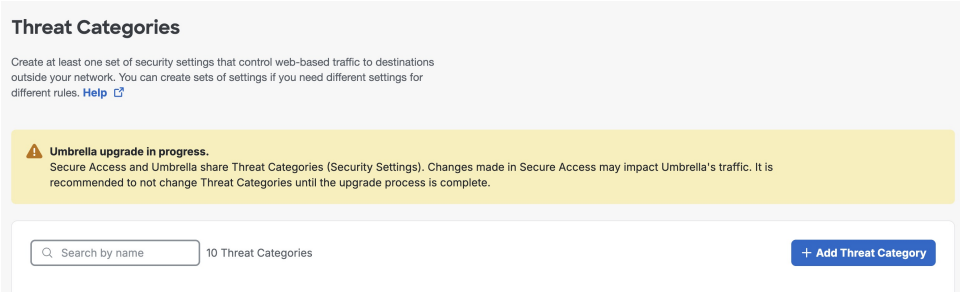
For example, you may want to block access to potentially risky sites for some users, even if this means potentially blocking access to legitimate sites, while for other users you may want to avoid blocking access to any legitimate sites even if it may expose them to risky sites.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

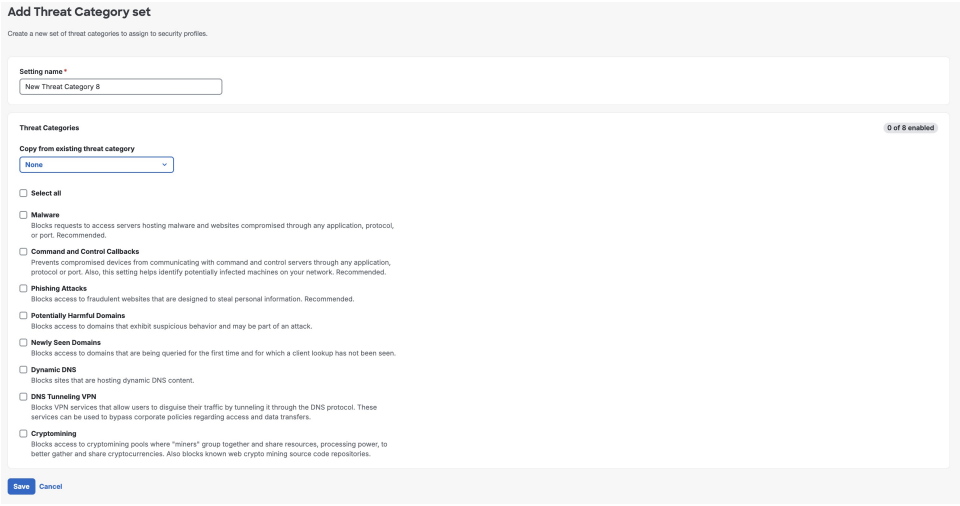
Procedure

1. Navigate to **Secure** > **Settings** > **Threat Categories** and click **Add Threat Category**.

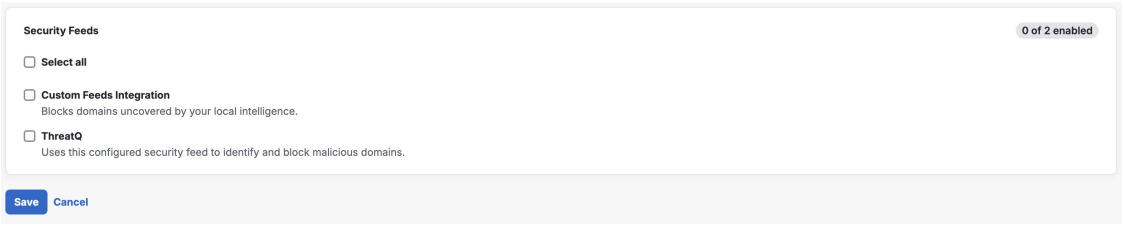


2. Give your setting a good descriptive **Setting Name**.
3. Select **Security Categories**.

   For more information about the categories, see Manage Threat Categories.



4. Select **Security Feeds**.



5. Click **Save**.

   This new threat category list is now available for selection when you Add a Security Profile for Internet Access.

Dispute a Threat Categorization

Provides instructions for completing the Dispute a Threat Categorization workflow in Cisco Secure Access. You must have credentials for your Cisco account.

When a destination is classified in a category which you disagree with, you can dispute the categorization. Secure Access and Cisco Talos share a unified set of threat categories. You can submit a category dispute request through Cisco Talos.

Before you begin

- You must have credentials for your Cisco account.

Procedure

---

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow instructions on the screen.

How to Dispute a Threat Categorization

Describes How to Dispute a Threat Categorization in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Prerequisites:

You must have credentials for your cisco.com account.

1. Navigate to talosintelligence.com.
2. Click **Support**.
3. Click **Content Categorization**.
4. Click **Cisco Login**.
5. Sign in with your cisco.com credentials.
6. Follow instructions on the screen.

34 Traffic Decryption

Topics:

- Manage Traffic Decryption

Provides an overview of Traffic Decryption in Cisco Secure Access, including Manage Traffic Decryption. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Traffic Decryption

Describes Manage Traffic Decryption in Cisco Secure Access and explains Decryption Requires Certificates, Decryption Logging, and Troubleshooting Decryption. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Decryption is used for various purposes in Secure Access. You can configure decryption on these components:

- **Security Profiles**–For more information, see Security profiles for Internet Access.
- **Do Not Decrypt List**–For more information, see Add a Do Not Decrypt List for Security Profiles and Internet Access.
- **Private Resources**–For more information, see Add a Private Resource.
- **Global Settings**– Several settings affect decryption for private or internet traffic or both. For more information, see Global Settings.

Decryption Requires Certificates

In most cases, decryption requires that you upload or install certificates. Intrusion Prevention (IPS) requires decryption in order to effectively evaluate threats in traffic.

For internet traffic, see Certificates for Internet Decryption.

For private resource destinations, see Manage Certificates for Private Resource Decryption.

Decryption Logging

You can enable or disable decryption logging in the Global Settings of the Access policy. For more information, see Edit Rule Defaults and Global Settings.

To view your decryption logs, see Reports.

Troubleshooting Decryption

If you suspect decryption is causing issues, check your decryption logs or temporarily disable decryption globally on the Global Settings page for the specified features. For more information, see Global Settings for Access Rules and Edit Rule Defaults and Global Settings.

Your issue may not be specifically related to decryption. For example, see Troubleshoot Private Access Rules and Troubleshoot Internet Access Rules.

Internet Access Features That Require Decryption

Describes Internet Access Features That Require Decryption in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The following features require decryption or do not work effectively on encrypted traffic:

- Intrusion prevention (IPS) for traffic to internet destinations.

  Traffic must be decrypted to inspect HTTPS traffic for known threats and behaviors.

- Security features configured in security profiles.

  Decryption is required for inspection by the security and acceptable use features. The security profile specified in any internet access rule should have decryption enabled, unless the destinations are trusted.

- File inspection and analysis and enforcement of file type controls.

See Manage File Inspection and File Analysis and Manage File Type Control.

- Destinations that are derived from SAML configurations
- Remote browser isolation (RBI).

  If you choose Isolate as the rule action in an internet access rule, affected traffic must be decrypted. Enable decryption in the security profile that you choose for that rule.

- Displaying block and warning notifications to end users

  When a destination triggers a warning page, users can only access that destination by clicking the link in the warning notification. See Manage Notification Pages for more information.

- Tenant Controls
- Advanced Application Controls.
- Data Loss Prevention

Sites that use HTTP rather than HTTPS do not require decryption to benefit from the functionality listed above. However, most sites use HTTPS. Enforcement based on threat categories never requires decryption.

Internet Traffic That Should Not Be Decrypted

Describes Internet Traffic That Should Not Be Decrypted in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Traffic that should not be decrypted	How to Configure, and More Information
Traffic to confidential internet destinations, based on laws, regulations, or policy	See Important Information About Do Not Decrypt Lists.
Sites with pinned certificates (for IPS)	See Global Settings for Access Rules.
Sites with pinned certificates (for other features)	N/A
Microsoft 365 applications	See Global Settings for Access Rules.
Trusted files	
Traffic from certain sources, such as printers or IoT devices, on which certificates cannot be installed	See the **Disable Decryption for Specific Sources** section in Global Settings for Access Rules.

Decryption in Private Access Rules

Describes Decryption in Private Access Rules in Cisco Secure Access. Decryption is required for effective Intrusion prevention (IPS), file inspection, and file type blocking.

Decryption is required for effective Intrusion prevention (IPS), file inspection, and file type blocking. Traffic must be decrypted in order to inspect it for known threats and behaviors.

Traffic to private resources will be decrypted only if decryption is enabled for that resource and the required certificate is present. Configure decryption for private resources when you configure the private resource. For more information, see Add a Private Resource.

> **Note**
>
> If you enter the configuration of the private destinations directly on the private access rules, traffic to these private destinations is not decrypted.

Important Information About Do Not Decrypt Lists

Describes Important Information About Do Not Decrypt Lists in Cisco Secure Access. Traffic that is not decrypted cannot be effectively inspected for threats.

Traffic that is not decrypted cannot be effectively inspected for threats.

However, in order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted. You can use Do Not Decrypt lists to specify these destinations.

Do Not Decrypt lists apply only to destinations in internet access rules, and they are used for intrusion prevention (IPS) and for features configured in security profiles.

Currently, IPS profiles and security profiles support Do Not Decrypt lists differently:

- All IPS profiles use a single Do Not Decrypt list.
- Each security profile for internet access can use any Do Not Decrypt list.
- The types of destinations that you can specify for IPS and for a security profile are different. See the applicable sections below.

Do Not Decrypt List for IPS

Destinations on the system-provided Do Not Decrypt list are not decrypted for inspection by the intrusion prevention (IPS) feature.

All IPS profiles use the system-provided Do Not Decrypt list that ships with Secure Access. You can add destinations to this list.

To configure this list, navigate to **Secure** > **Settings** > **Do Not Decrypt Lists**.

> **Note**
>
> Do not use the system-provided Do Not Decrypt list for private destinations. Instead, you can configure a private resource and not enable decryption for that resource. See Add Private Resources.

Do Not Decrypt Lists for Security Profiles for Internet Access

When a Do Not Decrypt list is associated with a security profile for internet access, destinations on the list will not be decrypted by the security and acceptable use features enabled in that profile.

Initially, the default Do Not Decrypt List for security profiles is the same system-provided Do Not Decrypt List that is used for IPS. You can either use this single list for both IPS and security profiles for internet access, or you can create additional do-not-decrypt lists for use in security profiles for internet access. See Add a Do Not Decrypt List for Security Profiles for Internet Access.

Differences Between IPS and Features in Security Profiles

The types of destinations that you can choose not to decrypt is different for IPS and features configured in security profiles for internet access:

	Applications	Sites that belong to specified Content Categories	Domains
IPS	No	Yes	Yes
Features in Security Profiles	Yes	Yes	Yes

The System-Provided Do Not Decrypt List

The system-provided Do Not Decrypt list is the only list used by the IPS feature. The same list is the default list used by the features in the security profile for internet access. The system-provided Do Not Decrypt list does not include the ability to specify applications; this option is available only in custom lists.

Initially, this list is empty. Add the destinations that are important to your organization.

Limitation: Do Not Decrypt Based on Content Category

While web site categorization is updated continuously, it is not possible to categorize all web sites on the internet, and some sites may be categorized incorrectly. Therefore, if you choose not to decrypt traffic based on content category, it is possible that traffic to sites that should not be decrypted may be decrypted, and traffic that should be decrypted may not be decrypted.

This limitation is not unique to Cisco.

Add a Do Not Decrypt List for Security Profiles and Internet Access

Provides instructions for completing the Add a Do Not Decrypt List for Security Profiles and Internet Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In order to comply with the local confidentiality you can exclude specific traffic from decryption.

Create a custom Do Not Decrypt list to specify destinations that will not be decrypted by the security and acceptable use features configured in a security profile for internet access. HTTPS traffic to these destinations cannot be properly inspected for threats when traffic is not decrypted.

If you need to specify a Do Not Decrypt address for IPS profiles, edit the system-provided Do Not Decrypt List.

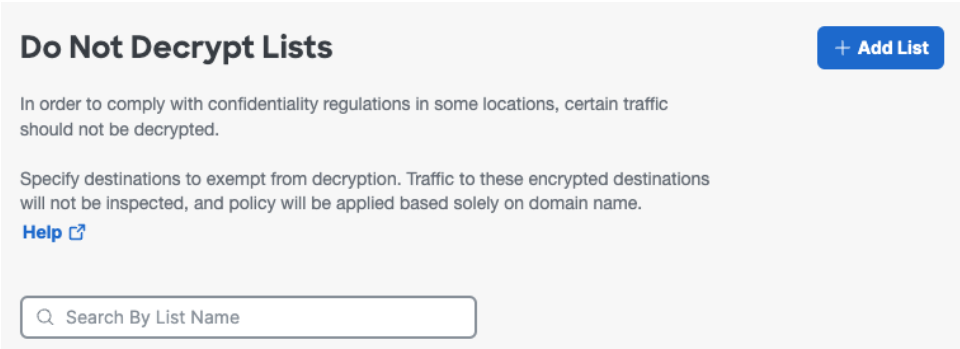
> **Note**
>
> To exclude all applications that use Google APIs from decryption, select **Google APIs** from the application list and add the domain **googleapis.com** to the list of domains.

Before you begin

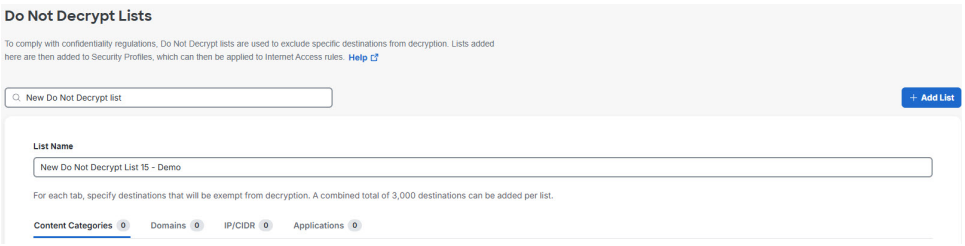
- Full Admin user role. For more information, see Manage Accounts.

Procedure

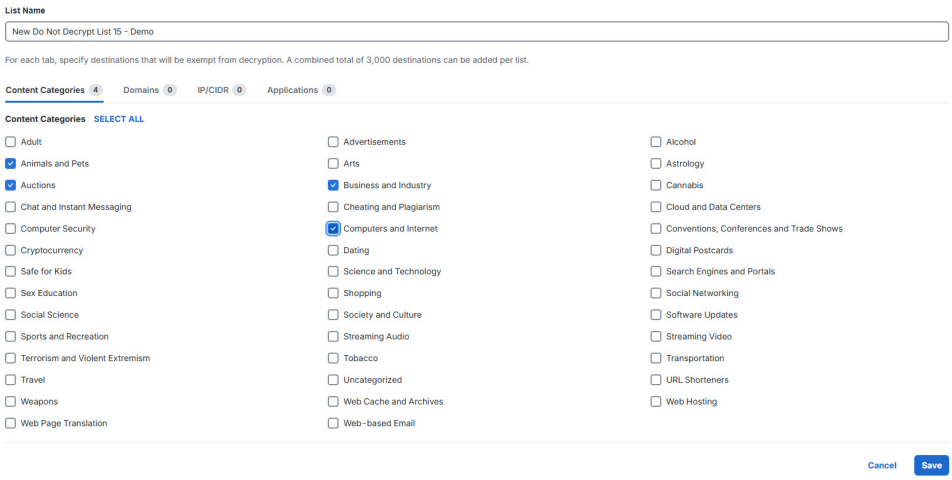
1. Navigate to **Secure** > **Settings** > **Do Not Decrypt Lists** and click **+ Add List**.



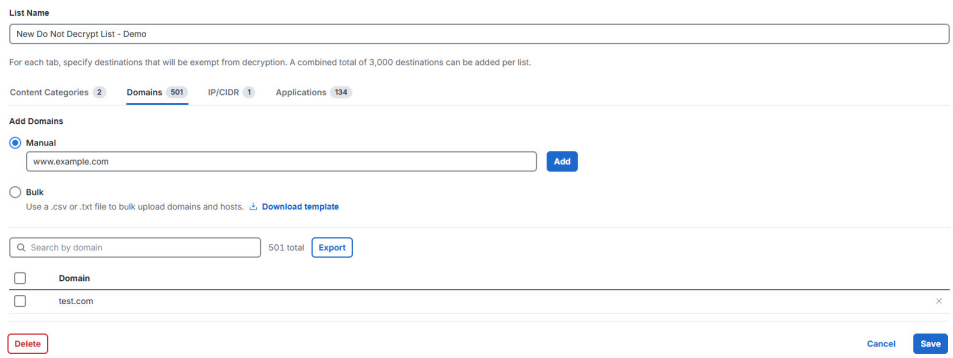
2. Enter a descriptive name for your list in the **List Name** field.



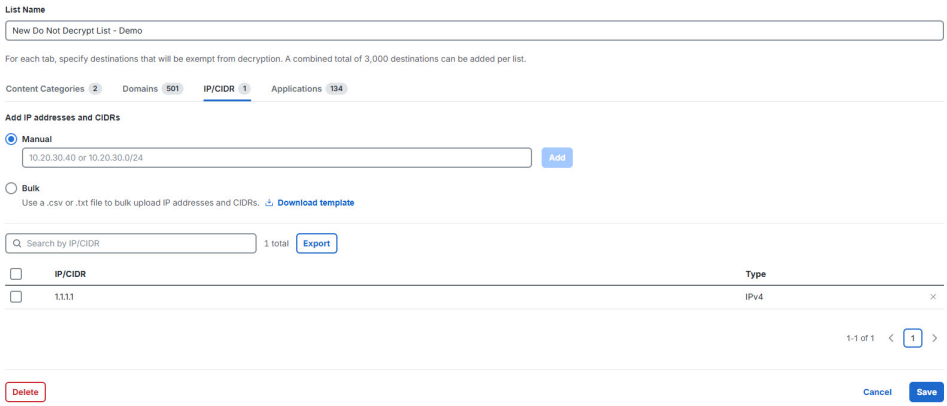
3. Add content categories, applications, and domains that will be exempt from decryption.
   a) Under **Content Categories**, check one or more **Content Categories** checkbox to exempt from HTTPS inspection, then click **Save**.



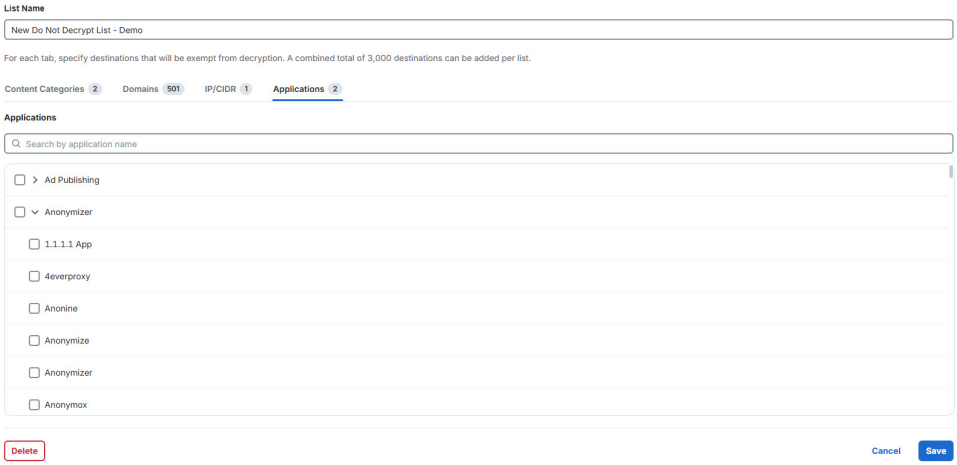
   b) Under **Domains**, to add multiple domains manually, click the **Manual** radio button, enter the doamin, then click **Add** to exempt domain from HTTPS inspection, and then click **Save**. Optionally, to upload multiple domains and hosts in bulk, click the **Bulk** radio button, upload the list in a .csv or .txt file, and then click **Save**.



c) Under **IP/CIDR**, to add multiple IP addresses and CIDRs manually, click the **Manual** radio button, enter the IP address and CIDR, then click **Add** to exempt IP addresses and CIDRs from HTTPS inspection, and then click **Save**. Optionally, to upload multiple IP addresses and CIDRs in bulk, click the **Bulk** radio button, upload the list in a .csv or .txt file, and then click **Save**.



d) Under **Applications**, check one or more **Applications** checkbox to exempt from HTTPS inspection, and then click **Save**.



> **Note**
>
> When you create a new list, add entries manually one at a time. After you save the list, the **Bulk** add domain option becomes available for the **Domain** and **IP/CIDR** sections. You can add a combined total of two thousand destinations per list globally across all sections.

After you add your custom Do Not Decrypt List, you can select the Do Not Decrypt List in a security profile for internet access.

4. Click **Save**.

After you add your custom Do Not Decrypt List, you can select the Do Not Decrypt List in a security profile for internet access.

35 Schedules for Access Rules

Topics:

- Manage Schedules

Provides an overview of Schedules for Access Rules in Cisco Secure Access, including Manage Schedules. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Schedules

Describes Manage Schedules in Cisco Secure Access. In Cisco Secure Access, you can configure Schedule resources to manage the enablement of internet or private access rules in the Access policy.

In Cisco Secure Access, you can configure Schedule resources to manage the enablement of internet or private access rules in the Access policy. A Schedule resource includes a time zone, start and end dates, and time periods in specific days of the week. Secure Access supports an unlimited number of Schedule resources in an organization.

After you add a Schedule resource in Secure Access, enable the **Schedule Enablement Time and Date** setting on an access rule and include the Schedule resource on the rule. For information about enabling Schedules on access rules, see Add an Internet Access Rule and Add a Private Access Rule.

About Configuring Schedule Resources

A Schedule resource requires multiple time-based configuration settings to manage the enablement of an access rule. Secure Access combines these settings together in the Schedule resource:

- The time zone for the selected dates and times.
- The start and end dates selected on a days of the month calendar.
  - Choose the start date when Secure Access enables the access rule.
  - Choose the end date when Secure Access disables the access rule.
- The start and end times during the 24-hour time period when Secure Access enables the access rule on the selected days of the week.
  - Choose the days of the week when Secure Access enables the access rule.
  - Choose the AM or PM hour in the 24-hour time period for the selected days of the week.

Guidelines for Creating Schedules

- You can include a Schedule on an internet or private access rule.
- You do not have to enable an access rule to add the **Schedule Enablement Time and Date** setting and select the Schedule on the access rule.
- If Secure Access enables an access rule with a Schedule and the Schedule expires, Secure Access disables the Schedule and the access rule in the Access policy.
- After you include a Schedule on an access rule, Secure Access manages the enablement of the access rule according to the dates and times configured in the Schedule.

Get Started with Schedules

1. Add a Schedule resource in the organization. For more information, see Add a Schedule.
2. Enable the **Schedule Enablement Time and Date** setting and select a Schedule on an access rule. For more information, see Schedule Enablement Time and Date.
3. View and manage Schedules. For more information, see View and Manage Schedules.

Add a Schedule

Provides instructions for completing the Add a Schedule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Cisco Secure Access, you can configure and add Schedule resources to your organization. A Schedule includes a time zone, start and end dates, and time periods on the selected days of the week. For more information, see About Configuring Schedule Resources.

Once you add the Schedule resource, enable the **Schedule Enablement Time and Date** setting on any internet or private access rules in the Access policy and select the Schedule on the access rule. Secure Access applies and enforces the settings in the access rule during the dates and times configured in the Schedule.

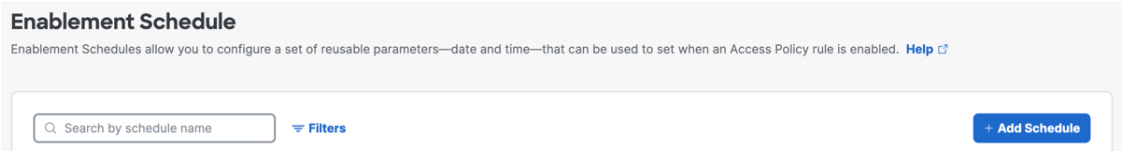
Configure the Schedule with the time zone, start and end dates, and days of the week with the time period for each day.

Before you begin

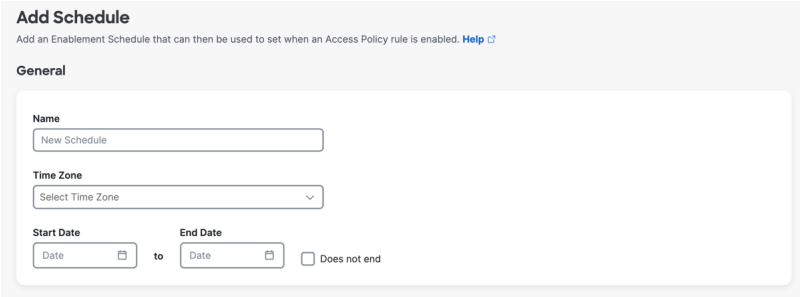
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Settings** > **Enablement Schedule**.
2. Click **Add Schedule**.

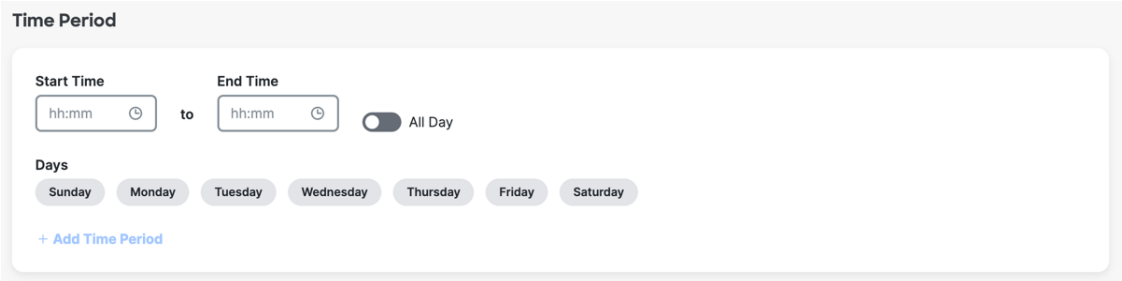


3. On **Add Schedule**, navigate to **General**.

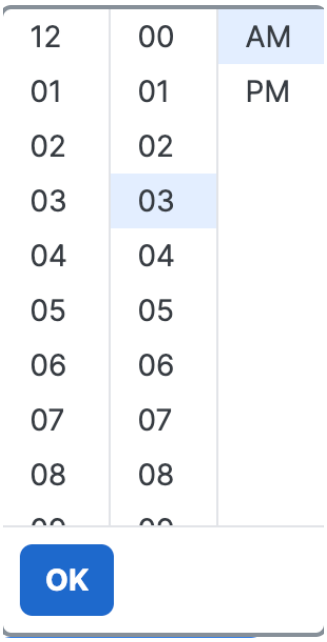


   - (Required) For **Name**, enter a unique name for the Schedule.
   - (Required) For **Time Zone**, choose the time zone that Secure Access will apply to the date and time configured in the Schedule.
   - (Required) For **Start Date**, choose the date when Secure Access will enable the access rule.
   - (Required) For **End Date**, choose the date when Secure Access will disable the access rule, or click **Does not end** to indicate that the Schedule does not expire and the access rule will remain enabled indefinitely.

4. Navigate to **Time Period**.

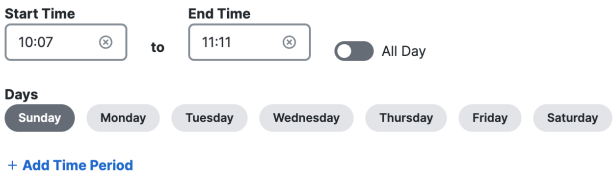


5. Choose the time of day for the schedule or enable **All Day**.
   a) (Required) For **Start Time**, choose the hour, minute, and **AM** or **PM** for the 24-hour time period when Secure Access will enable the access rule, and then click **OK**.

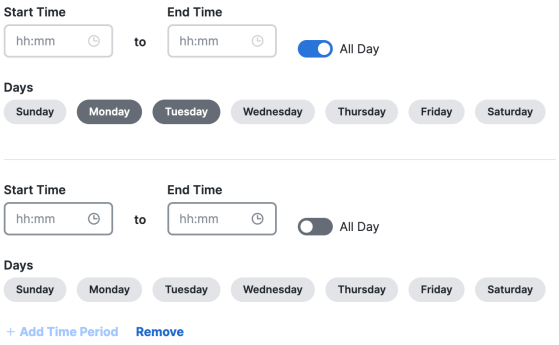


b) (Required) For **End Time**, choose the hour, minute, and **AM** or **PM** for the 24-hour time period when Secure Access will disable the access rule, and then click **OK**.

c) (Required) For **Days**, click on the days of the week when Secure Access will enable the access rule.



d) (Optional) Click **Add Time Period** to create another time period for the Schedule. (Optional) Repeat Steps 8-10 to add another time period to the Schedule.



e) (Optional) Click **Remove** to delete a configured time period.

6. Click **Save**.

View and Manage Schedules

Describes View and Manage Schedules in Cisco Secure Access. After you add a Schedule resource in Cisco Secure Access, you can include the Schedule on an internet or private access rule.

After you add a Schedule resource in Cisco Secure Access, you can include the Schedule on an internet or private access rule. You can also view, edit, or delete the Schedule. A Schedule configures the time zone, date and time ranges, and

days of the week when Secure Access enables the access rule. For more information, see About Configuring Schedule Resources.

To begin to use the Schedule resource, enable the **Schedule Enablement Time and Date** setting and select the Schedule resource on an access rule. For more information, see Schedule Enablement Time and Date.

View Schedules in Secure Access

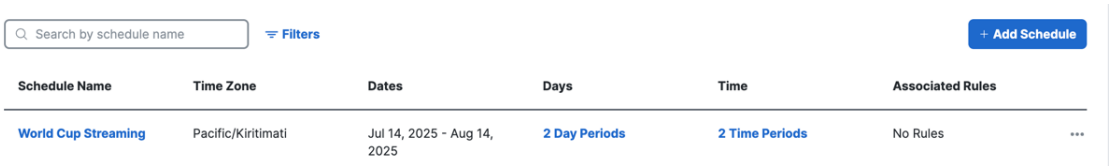
Provides instructions for completing the View Schedules in Secure Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

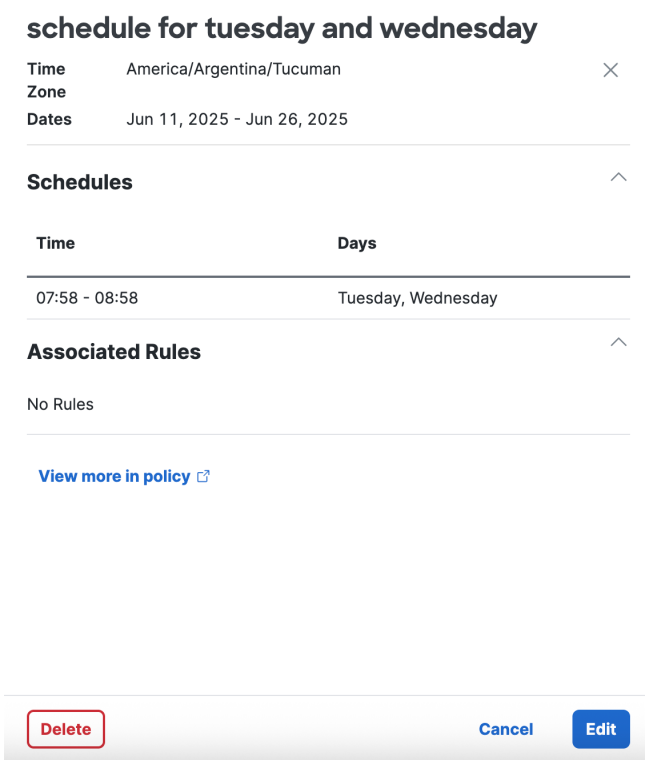
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Resources** > **Settings** > **Enablement Schedule**.



2. Navigate to a Schedule.
   - **Schedule Name**–The name of the Schedule.
   - **Time Zone**–The time zone applied to the date and time ranges configured in the Schedule.
   - **Dates**–The range of dates when Secure Access applies the Schedule.
   - **Days**–The days of the week when Secure Access applies the Schedule.
   - **Time**–The configured time periods for the selected days of the week when Secure Access applies the Schedule.
   - **Associated Rules**–The list of of the access rules that include the Schedule or **No Rules** if the Schedule is not included in any access rules.
3. (Optional) Click on the name of a Schedule to view the configured times, time zone, and the access rules that include the Schedule.
   a. General Schedule information.
      - **Schedule Name**–The name of the Schedule. The name is unique for the Schedules in the organization.
      - **Time Zone**–The time zone where the traffic occurs.
      - **Dates**–The range of dates when Secure Access applies the Schedule.
   b. Time and days Schedule information.
      - **Time**–The list of configured time periods when Secure Access applies the Schedule.
      - **Days**–The specific days of the week when Secure Access applies the Schedule.
   c. **Associated Rules**–The list of of the access rules where Secure Access applies the Schedule.
      - Click **View more in Policy** to navigate to the Access Policy in Secure Access.



Edit a Schedule

Provides instructions for completing the Edit a Schedule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

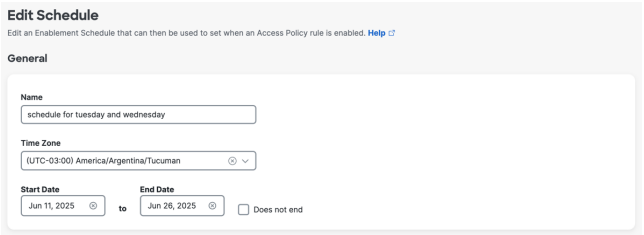
Edit a Schedule in Secure Access.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

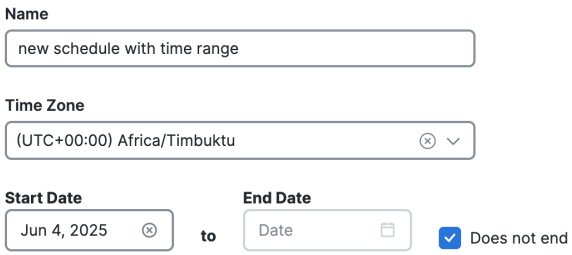
Procedure

1. Navigate to **Resources** > **Settings** > **Enablement Schedule**.
2. Navigate to the **Enablement Schedules** table.
   a) Navigate to a Schedule in the table, click on the ellipsis (**...**), and then choose **Edit**.
   b) Navigate to the **Schedule Name** column, click on the name of a Schedule, and then click **Edit**.
3. On **Edit Schedule**, navigate to **General**.



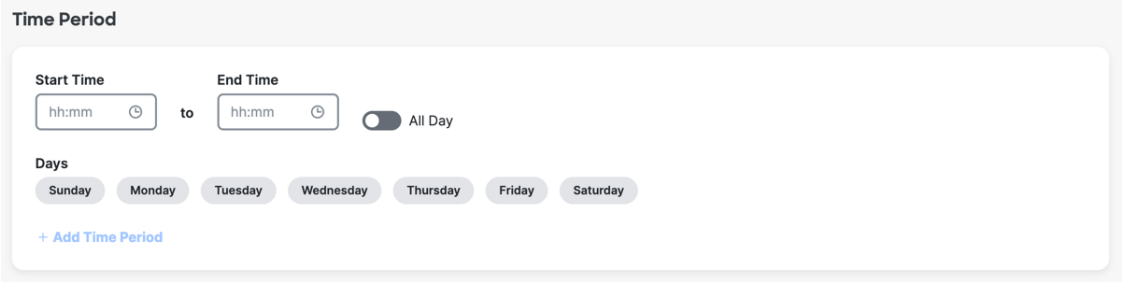
   - (Required) For **Name**, enter a unique name for the Schedule.

- (Required) For **Time Zone**, choose the time zone that Secure Access will apply to the date and time configured in the Schedule.
- (Required) For **Start Date**, choose the date when Secure Access will enable the access rule.

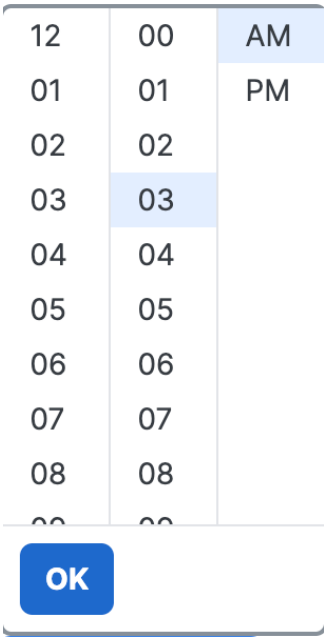


- (Required) For **End Date**, choose the date when Secure Access will disable the access rule, or click **Does not end** to indicate that the Schedule does not expire and the access rule will remain enabled indefinitely.

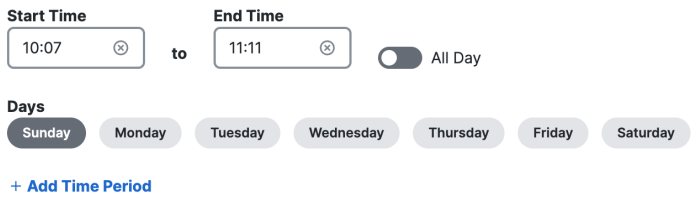
4. Navigate to **Time Period**.



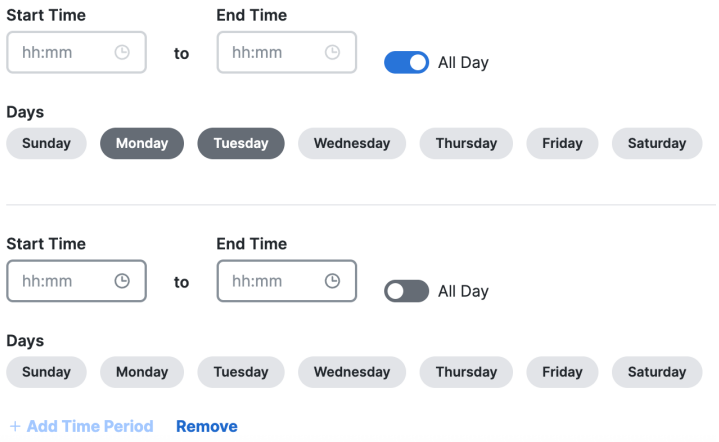
5. Choose the time of day for the schedule or enable **All Day**.
   a) (Required) For **Start Time**, choose the hour, minute, and **AM** or **PM** for the 24-hour time period when Secure Access will enable the access rule, and then click **OK**.



   b) (Required) For **End Time**, choose the hour, minute, and **AM** or **PM** for the 24-hour time period when Secure Access will disable the access rule, and then click **OK**.
   c) (Required) For **Days**, click on the days of the week when Secure Access will enable the access rule.



d) (Optional) Click **Add Time Period** to create another time period for the Schedule. (Optional) Repeat Steps 8-10 to add another time period to the Schedule.



e) (Optional) Click **Remove** to delete a configured time period.

6. Click **Save**.

Delete a Schedule

Provides instructions for completing the Delete a Schedule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Secure Access, you can remove a Schedule only if it is not associated with any access rules in the Access policy.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

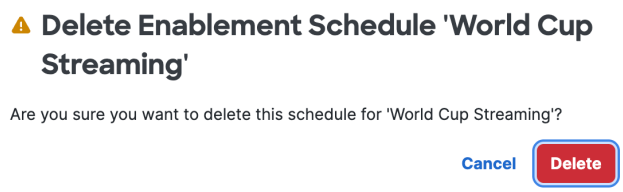
---

1. Navigate to **Resources** > **Settings** > **Enablement Schedule**.



2. Navigate to the **Enablement Schedules** table.
   a. For **Associated Rules**, confirm that Secure Access displays **No rules**, which indicates that no access rules include the Schedule.
   b. If the Schedule has associated rules, you must remove the Schedule from the access rules. For more information, see Schedule Enablement Time and Date.
3. Remove the Schedule resource in the organization.

a) Navigate to a Schedule in the table, click on the ellipsis (**...**), and then choose **Delete**.
b) Navigate to the **Schedule Name** column, click on the name of a Schedule, and then click **Delete**.



4. Click **Delete** to confirm the removal of the Schedule in Secure Access.

36 Virtual Private Networks and Proxy Settings

Topics:

- Manage Virtual Private Networks
- Manage Machine Tunnels
- Manage Application-Based Remote Access VPN (Per App VPN)
- Manage Secure Client Scripts
- Manage VPN Connection Posture Profiles
- Manage Proxy Chaining

Provides an overview of Virtual Private Networks and Proxy Settings in Cisco Secure Access, including Manage Virtual Private Networks, Manage Machine Tunnels, and Manage Application-Based Remote Access VPN (Per App VPN). It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Virtual Private Networks

Virtual Private Networks (VPNs) enable users to access your network from a remote location safely and securely.

A remote access VPN allows individual users to connect to a network from a remote location using a computer or other supported device that is connected to the internet. This allows mobile workers to connect from their home networks or a public Wi-Fi network, for example.

Manage the settings and profiles of your remote access VPNs that are registered with Secure Access:

1. A secure VPN connection requires a VPN profile. A VPN profile is the set of configuration settings that define how a VPN connection will be established, including details like authentication methods, encryption protocols, and server addresses, essentially providing the framework for creating a secure connection to a specific network. For more information, see Manage VPN Profiles.
2. A fully qualified domain name (FQDN) adds an extra layer of flexibility and precision when you create VPN profiles and access rules, providing enhanced security and simplifying network management. For more information, see FQDNs for Network Connections.
3. Cisco Secure Access protects the DNS traffic in your organization. Optionally, DDNS (Dynamic DNS) service updates the mappings of domain names to IP addresses to provide accurate IP addresses to DNS clients. For more information, see Manage DNS and DDNS Servers.
4. Manage your organization's regions and IP address pools that are used to secure the request and response traffic of your remote access VPN profiles. For more information, see Manage Regions and IP Pools.
5. A remote access VPN machine tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. For more information, see Manage Machine Tunnels.
6. (Optional) Configure a RADIUS group and add servers to the group to apply Authentication, Authorization, and Accounting (AAA) methods to a VPN profile configurations. For more information, see Add a RADIUS Group.

Manage Regions and IP Pools

Describes Manage Regions and IP Pools in Cisco Secure Access. When setting up a VPN profile, you choose the Secure Access region where your data center is located, which determines where the VPN traffic will be routed within your network.

When setting up a VPN profile, you choose the Secure Access region where your data center is located, which determines where the VPN traffic will be routed within your network.

- A Secure Access region is a cluster of data centers in a specific geographic area, such as the Northeastern United States or Western Europe. It is best practice to choose a region that is geographically close to users; this reduces latency because data reaches the users more quickly. We strongly recommend adding two regions located as close together as possible to support failover conditions.
- An IP address pool is a sequential range of IP addresses within a certain network. You can have multiple pool configurations. VPN profiles require IP addressing pools in order to be fully-functional. In addition, control plane traffic such as RADIUS is sourced from the Secure Access IP address pools defined as the System IP pool on the dashboard.
- Ensure the IP addresses included in System IP pool are allowed to communicate with necessary services hosted on your premises such as Radius servers, DNS servers, CRL/OCSP servers, and other components of Secure Access.

For more information, see Add an IP Pool.

RAVPN IP Pools Best Practice

If the RAVPN service is deployed across multiple regions, each region should be sized to support both normal user load and expected failover scenarios. For example, assume a region normally supports 100 users and requires 100 available client IP addresses to support those users.

For regional failover, if another region becomes unavailable, the surviving region must have enough IP capacity to support its own normal users plus any users failed over from the unavailable region.

For example, if a surviving region normally supports 100 users and also needs to absorb 100 users from another unavailable region, it must support 200 active VPN users and therefore requires 200 available client IP addresses.

The surviving region should also have enough reserved IP capacity to support this 200-user load even if one vEDC in that region becomes unavailable. In this example, the surviving region should have 400 available client IP addresses.

Failover in Regions and IP Pools

For every region selected in this process Secure Access polls different locations within that region to ensure the best VPN connectivity is promoted. To ensure that when failover happens in your region your environment does not affect your connectivity, we recommend adding at least two regions as geographically close as possible. This protects and ensure user connectivity because if data center A is not operating correctly or is experiencing connectivity issues and becomes unavailable, data center B remains active and detects the drop. Data center B automatically loadbalances users from data center A; this action appears as a reset and then users are transferred from data center A to data center B. If you create two data centers in two different regions, the IP addresses may not be viable.

To address failover we strongly recommend adding two regions and also to committing to twice the number of IP addresses in your IP pools to cover all of the users per data center. That means that if there are 150 users per region, you should create a combined IP pool that contains at least 300 IP addresses to accommodate the additional users in a failover scenario.

Add a Region Configuration

Provides instructions for completing the Add a Region Configuration workflow in Cisco Secure Access. Add an IP pool that is used to manage a set of IP addresses for your VPN profile.

Add an IP pool that is used to manage a set of IP addresses for your VPN profile. Optionally, add a RADIUS group for VPN profiles.

Use the following procedure to add new locations with region names, geographic details, and IP address ranges. This creates different regions based on where your users are accessing the internet from. Remember to associate appropriate security policies with each location to manage traffic based on region.

Note that this allows you to create and subsequently add this to an Access Policy rule, making the focus based on an IP address or ip pool. We **strongly** recommend the folowing practices when crating a region:

- Create rules based on machine or device identity instead.
- Add two regions as geographically close as possible to avoid failover.

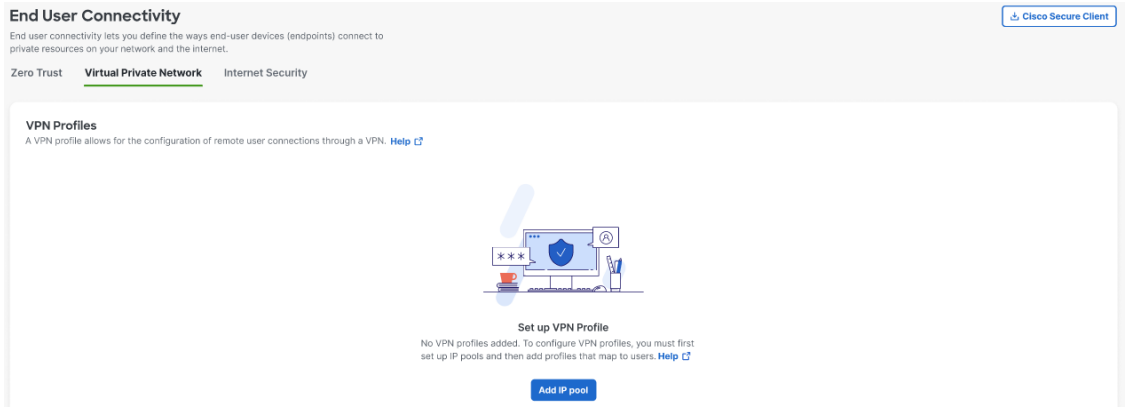
To add a region configuration, which includes managed IP pools, complete the following steps:

Before you begin

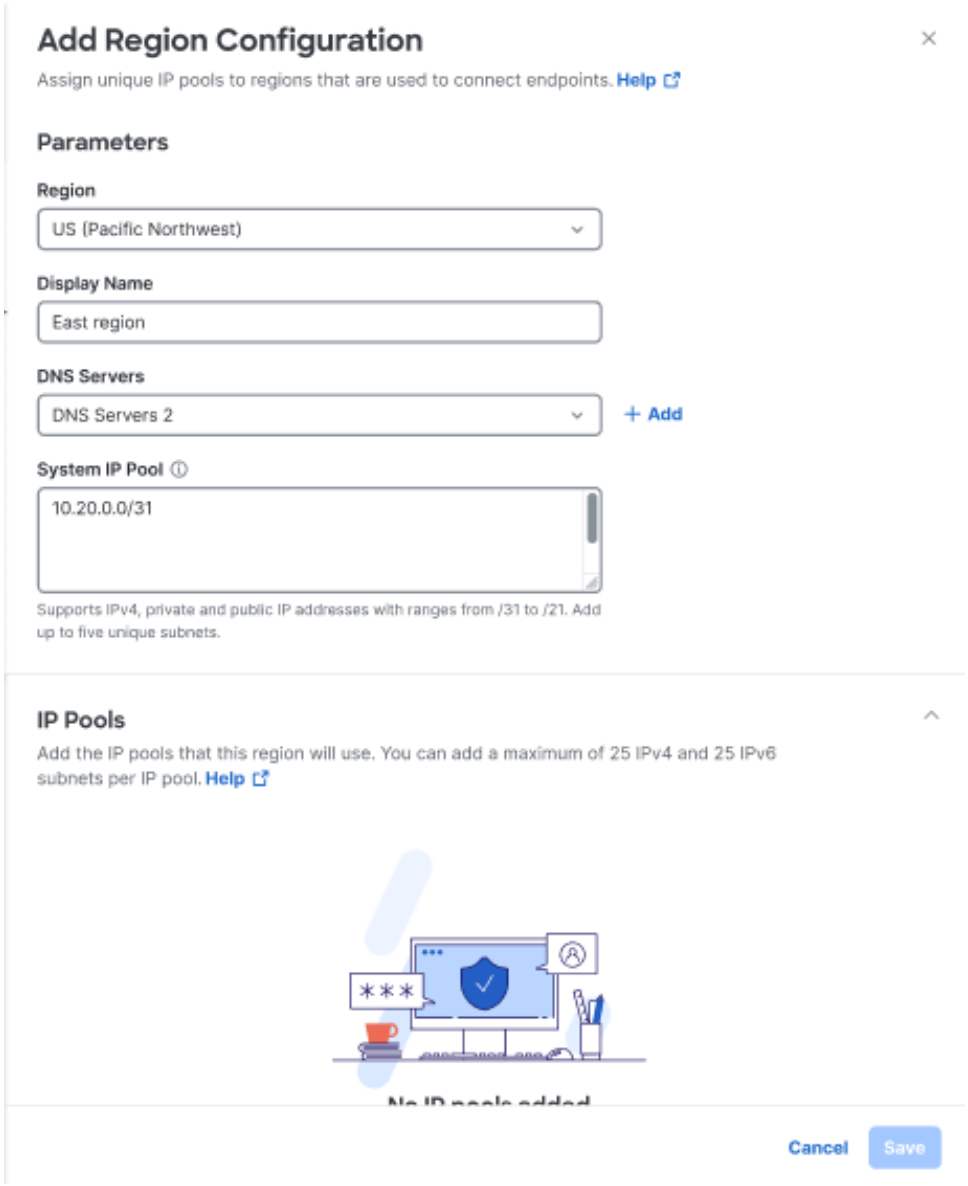
A Full Admin user role is required. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Click **Add IP pool** to define IP pools that can be used to distribute IP addresses for remote access VPN profiles.



3. Define **Parameters** required to **Add a Region Configuration**.



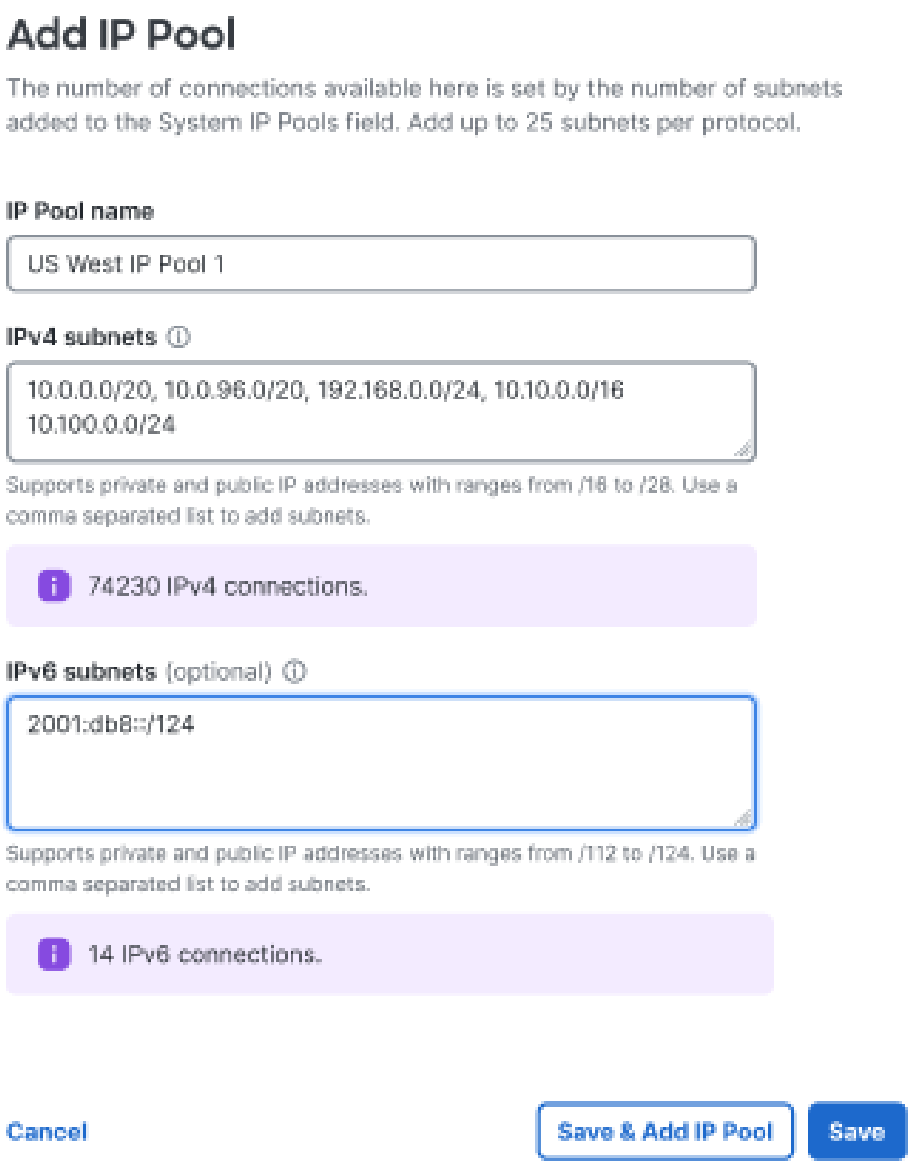
a) Map the IP pool to an available **Region**.
b) Add a meaningful **Display name**.
c) Choose a pair of **DNS Servers** from the drop-down, or click **Add** to add a new DNS pair.

d) For the **System IP Pool** add subnets needed for remote management access to the VPN headend. Supports ranges from /31 to /21. You can add add up to 5 comma-separated ranges. Subnets added here limit the total number of connections added through IP Pools section.

4. **Note**

   To prevent a possible network outage caused by server failure or connectivity issue, we recommend configuring at least two IP pool regions with the secondary region located as close to the primary IP pool region as geographically possible.

Scroll down and click **Add IP pool** to define the IP pools needed for the region configuration.



a) Input an **IP Pool name** that identifies the pool for use with remote access VPN endpoint devices. Each endpoint will be assigned an IP address from a defined IP pools.

b) Add **IPv4 subnets** needed for use with remote access VPN endpoints. Each endpoint will be assigned an IP address from the defined IP pool. Supports ranges from /28 to /16. You can add multiple comma-separated ranges.
c) Add **IPv6 subnets** (optional). Supports ranges from /124 to /112. You can add multiple comma-separated ranges.

5. Click **Save**.

Enable or Disable VPN Regions

Before you enable or disable a region in your organization be aware that this act can drastically alter how your environment operates. If you opt to **disable** a region be aware of the following consequences:

- All users connected to the region are immediately disconnected.
- The disabled region is unreachable to all users.
- New connections are now routed to other available regions.

You must enable or disable each region individually; you cannot change the status of multiple regions simultaneously by using this tool.

Before you begin

You **must** have at least one region already configured and deployed in a VPN profile before you can enable or disable a VPN region out of rotation. This action is not available if no regions are configured. For more information see Add a Region Configuration.

> **Note**
>
> While you must have at least one region already configured and associated with a VPN profile, to disable a region, you can disable a region even if it is the only region within you organization.

Procedure

---

1. Navigate to **Connect** > **User Connectivity** > **Virtual Private Network**.
2. Either examine the **Regions and IP Pools** widget at the top of the window and click **Manage**. Alternatively, if you are looking for a specific region that is currently enabled or disabled you can click inside the interactive **Enabled** or **Disabled** tiles to filter the Regions page by status.
3. If you did not click the interactive **Enabled** or **Disabled** tiles in the previous step, feel free to interact with the tiles in the **Regions and IP Pools** page to filter the regions displayed.
4. Locate the region you want to enable or disable from your VPN rotation and click the blue ellipsis at the right end of the row for the region you want to modify.
5. Select either **Enable** or **Disable**.

> **Note**
>
> If you are **Disabling** a region you must confirm the action in the pop-up window by checking the I understand and wish to proceed announcement and then click **Disable**. It may take several minutes to completely disable the region from your VPN configuration.

What to do next

Depending on the action you took, the region is immediately marked as either enabled or disabled in both the **Regions and IP Pools** and the **End User Connectivity** page.

To view details about the connection events for the region or regions that are now disabled, see the Remote Access Log.

Add an IP Pool

Provides instructions for completing the Add an IP Pool workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

An IP address pool is a sequential range of IP addresses within a network, and multiple pools can be configured. VPN profiles require at least one IP pool to function properly. Control plane traffic, such as RADIUS, also uses IP addresses from these pools. IP address pools provided by Secure Access define the parameters used to secure request and response traffic for your VPN connections.

Common uses for IP address pools include:

- Reserving resources for specific users or groups.
- Assigning dedicated IP ranges for specific applications.
- Organizing and securing network traffic based on user roles.

Managing IP address pools helps secure and organize remote access VPN traffic effectively. Use the following procedure to configure IP pools for remote access VPNs in Secure Access.

> **Note**
>
> Note: To ensure optimal performance, follow these IP address allocation guidelines:
>
> - Allocate at least one system IP per 1,000 anticipated VPN connections.
> - Use a minimum IP block size of /28 (16 addresses).

Before you begin

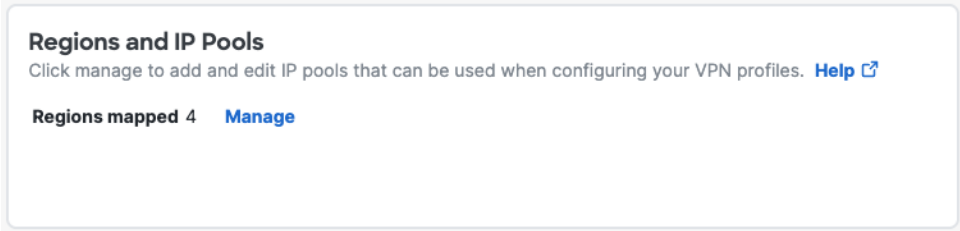
This procedure requires the following:

- Full Admin user role. For more information, see Manage Accounts.
- If you are adding an IPv6 IP pool, ensure your infrastructure and environment is compatible and supports IPv6 connections. Failures occur when there is a mismatch between IP protocols.

- Unless you have configured your devices to use an alternate CGNAT IP address range, we do not recommend using multicast, RA VPN, CGNAT IP pools or any IP ranges already in use for this procedure. Use non-RFC1918 IP addresses.
- IP pools cannot include addresses/networks listed in IP Address Restrictions.
- If you intend to create an IP pool for an ISE integration, confirm any private applications are correctly segregated. Failure to segregate private applications introduces the possibility of the ISE server subnet getting assigned to a ZTA end user. This causes unpredictable behavior when matching traffic against the private application policy.

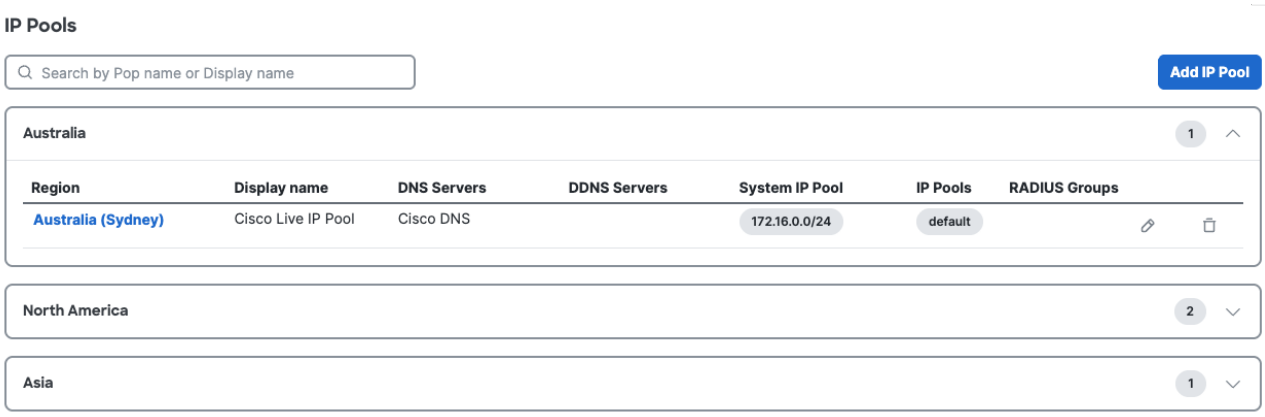
Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Under **Regions and IP Pools**, click **Manage**

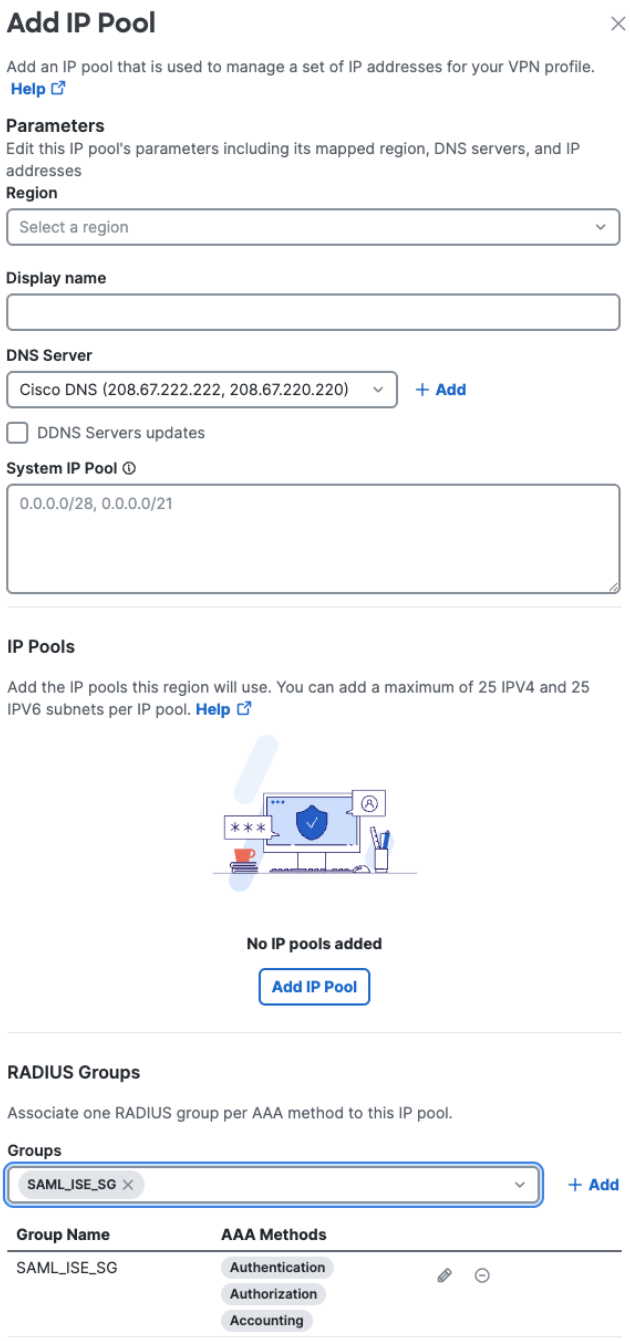


The **IP Pools** page opens. Each region must have a unique IP pools configured. These IP pools are used to assign IP addresses to endpoint devices connecting via remote access VPN. Proper configuration ensures that VPN clients receive unique IP addresses from the pool associated with their region, preventing IP address conflicts and enabling efficient routing and management of remote access VPN connections.

3. Take the following actions to manage IP pools.
   - Click **Add IP Pool** to open a dialog for creating a new IP pool.
   - Click an existing IP pool's region name to view the **IP pool detailed information** pane.
   - Click the **pencil icon** to edit an IP pool.



4. Configure IP pool parameters:



a) Select an available **Region**.
b) Enter a **Display name**.
c) Select a **DNS Server** pair from the dropdown, or click **+ Add** to create a new DNS pair.
d) **DDNS Servers updates** (optional): Check the box to select an existing DDNS server, or click **+ Add** to create a new DDNS pair.
e) **System IP Pool** (optional): Add up to five subnets with IP ranges from /28 to /21 to grant Secure Access permission to obtain IP addresses for administrative connections to customer data centers. Subnets added as system IP pools count against the total number of IP pools available in the next step.

5. **IP Pools**: Add the IP pools this region will use. You can add a maximum of 25 IPv4 and 25 IPv6 subnets per IP pool.



> **Note**
>
> IP pools cannot include addresses/networks listed in IP Address Restrictions.

a) Enter an **IP pool name**.
b) Add **IPV4 subnets** for remote access VPN user connections. Each user endpoint will receive an IPv4 address from the IP pool. You may add multiple comma-separated ranges from /28 to /16.
c) Add **IPv6 subnets** (optional) for remote access VPN user connections. If configured, each user endpoint will receive an IPv6 address from the IP pool. You may add multiple comma-separated ranges from /124 to /112. The IPv6 user connection count must be greater than or equal to the IPv4 user connection count configured for this IP pool.

6. **RADIUS Groups** (optional): Select an existing RADIUS group or click **Add RADIUS Group** to associate a RADIUS group with this IP pool. For more information, see Add a RADIUS Group.
7. Click **Save & Add IP Pool** to finish configuring a new IP pool. Click **Save** to finish editing an existing IP pool.

Assign an IP Pool

Provides instructions for completing the Assign an IP Pool workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access provides IP pool configurations to secure the request and response traffic of your VPN profiles. Typically, IP pools would be used to reserve resources for particular users or groups or to make sure that certain ranges are used for particular purposes.

VPN profiles require that you configure and assign at least one IP address pool in order to be fully-functional. IP address pools are managed through the **Regions and IP Pools** console, which allows you to organize and allocate IP addresses across your regions. You can create pools to represent different organizational units, environments, or regions, making it easier to manage your IP address space.

To assign an IP pool to manage a set of IP addresses for your VPN profile, complete the following steps:

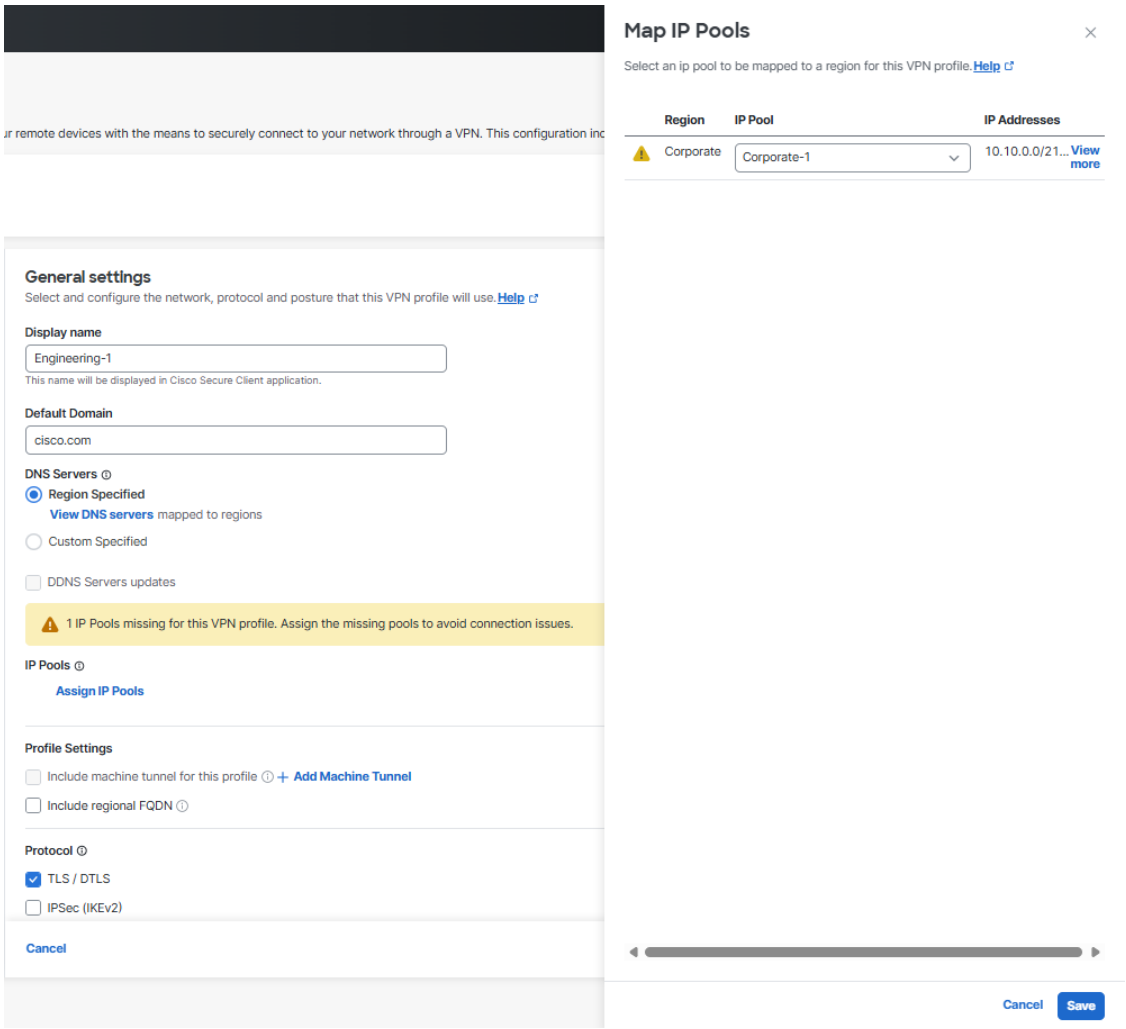
Before you begin

The following are required:

- Full Admin user role. For more information, see Manage Accounts.
- At least one IP pool defined for use in VPN profiles.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click on a profile to modify or click **+ VPN Profile** to add a new profile.
3. Under **General Settings**, click **Assign IP Pools** and select one IP pool per region from the IP Pool drop-down. VPN profiles must have at least one IP pool assigned in each region for a valid configuration. For more information, see Add an IP Pool.



4. Click **Save** to assign the IP pool to the VPN profile and to clear the alert.

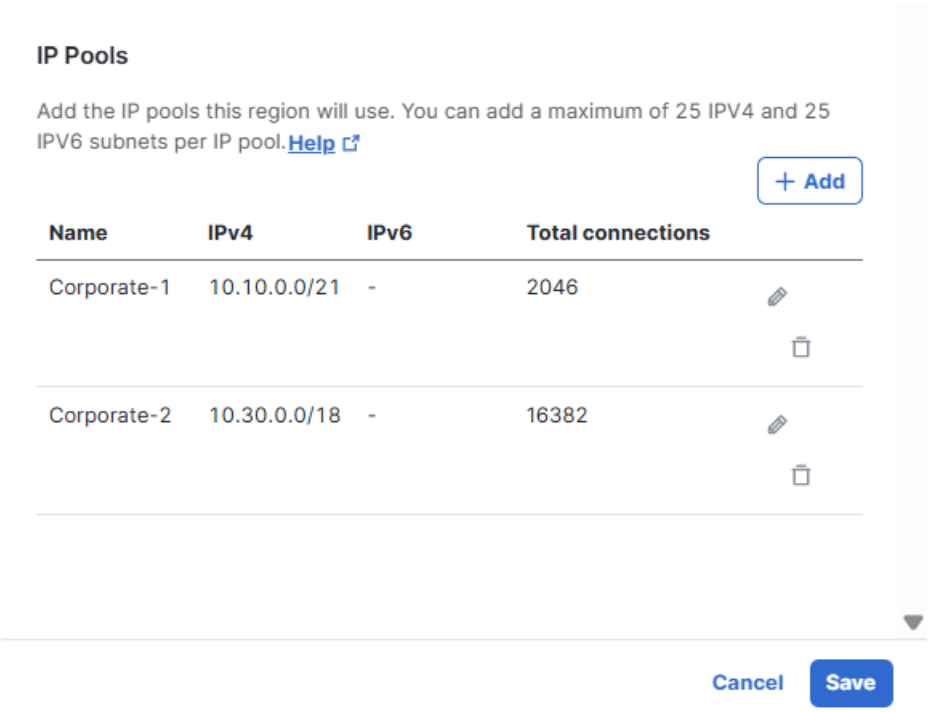
Modify IP Pools

Provides instructions for completing the Modify IP Pools workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can modify IP address pools. You can edit a pool's CIDR and other settings through the **Regions and IP Pools** console.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **Regions and IP Pools**, click **Manage**.
3. Select a region or data center to modify and click the edit icon.
4. Scroll to **IP Pools** to edit a pool's CIDR and to add or remove subnets.



5. Optionally, click **+ Add** to create a new IP pool for the region.
6. Click **Save** to commit changes or **Cancel** to exit.

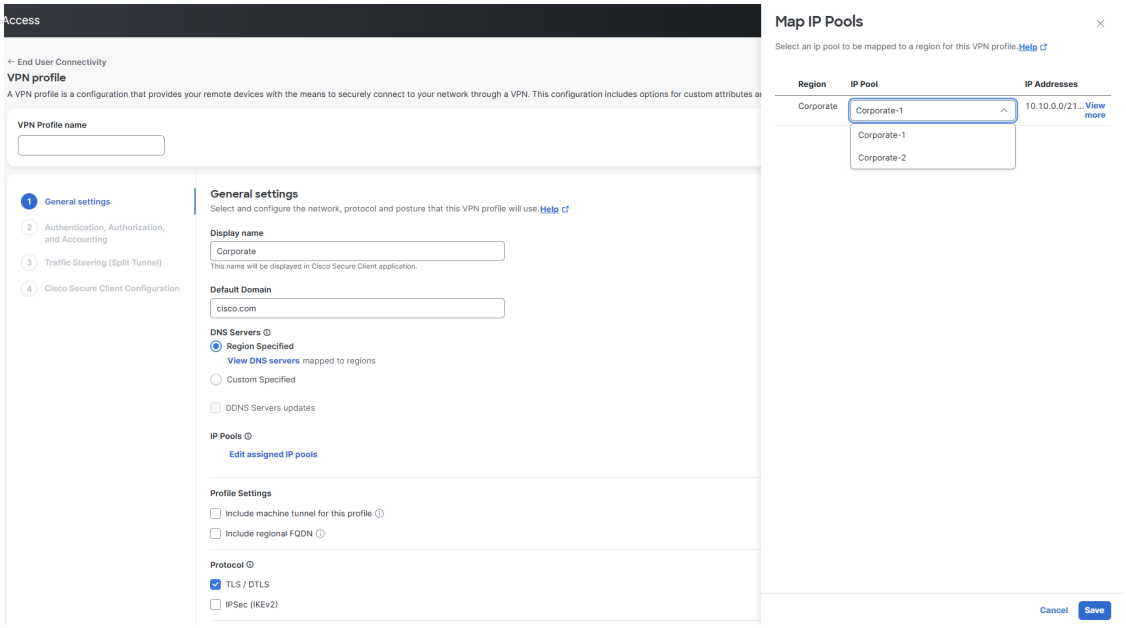
Modify IP Pool Assignment

Provides instructions for completing the Modify IP Pool Assignment workflow in Cisco Secure Access. You can modify which IP pools are mapped to a VPN profile.

You can modify which IP pools are mapped to a VPN profile. You can edit a pool's assignment through the **VPN Profile** console.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Choose the profile to modify under **VPN Profiles** and click the edit icon.
3. Under **General Settings**, click **Edit assigned IP pools** and select another pool from the **IP Pool** drop-down. VPN profiles must have at least one IP pool assigned in each region for a valid configuration. For more information, see Add an IP Pool.



4. Click **Save** to assign the selected IP pool to the VPN profile.

Manage RADIUS Servers and Groups

Describes Manage RADIUS Servers and Groups in Cisco Secure Access. Cisco Secure Access integrates with Cisco Identity Services Engine (ISE) to support centralized RADIUS servers that provide Authentication, Authorization, and Accounting (AAA) services for remote users accessing the network.

Cisco Secure Access integrates with **Cisco Identity Services Engine (ISE)** to support centralized RADIUS servers that provide **Authentication, Authorization, and Accounting (AAA) services** for remote users accessing the network.

- **Authentication** verifies the identity of the user.
- **Authorization** enforces policies that determine which resources and services an authenticated user can access.
- **Accounting** tracks user activity for billing, monitoring, and security.

Guidelines for RADIUS protocol and AAA methods:

- Specify the IP address, port number, and shared key for each RADIUS server. Other settings, such as RADIUS username format and retransmission counts, have default values and can be adjusted based on network requirements.
- RADIUS server group settings like username format and shared key must match those on the RADIUS server.
- A maximum of eight servers can be added to a Secure Access RADIUS group.
- The order of server groups and servers within groups determines the server access order.
- **Authentication Mode:** Methods such as MS-CHAPv2 and PAP are supported. The default RADIUS authentication port is 1812 (valid range 1-65535).
- **Authorization Mode:** The default RADIUS authorization port is 1812 (valid range 1-65535). Use the Change of Authorization (CoA) port when using the RADIUS group for ISE Policy Enforcement in remote access VPNs. The CoA port is defined in the network device profile and can be modified – ensure consistency between the network device profile and the network device if the CoA port is changed.
- **Accounting Mode:** The RADIUS Accounting report tracks user session durations and can help diagnose connectivity issues. The default RADIUS accounting port is 1813 (valid range 1-65535).

- Environments with an ISE integration and a CNHE network tunnel must have a private access policy; this means that your source should be a Region IP pool and the destination should be an ISE Server IP address.

> **Note**
>
> RADIUS servers cannot use addresses/networks listed in IP Address Restrictions

Add a RADIUS Group

Provides instructions for completing the Add a RADIUS Group workflow in Cisco Secure Access. This section describes how to configure a RADIUS group and add servers to the group.

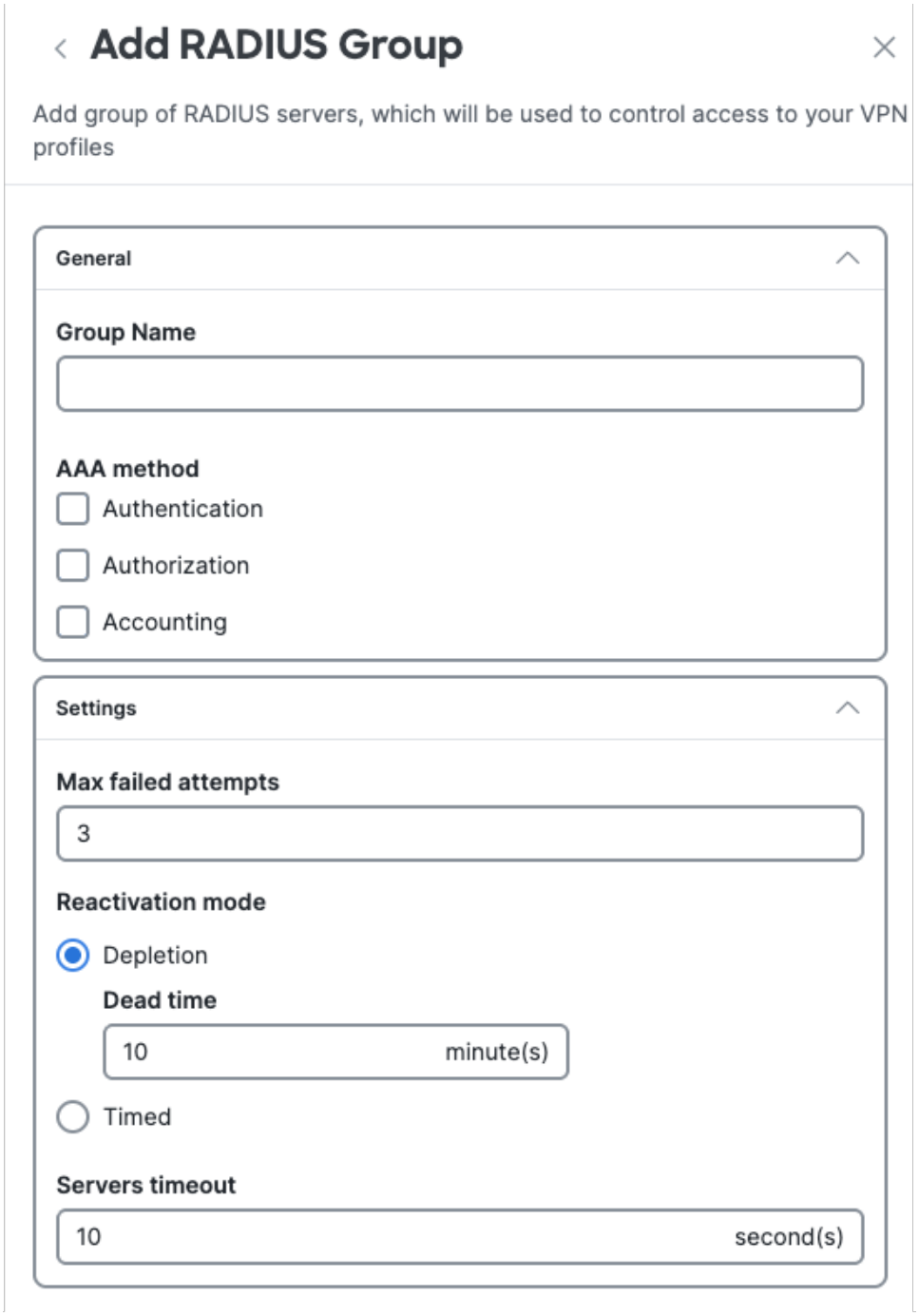
This section describes how to configure a RADIUS group and add servers to the group. This RADIUS group can be applied to the Authentication, Authorization, and Accounting (AAA) methods of a VPN profile configuration and mapped to other VPN profiles.

Before you begin

A Full Admin user role is required. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Under **VPN Profiles**, click **Add**.
3. Complete **General settings** of the VPN Profile and click **Next**.
4. Under **Authentication, Authorization, and Accounting**, expand **Map authentication groups to regions**, then click **+ Group**.



RADIUS Servers

You can add up to 8 servers in each group

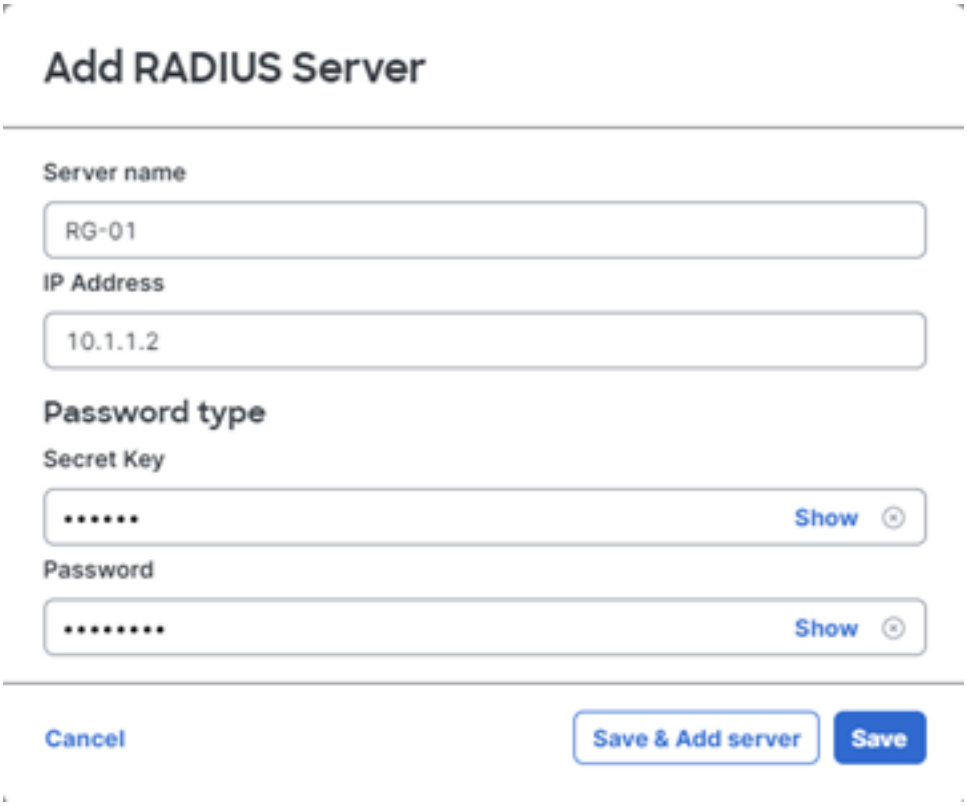
Assign servers

test ×

+ Add

#	Server Name	IP Address
1	test	172.16.12.111

5. Associate up to one RADIUS group per AAA method to control access to VPN profiles. Add up to eight RADIUS servers to each group.
   a) Enter a **Group Name**.
   b) Choose and configure one or more **AAA methods**.
      - Each method requires a port number between 1 to 65535 for RADIUS authentication.
      - **Authentication**:
        - The default port number is 1812.
        - The **Authentication** and **Authorization** methods must have the same port number when used together.
        - Check **Microsoft CHAPv2** to use Microsoft Challenge Handshake Authentication Protocol Version 2 as the authentication method.
      - **Authorization**:
        - The default port number is 1812.
        - The **Authentication** and **Authorization** methods must have the same port number when used together.
        - Check **Authorization mode only** to require no common password.
        - Check **Change of authorization (CoA) mode** to register the RADIUS server group for CoA notification. If you enable CoA, the listening port for RADIUS CoA requests uses the default of 1700. Use the CoA port when using the RADIUS group for ISE Policy Enforcement in remote access VPNs. The CoA port is defined in the network device profile and can be modified – ensure consistency between the network device profile and the network device if the CoA port is changed.
      - **Accounting**:
        - The default port number is 1813.
        - Under **Accounting mode** select **Single** to send accounting data to one server, or **Simultaneous** to send accounting data to all servers in the group.
        - When Cisco ISE is integrated with a Cisco ASA, set the ASA **Accounting mode** to **Single**.
        - Check **Interim accounting update** to enable the periodic generation of RADIUS interim-accounting-update messages.
   c) Configure **Settings**.
      - **Max failed attempts**: Configure the maximum number of failed AAA transactions (from 1 to 5; default is 3) before authentication will try the next RADIUS server in the group.
      - **Reactivation mode**:
        - Select **Depletion** to reactivate failed servers only after all of the servers in the group are inactive. Configure the **Dead time** (0 to 1440 minutes; default is 10 minutes) that must elapse between the time when the last RADIUS server in the group is disabled and the time when all servers will be reenabled. Authentication will be attempted locally until dead time elapses. **Note:** Dead time applies only when fallback to the local database is configured.
        - Select **Timed** to reactivate failed servers after 30 seconds of down time.
        - **Servers timeout**: The number of seconds to wait for a response from a RADIUS server. Default is 10 seconds.
   d) **RADIUS Servers**: Add up to eight existing RADIUS servers to the group, or click **+ Add** to configure a new RADIUS server.



Note

RADIUS servers cannot use addresses/networks listed in IP Address Restrictions.

e) Click **Save**.

Test a RADIUS Server Connection

Regions are used to map RADIUS server or groups for authentication, authorization, and accounting (AAA) purposes. When configuring a RADIUS server in Secure Access, you must select the regions and associate them with the appropriate RADIUS groups to ensure the servers are correctly assigned per each region. We recommend testing server connectivity prior to deploying as connectivity to regions immediately affects the mapping to all three AAA functions. Note that you must test each connection individually, but you can test one connection against multiple regions simultaneously.

Before you begin

Before you can test the connection with the configured RADIUS server, you must have the following established:

- You must have an AAA sever already configured.
- The CNHE tunnel must be established and connected. Check your configuration and tunnel status in the Network Tunnel Groups tab of the **Connect** > **Network Connections** page.
- The user you intend to test the connection with should be included the **Users** tab of the **Connect** > **Users, Groups, and Endpoint Devices** page. If there are no users then you cannot test in that region.
- You must have at least one group assigned to the region.
- You must have at least one VPN profile deployed within the region you intend to test.

Procedure

1. Log into your Cisco Cloud Control organization and navigate to **Security** > **Resources** > **Configuration** > **AAA Servers** .
2. Click the **RADUS Servers** tab.
3. Click **Test Connection**.
4. Use the drop-down menu and select the RADIUS server want to test.
5. In the **Server Info & Credentials** window confirm the following:
   - Server IP address.
   - Authentication type.
   - Groups associated.
   - VPN Profiles.
6. In the **Test Account Credentials** enter your organization username and password.
7. Expand the **Regions to test** window and expand the drop-down menu to select at least one region to test against. While the group that is already associated with the region is automatically selected by the system and is listed at the top of the drop-down menu, you can select any region to test with.
8. Click **Run Test.** A system-issued test executes and runs for 30 seconds per test before timing out. Test results are displayed within this window. Click **View details** to review unsuccessful connection test details to troubleshoot the connection.

What to do next

If you experience issues with connectivity, contact Cisco Support.

Manage VPN Profiles

Describes Manage VPN Profiles in Cisco Secure Access. A Remote Access Virtual Private Network (VPN) enables individual users to securely connect to a private network from any remote location using a computer or other supported device with Internet access.

A **Remote Access Virtual Private Network (VPN)** enables individual users to securely connect to a private network from any remote location using a computer or other supported device with Internet access. This functionality is particularly valuable for mobile workers who need to connect from home networks or public Wi-Fi environments.

You can enable persistent remote access in your VPN profiles with the **Always On** option.

Key features of Always On:

- **Automatic connection:** AnyConnect automatically connects to the VPN when the user logs in to their computer.
- **Policy enforcement:** Protects the computer from security threats by preventing access to Internet resources when not connected to a trusted network.

Important considerations when using Always On:

- **Digital certificates:** We recommend purchasing a digital certificate from a certificate authority and enrolling it on secure gateways.
- **User login requirement:** If Always On is enabled but the user does not log on, the AnyConnect VPN connection will not be established.

- **Windows Updates:** We strongly recommend ensuring both your Windows operating system is up to date with sustem-provided updates and your Windows Defender account is **not** out of date. Insufficient versioning and noncompliance causes policy failure.

The **Allow VPN Disconnect** feature accompanies Always On functionality, providing users with the flexibility to disconnect from their current VPN session when needed. Common use cases of Allow VPN Disconnect:

- Selecting an alternative secure gateway due to performance issues.
- Resolving reconnection issues following a VPN session interruption.
- Troubleshooting connectivity problems.

For additional configuration details, refer to the following documentation:

- Add VPN Profiles
- Manage IP Pools
- Add a RADIUS Group
- Manage VPN Settings

Add VPN Profiles Step 1 – General Settings

Provides instructions for completing the Add VPN Profiles Step 1 – General Settings workflow in Cisco Secure Access. This procedure requires the Full Admin role in Secure Access.

A virtual private network (VPN) connection establishes a secure tunnel between endpoint devices over a public network such as the Internet. This section describes how to create VPN profiles to allow for configuration of remote user connections through a VPN.

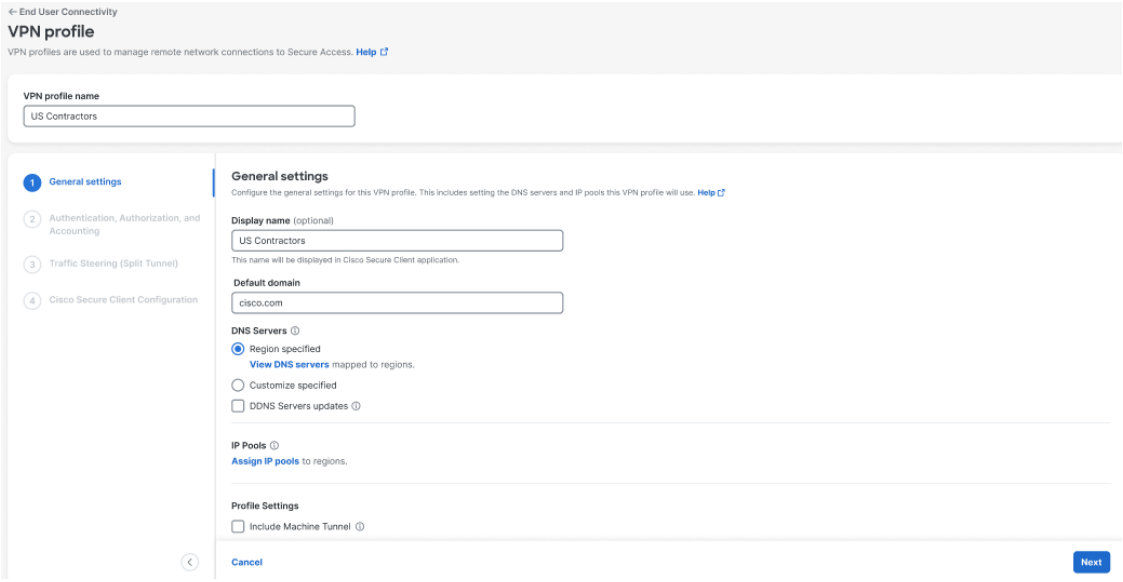
The first step is to name and configure the general settings of the VPN profile.

Before you begin

This procedure requires the Full Admin role in Secure Access. See Manage Accounts for more information.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Under **VPN Profiles**, click **+ VPN Profile**.



3. Enter basic profile information.

Field	Description	Required
VPN profile name	Enter a name to identify this profile.	Yes
Display name	Enter a customizable label that end-users will see in Cisco Secure Client when selecting a profile.	No
Default Domain	Specify the default domain for this profile.	Yes

4. Configure DNS settings.
   a) By default, **DNS Servers** is set to **Region specified**, meaning the VPN profile uses the DNS servers designated for each region.

Option	Description	Required
View DNS servers	Click to see the list of DNS servers mapped to regions	No
Custom specified	Select to use a custom DNS pair instead of the regional default. Click **Map DNS** servers to open the configurable view and select from available DNS servers. For detailed instructions, see Map DNS Servers to Regions	No

   b) By default, **DDNS Servers** is set to **Region specified**, meaning the VPN profile uses the DDNS servers designated for each region.

Option	Description	Required
DDNS Servers updates	Check to enable dynamic updates to domain name-to-IP address mappings when a remote user's network IP address changes. For more information, see Map DDNS Servers to Regions	No

5. Click **Assign IP pools** and select one IP pool per region from the **IP Pools** drop-down.
   Important

   VPN profiles must have at least one IP pool assigned in each region for a valid configuration. For more information, see Add an IP Pool.

6. Under **IP version mode**, select one or both options:
   - **IPv4**
   - **IPv6**
7. Under **Protocol**, select at least one protocol:
   - **TLS/DTLS**
   - **IKEv2**

   Note

   If both protocols are selected, choose the primary protocol from the **Primary** drop-down menu.

8. From the **Connect time posture** drop-down, select a posture profile if required. For more information, see Add a VPN Connection Posture Profile.
9. Click **Next** to proceed to Add VPN Profiles Step 2 - Authentication, Authorization, and Accounting.

Add VPN Profiles Step 2 – Authentication, Authorization, and Accounting

Describes Add VPN Profiles Step 2 - Authentication, Authorization, and Accounting in Cisco Secure Access. Authentication is how a remote user is identified before being allowed to access networks and network resources over VPN.

Authentication is how a remote user is identified before being allowed to access networks and network resources over VPN. Authentication requires valid user credentials, a certificate, or both. Use authentication alone, or with authorization and accounting.

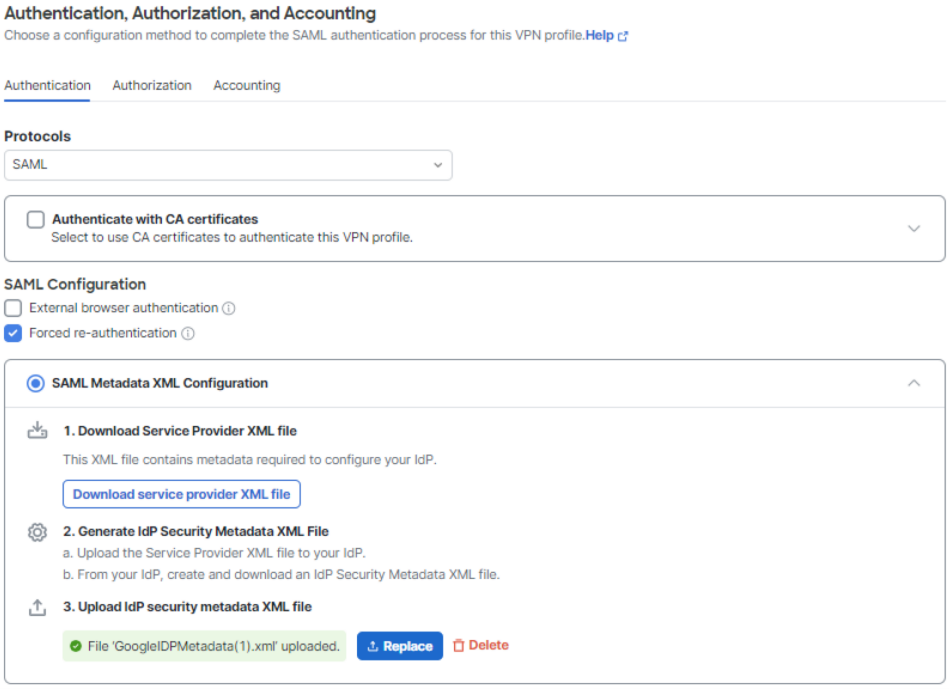
Choose one of the following authentication methods from the **Protocols** drop-down, then follow the procedure for that method.

- SAML
- RADIUS
- Certificate

Add VPN Profiles Step 2 - SAML

Provides instructions for completing the Add VPN Profiles Step 2 - SAML workflow in Cisco Secure Access. When you choose SAML for remote access VPN authentication, each user is authenticated using the SAML single sign-on server.

When you choose SAML for remote access VPN authentication, each user is authenticated using the SAML single sign-on server. SAML authentication for remote access VPN supports SAML, SAML + Single CA certificate, and SAML + Multiple CA Certificates.

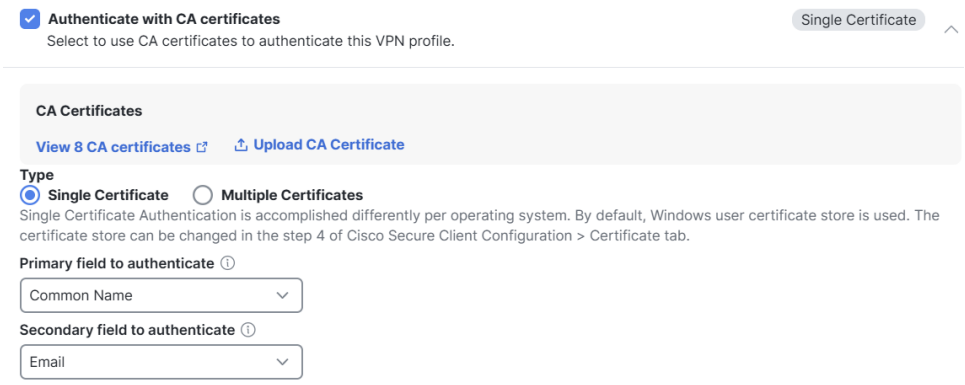


Important

In Secure Access, you can add the same SAML identity provider (IdP) in multiple VPN profiles. Secure Access does not support the configuration of different settings for the same SAML IdP in multiple VPN profiles so you must configure the same SAML IdP metadata in all of the VPN profiles in order to use the IdP for more than one profile, as well as enable the same metadata, certificate, and re-authentication settings for the SAML IdP. Without this information present in all the affected profiles, the user credentials fail for the IdP serivce.

Procedure

1. Select `SAML` from the **Protocols** drop-down.
2. **Authenticate with CA certificates**: Select to use CA certificates to authenticate this VPN profile.



> **Note**
>
> If you select SAML attribute name with the intention of selecting the posture profile with the VPN profile, then the authentication type of said VPN profile should be **SAML+Cert** or **SAML+Multicert** based on how many certificates you want to select for posture endpoint. The SAML attributes must be present and match the certificate attributes.

3. Select options under **SAML Configuration**:
   - **External browser authentication** – Select this option to have Secure Client use a local browser for authentication. When selected, Secure Client can support other SAML-based web authentication options, such as Single Sign On, biometric authentication, or other enhanced methods that are unavailable with an embedded browser.
   - **Forced re-authentication** – Select this option to force a re-authentication whenever a VPN connection is initiated. Forced re-authentication is related to the Session Timeout setting. For more information see Cisco Secure Client Configuration.

4. Choose a configuration method.
   a) Click **SAML Metadata XML Configuration** to configure SAML authentication with your service provider XML file.
      1. Click **Download service provider XML file**. This XML file contains metadata required to configure your IdP. Upload this file to your IdP.
      2. **Generate IdP Security Metadata XML file** – From your IdP, create and download an IdP Security Metadata XML file.
      3. **Upload IdP security metadata XML file** to the SAML metadata XML configuration in Secure Access.

   b) Click **Manual Configuration** to configure SAML authentication manually with information from your Service Provider (SP) and Identity Provider (IdP).
      1. Download the SP Certificate.
      2. Obtain the following from the SAML IdP:
         - Identity Provider Entity ID URL.
         - Sign-in URL.
         - Sign-out URL.
         - IdP Certificate.

- Request Signature.

What to do next

For more information about Secure Access and SAML for VPNs with a configured VPN profile, see Manage SAML Certificates for Identity Providers.

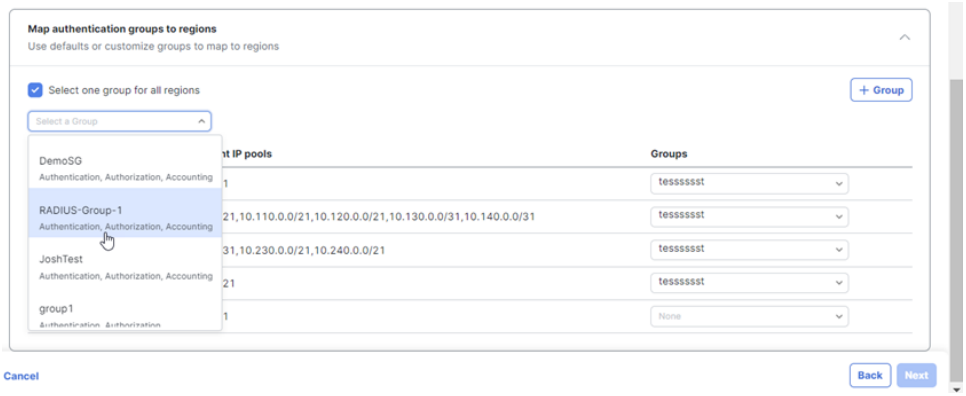
Add VPN Profiles Step 2 - RADIUS

Describes Add VPN Profiles Step 2 - RADIUS in Cisco Secure Access. Use this option to authenticate users on a RADIUS server.

Use this option to authenticate users on a RADIUS server.

> **Note**
>
> Cisco strongly discourages the use of RADIUS (RADIUS username/password only) as a single form of authentication. If the RADIUS server does not provide multi-factor authentication (MFA), then you must enable a second factor of authentication in Secure Access for VPN authentication. You can configure certificates in Secure Access as the second form of authentication.

When you choose **RADIUS**, each user is authenticated using RADIUS group servers. RADIUS authentication for remote access VPNs supports **RADIUS**, **RADIUS+ Single CA certificate**, and **RADIUS+ Multiple CA Certificates**.



Add VPN Profiles Step 2 - Certificates

Describes Add VPN Profiles Step 2 - Certificates in Cisco Secure Access. Use this option to authenticate users with trusted certificate authorities (CAs).

Use this option to authenticate users with trusted certificate authorities (CAs).

When you choose **Certificate**, each user is authenticated with a client certificate. The client certificate must be configured on VPN client endpoints. By default, the user name is derived from the client certificate fields CN and OU. If the user name is specified in other fields in the client certificate, use the **Primary field to authenticate** and **Secondary field to authenticate** field to map appropriate fields.

Select **Multiple Certificates** authentication to authenticate the VPN client using the machine and user certificates.

If have enabled **Multiple Certificates** authentication, you can select one of the following certificates to map the username and authenticate the VPN user:

- **First Cert**–Select this option to map the username from the machine certificate sent from the VPN client.

- **Second Cert**–Select this option to map the username from the user certificate sent from the client.

> **Note**
>
> If you do not enable multiple certificate authentication, the user certificate (second certificate) is used for authentication by default.

Add VPN Profiles Step 3 – Traffic Steering (Split Tunnel)

Describes Add VPN Profiles Step 3 – Traffic Steering (Split Tunnel) in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Step 3a – Traffic Steering (Split Tunnel)
- Step 3b – Proxy and DNS Steering Settings

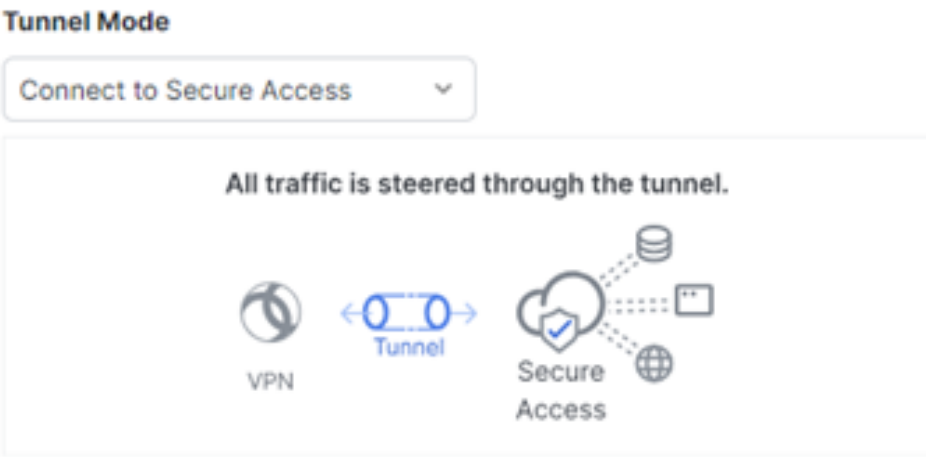
Step 3a – Traffic Steering (Split Tunnel)

Provides instructions for completing the Step 3a – Traffic Steering (Split Tunnel) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

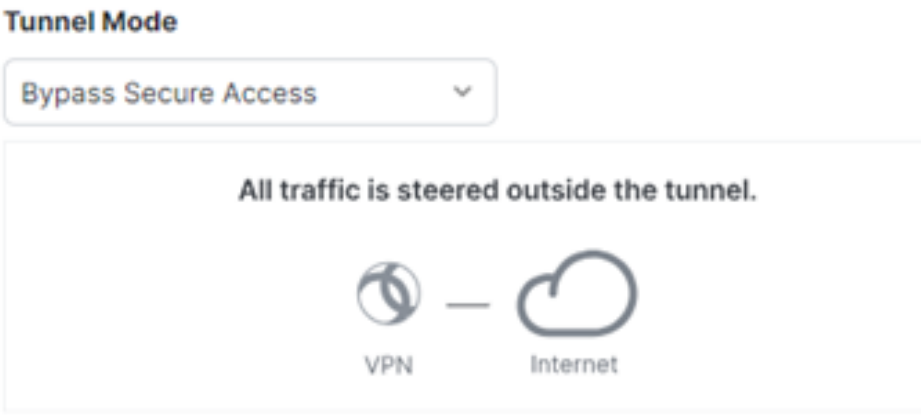
For **Traffic Steering (Split Tunnel)**, you can configure a VPN profile to maintain a full tunnel connection to Secure Access, or configure the profile to use a split tunnel connection to direct traffic through the VPN only if necessary.

Procedure

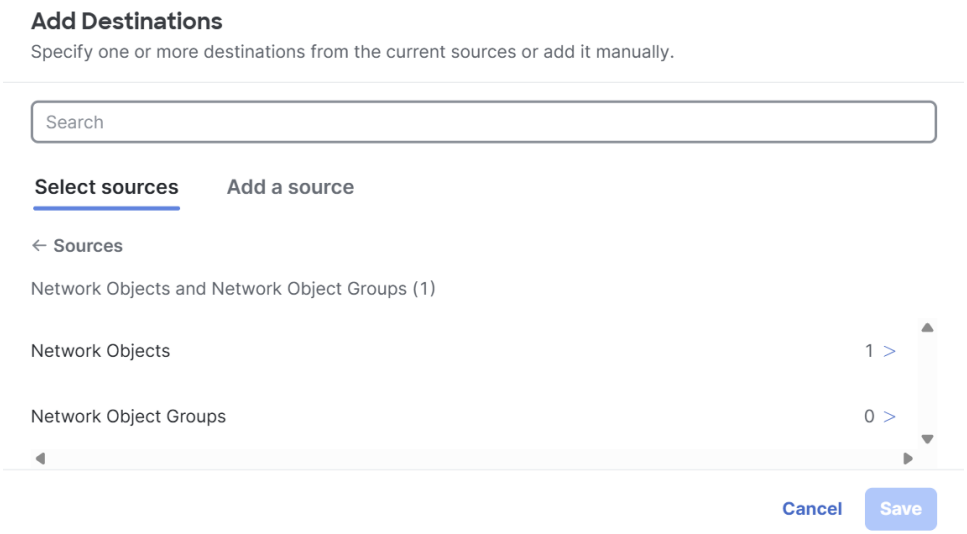
1. **Tunnel Mode**: Choose **Connect to Secure Access** or **Bypass Secure Access** for the default traffic steering mode.
   - **Connect to Secure Access** directs all traffic through the tunnel. Note that DNS names matching the configured DNS Names are routed over the local physical interface for the resolution. Any that do not match the configured DNS Names are routed via the encrypted Secure Client connection for resolution.



   - **Bypass Secure Access** directs all traffic outside the tunnel.

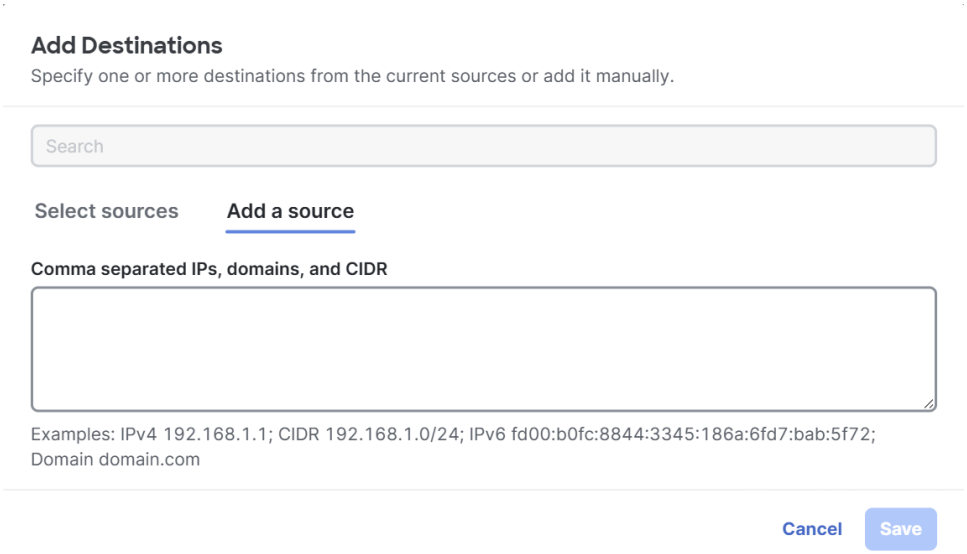


2. Add **Exceptions** for specific sources and destinations to steer traffic inside or outside the tunnel, depending on the **Tunnel Mode**.
   a. Click **+ Add**.
   b. Enter the name of a Network Object or a Network Object Group in the search bar and then select the same on the **Select sources** tab.



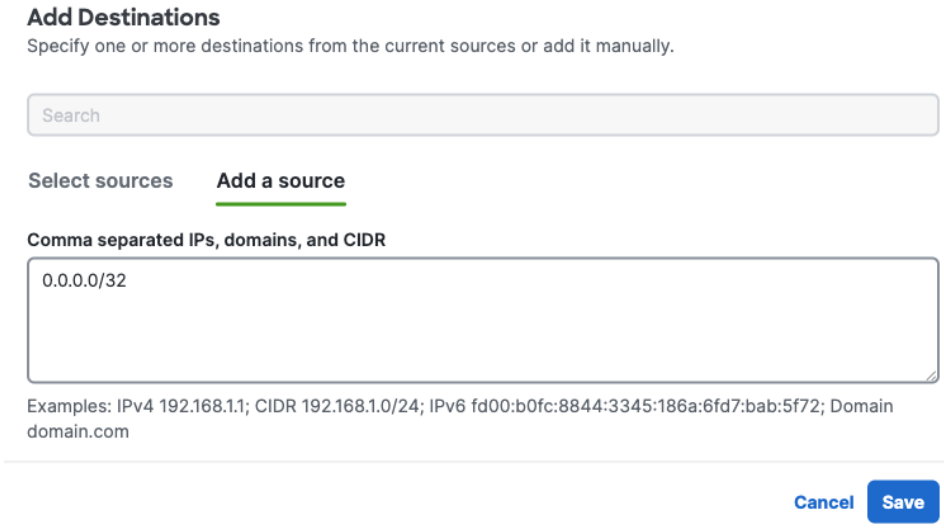
   Or

   On the **Add a source** tab, enter comma-separated IPs, domains, and network spaces.



c. Click **Save**.

3. **Local LAN Access**: If Cisco Secure Client will be configured in the next step to allow the user complete access to the local LAN connected to the remote computer during the VPN session to Secure Access, add a traffic steering exception configured for IP range `0.0.0.0/32`. For information about configuring **Local LAN Access**, see **Client Settings (General)** under Step 4 - Cisco Secure Client Configuration.



4. Click **Next** to configure the Cisco Secure Client.

Step 3b – Proxy and DNS Steering Settings

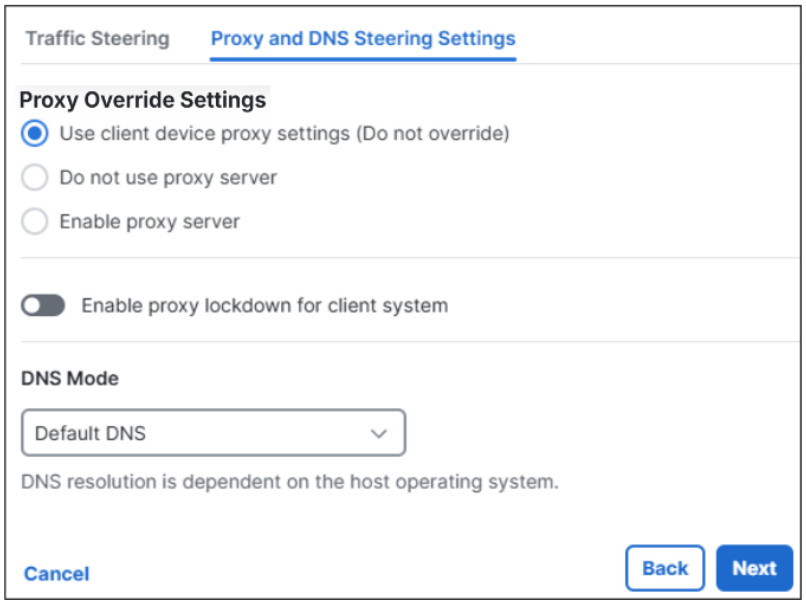
Provides instructions for completing the Step 3b - Proxy and DNS Steering Settings workflow in Cisco Secure Access. Use Proxy and DNS Steering Settings to manage how VPN clients handle proxy routing and DNS resolution.

Use **Proxy and DNS Steering Settings** to manage how VPN clients handle proxy routing and DNS resolution. You can configure the VPN profile to bypass the proxy server for specific destinations or ports, or enforce the use of an alternative proxy server.

Procedure

1. **For Proxy Settings**, choose one of the following options:
   - **Use client device proxy settings (Do not override)**: Allow the user to configure a browser proxy for HTTP traffic and use the proxy if it is configured.
   - **Do not use proxy server**: Prevent the use of browser-configured proxies. No browser connections will be routed through the proxy.
   - **Enable proxy server**: Configure and enforce the use of a proxy server for client devices.

   > **Note**
   >
   > Proxy Override Settings manage proxy behavior once the VPN tunnel is active. These settings are independent of the **Cisco Secure Client** proxy settings configured in Step 4 of the Add VPN Profiles Step 4 – Cisco Secure Client Configuration on page 1140 procedure, which specifically govern the client's VPN connection.



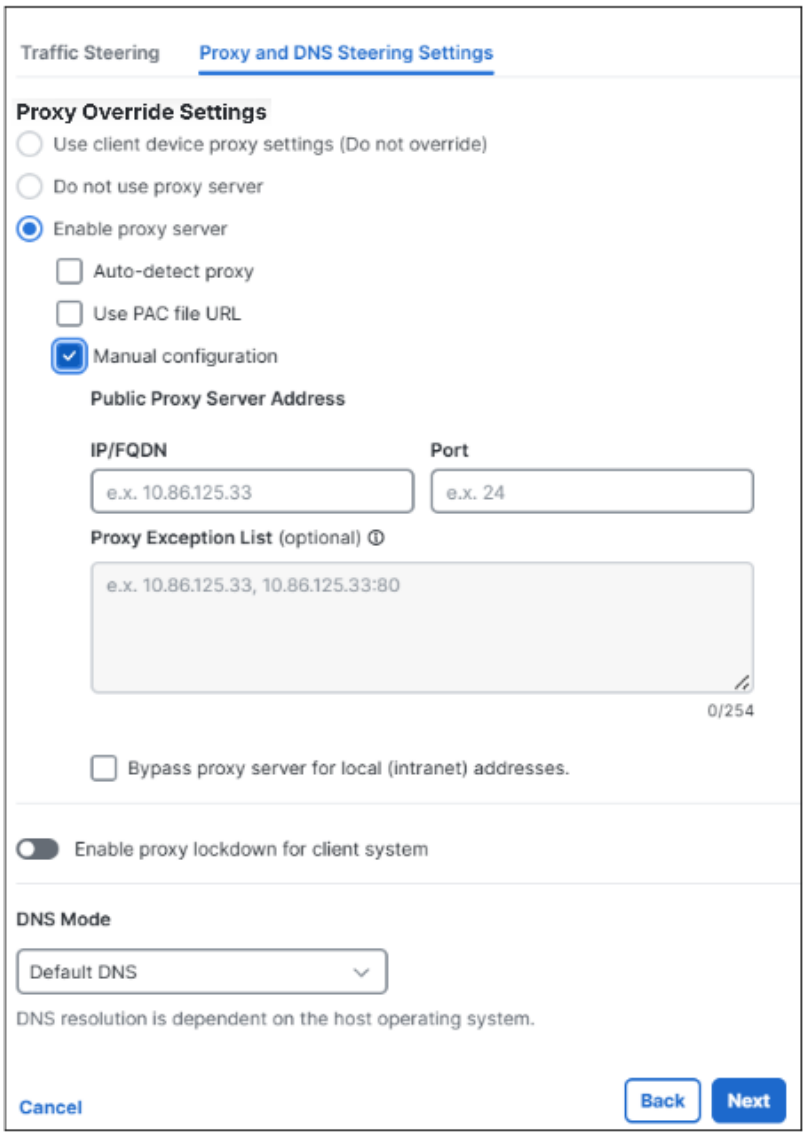
2. When **Enable proxy server** is chosen, the following proxy server settings options are displayed. Choose the required settings:
   - **Auto-detect proxy**: Check this box to specify the URL where the Proxy Auto-Configuration (PAC) file is located.
   - **Use PAC file URL**: Check this box to provide the PAC file URL.
   - **Manual configuration**: Check this box to manually define a proxy server to be used by all client devices for HTTP traffic. Then, configure the following:
     - **Public Proxy Server IP**: Enter the IP address or hostname of the public proxy server and specify the port.

> **Note**
>
> The combined length of the hostname and port cannot exceed 100 characters.

- **Proxy Exemption List (optional)**: Add host/port combinations that should bypass the proxy. Enter the public proxy server address before adding exceptions.

> **Note**
>
> You must enter the public proxy server address before adding exceptions.

> **Note**
>
> To bypass the proxy for local addresses, check the **Bypass Proxy Server for Local (Intranet) Addresses** checkbox.



3. (Optional) Use the **Enable Proxy Lockdown for Client System** toggle button to activate proxy lockdown for the client system.

4. For **DNS Mode**, choose one of the following:
   - **Default DNS**: This is the system-provided DNS option. All traffic is resolved with the default DNS server configured during the connector deployment stage.
   - **Tunnel all DNS**: Route all DNS traffic over the encrypted VPN connection.
   - **Split DNS**: Route DNS names are matched over the local physical interface. Names that do not match are handled through the VPN connection.
5. Click **Next** to configure the Cisco Secure Client.

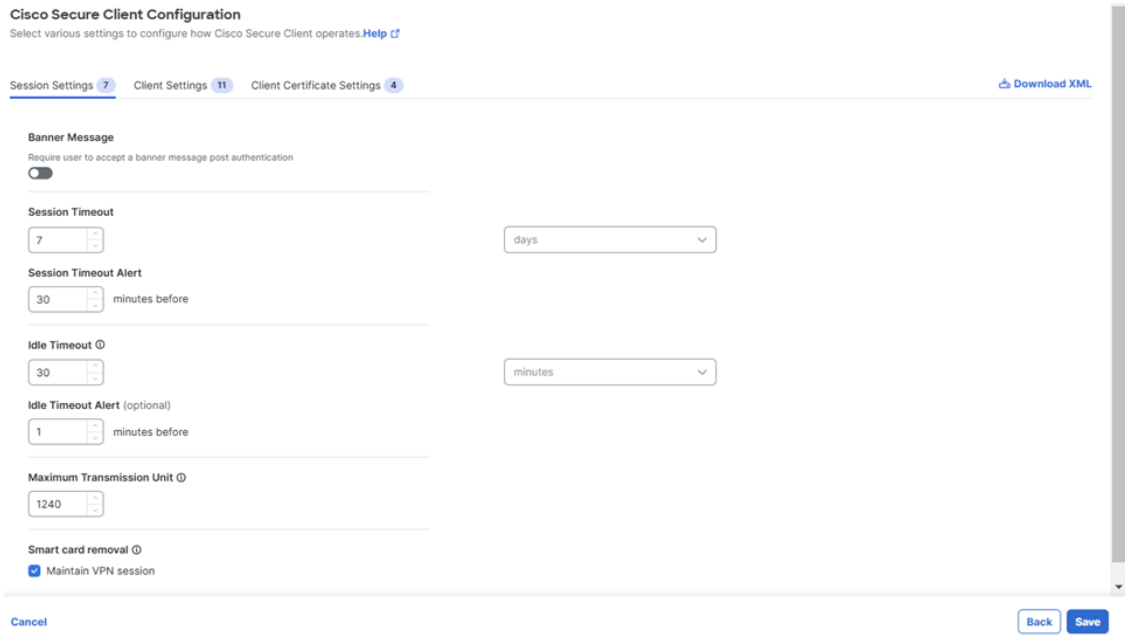
Add VPN Profiles Step 4 – Cisco Secure Client Configuration

Provides instructions for completing the Add VPN Profiles Step 4 - Cisco Secure Client Configuration workflow in Cisco Secure Access. You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN profile.

You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN profile.

Procedure

1. Click the **Session Settings** tab to modify session-specific settings:

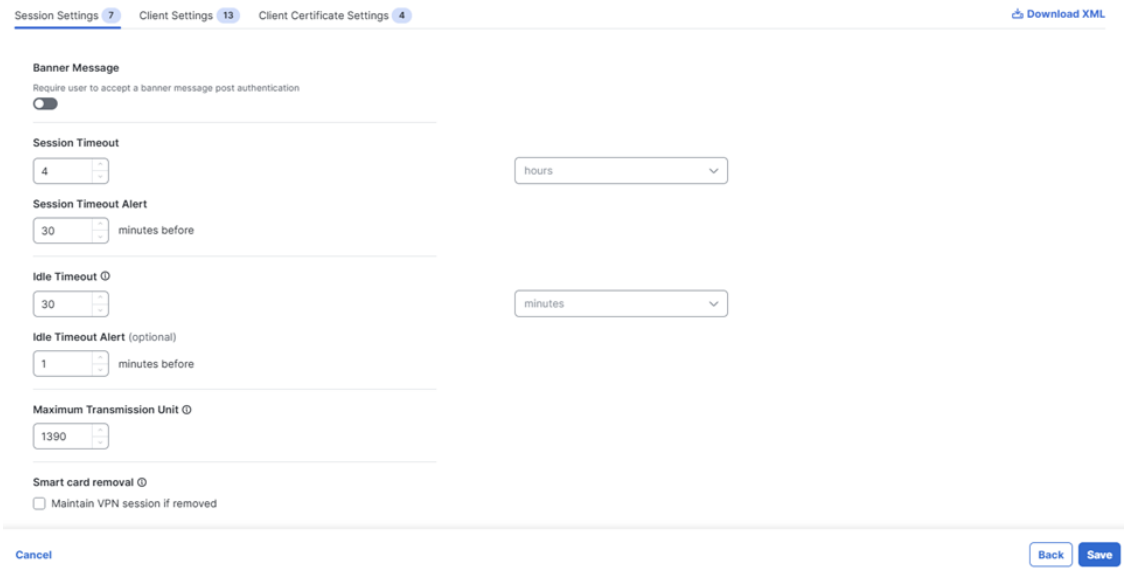


   - **Banner Message**–Configure a banner message for the user to accept after Secure Client authentication.
   - **Session Timeout**–Configure a time window after which the Secure Client session will end. The default is 4 hours.
   - **Session Timeout Alert**–Configure the number of minutes before the session timeout to alert the user. The default is 30 minutes.
   - **Idle Timeout** – Configure a time window for an idle Secure Client session, after which the session will end.

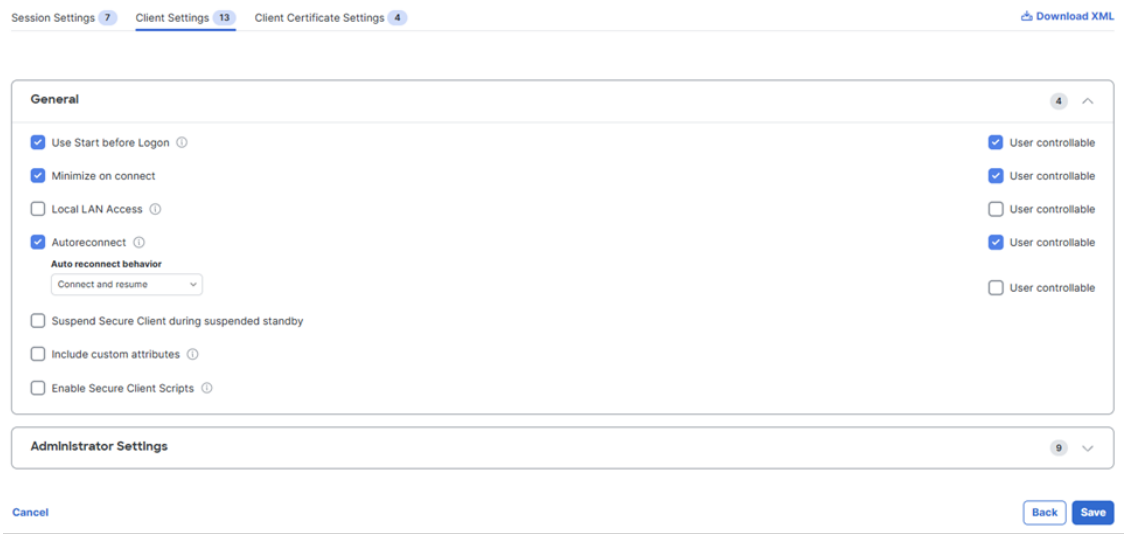
> **Note**
>
> This value affects the Disconnected Timeout configuration in your Cisco AnyConnect settings; which determines when AnyConnect/Secure Client ceases reconnect attempts since the session to the ASA has been interrupted.

- **Idle Timeout Alert**–Configure the number of minutes before the idle session timeout to alert the user. The default is 1 minute.
- **Maximum Transmission Unit (MTU)**–Configure the largest packet size that can be transmitted through the VPN tunnel before fragmentation. Accepts a value between 576 and 1390.
- **Smart card removal**–Check **Maintain VPN session** to continue the VPN connection in the event of a smart card removal. Otherwise the VPN connection is terminated when a smart card is removed.

2. Click the **Client Settings** tab then click **Edit** to modify client-specific sessions. See The Cisco Secure Client Profile Editor for complete information about Cisco Secure Client settings.
   a. Modify **Session Settings** as needed.

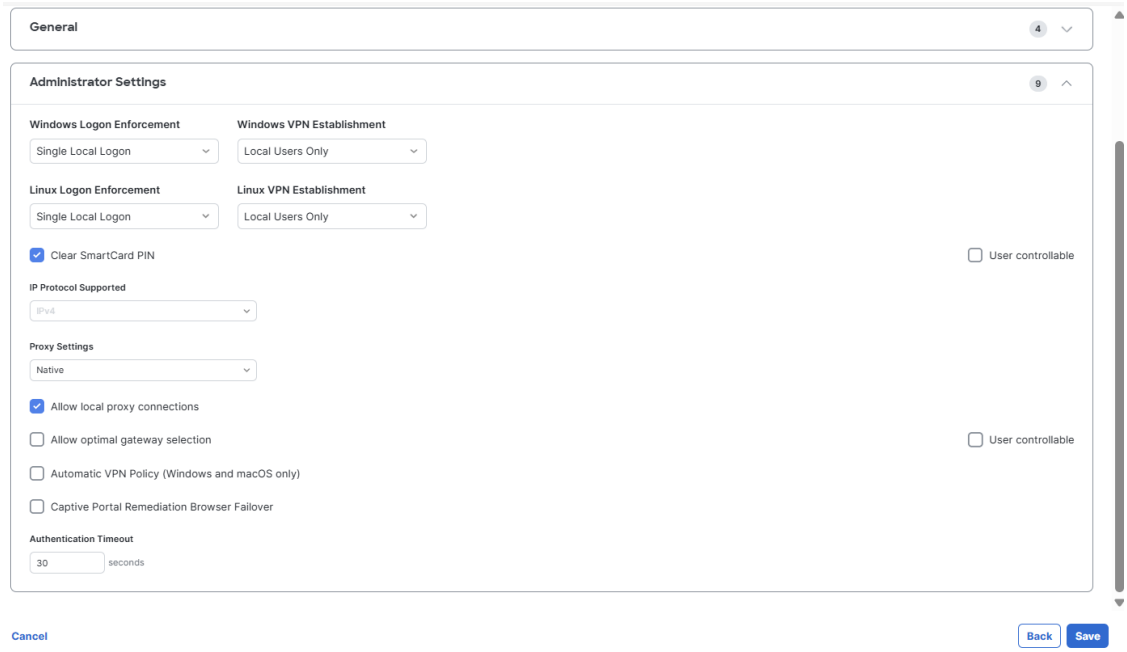


   b. Modify **Client Settings (General)** as needed.



> **Note**
>
> **Local LAN Access** allows the user complete access to the local LAN connected to the remote computer during the VPN session to Secure Access. If enabled, **Local LAN Access** requires a traffic steering exception configured for IP range `0.0.0.0/32`. For more information, see Step 3a - Traffic Steering (Split Tunnel).

c. Configure a time window for an idle Secure Client session, after which the session will end. Note: This value affects the Disconnected Timeout configuration in your Cisco AnyConnect settings; which determines when AnyConnect/Secure Client ceases reconnect attempts since the session to the ASA has been interrupted. Modify **Client Settings (Administrator)** as needed.



- **Windows Logon Enforcement**–Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session.
- **Windows VPN Establishment**– Determines how Cisco Secure Client behaves when a user remotely logs on to the client PC and establishes a VPN connection.

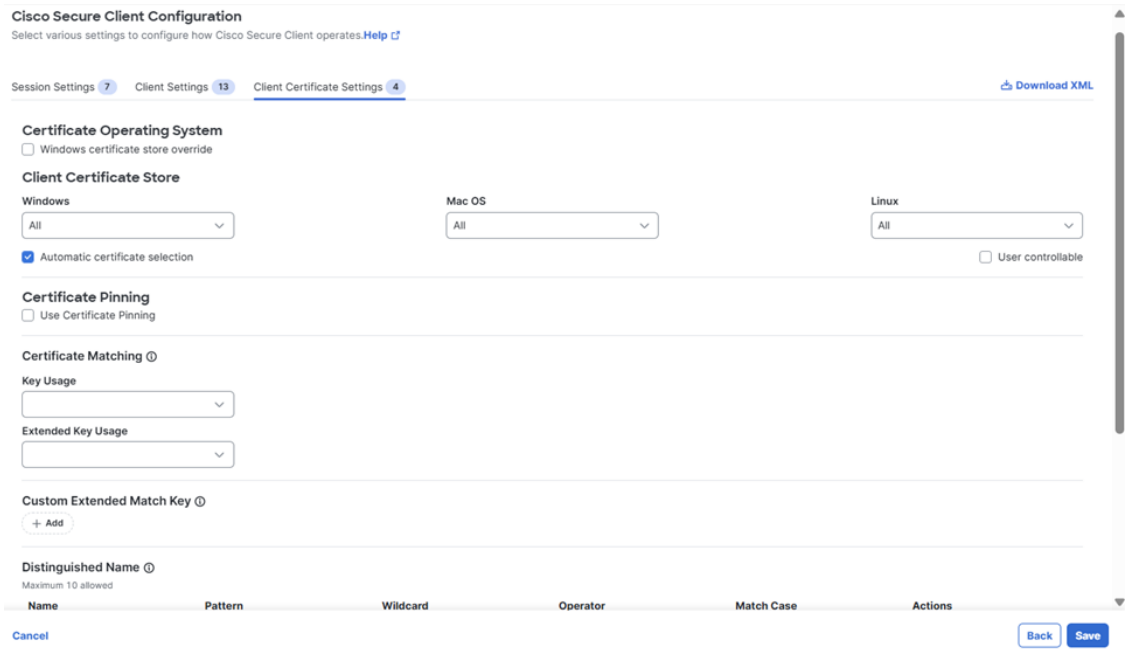
- **Linux Logon Enforcement**– Allows a VPN session to be established from an SSH session.
- **Linux VPN Establishment**– Determines how Cisco Secure Client behaves when a user logs on to the client PC using SSH and establishes a VPN connection.
- **IP Protocol Supported**–Cisco Secure Client decides which IP version to use, IPv4 or IPv6, when connecting to Secure Firewall ASA.
- **Proxy Settings**–Specifies a policy in the Cisco Secure Client profile to control access to a proxy server. Use this when a proxy configuration prevents a tunnel from being established outside the corporate network.
- **Authentication Timeout Values**–Defines the number of seconds the client waits for an authentication response after sending user credentials. Enter a number from 10 to 120.

> **Note**
>
> To enable and configure the **Always-On** operation, which prevents access to Internet resources without a server certificate when the computer is not on a trusted network (unless a VPN session is active), check the **Automatic VPN Policy** option, then scroll down and check the **Always on VPN** option, optionally.

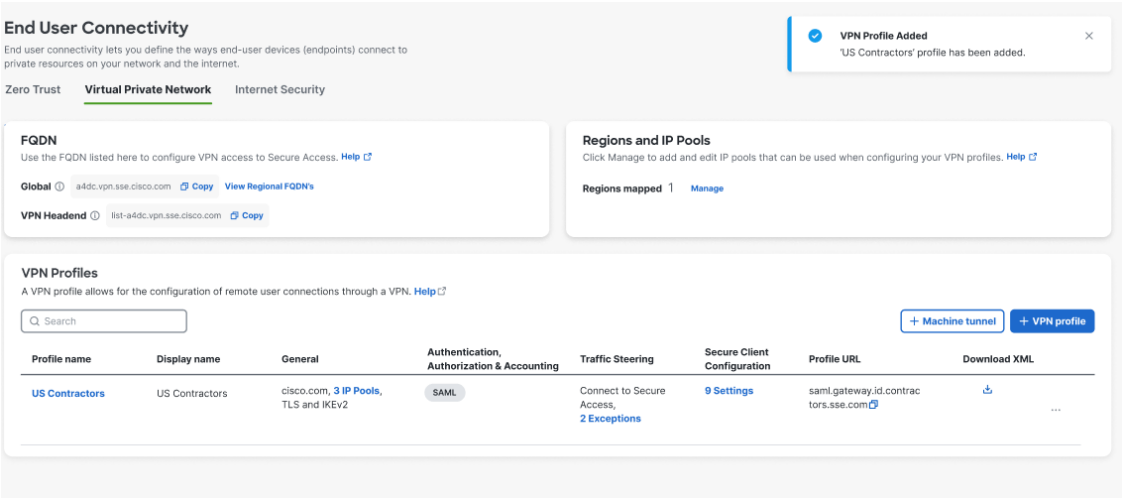
Automatic VPN Policy (Windows and macOS only)–Enables Trusted Network Detection allowing Cisco Secure Client to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

Accessible hosts with VPN disconnected: Enables endpoints to access the configured hosts while VPN is disconnected during Always On. Values are a comma-separated list of hosts which can be specified IP addresses, IP address ranges (CIDR format), or FQDNs. A maximum of 500 hosts are allowed, and wildcards are not supported.

3. Click **Save**.
4. Modify any **Client Certificate Settings** as needed.



5. Click **Save** to complete the VPN Profile.



Import ASA Device Configuration Files for Remote Access VPN

Describes Import ASA Device Configuration Files for Remote Access VPN in Cisco Secure Access. The remote access VPN Migration tool facilitates the transfer of remote access VPN configurations from your current firewall solution to the cloud-based Cisco Secure Access VPNaaS environment that provides enhanced security, centralized management, and scaling capabilities.

The remote access VPN Migration tool facilitates the transfer of remote access VPN configurations from your current firewall solution to the cloud-based Cisco Secure Access VPNaaS environment that provides enhanced security, centralized management, and scaling capabilities. As part of the migration process, the configuration file from your device is seamlessly translated into a Secure Access policy to recreate the remote access VPN configuration and minimize downtime.

Check the following required prerequisites and configurations before you import any ASA configuration files with this tool.

Prerequisites

Ensure the following prerequisites are established before you import a configuration file from your ASA device:

- Full admin access to the Secure Access dashboard.
- ASA Device with Remote Access VPN Configuration(s).

Supported Functionality

The following certificate authentication methods are supported with this import tool:

- SAML + Cert Authentication
- SAML-only Authentication
- RADIUS + Cert Authentication
- Radius-only Authentication
- Certificate-only Authentication

The following functionality is supported with this migration tool:

- Group policy
- Network Objects (split and full tunneling)

> **Warning**
>
> Nested network objects within a network object group may cause an error during the procedure.

- ACL redirect
- Custom attributes:
  - Per App VPN
  - Bypass Virtual Subnets
  - Split Exclude Failover
- SSL/IPsec settings
- IPsec/SSL VPN groups
- DNS server assignment
- Radius Servers with dedicated management platforms
- Radius Server Assignments
- CA Certificates
- Full support for VPN profile configurations

> **Note**
>
> The import function described here does **not** include upgrades for your Cisco Secure Client. As of the publication of this note you must upgrade the Client through the ASDM dashboard. See Migrate AnyConnect Host Scan Migration 4.3.x to 4.6.x and Later for more information.

Import an ASA Configuration to Secure Access Remote Access VPN Profile

Provides instructions for completing the Import an ASA Configuration to Secure Access Remote Access VPN Profile workflow in Cisco Secure Access. If you happen to log out or navigate away from the screen at any point after starting the import process, your progress is saved.

If you happen to log out or navigate away from the screen at any point after starting the import process, your progress is saved.

Use this procedure to import the ASA configuration file from a standalone ASA device to Secure Access. Complete the following procedure to migrate your existing remote access VPN tunnels from the ASA firewall to Secure Access and set up the settings in the resulting VPN profile.

> **Note**
>
> This procedure is for generating a VPN profile in Secure Access from an existing ASA remote access VPN configuration, not for creating a new profile independently.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. In the VPN Profiles section of the window select **Import from ASA**.
3. In the **Import from ASA** page, examine the **Upload ASA Configuration and XML Files** section of the window. Download the configuration file with either the ASDM dashboard or CLI and then drag one (or more) configuration files from your local device and drop it into the box or click inside the box and navigate to it when prompted.

   > **Note**
   >
   > Note that the files must be a maximum of 10 MB. The VPN XML profile can be obtained from the VPN endpoint in the Secure Client folder, with the exact location depending on your operating system. Refer to the "Locations to Predeploy the Cisco Secure Client Profiles" chapter of the Cisco Secure Client Administrator Guide, Release 5.1 for detailed folder locations.

   - We **strongly** recommend using the ASDM dashboard to upload the configuration. To download the ASA configuration file with ASDM, see Download an ASA Configuration File with ASDM on page 1147.
   - To download the ASA configural with CLI, see Download an ASA Configuration File with CLI on page 1147
   - To download the ASA XML file, see Download the ASA XML File on page 1148.

4. The status of the upload is visible in the upper right corner of the **Upload ASA Configuration and XML Files** window and the status of the file upload.

   > **Note**
   >
   > If a file fails to upload, confirm the file size is smaller than 10 MB and is a supported filetype. At this time only `.cfg` and `.xml` files are supported.

5. Click **Next**.
6. In the **Review Imported Objects** window, review and modify the list of servers and server groups (DNS servers, Radius Groups, Client Authentication certificates, and network objects and object groups) that get imported as part of the import. These items must be error-free to continue. Use the edit or delete icons for the corresponding entry that needs to be corrected and resolve any issues. Note that some objects may have errors due to incompatible or duplicate naming conventions.

> **Warning**
>
> Nested network objects within a network object group may cause an error. If you experience this issue, delete the affected network object groups from the list of objects to review and export your device configuration as a CSV file. Upload this file in the **Resources** > **Network and Service Objects** page and continue with this procedure.

7. Click **Next**
8. In the **Prerequisites** window, click **+Add Region** to create a new region and map the DNS Servers and radius group that was imported as part of the prevous step. If desired, expand the **DNS Servers** drop-down menu to opt to select "Imported from ASA" as your DNS selection.
9. **Save** the region and IP pool and click **Next**.
10. In the **Edit and Import Configuration Files** window, review the VPN profiles detected in the configuration files you uploaded.

> **Note**
>
> You cannot proceed if the imported VPN profiles have an incomplete status. Click the **edit** icon to edit the VPN profile configuration where prompted. See General Settings, Authentiation Authorization and Accounting, and Traffic Steering (Split Tunnel) for more information.

11. Click **Save**. You are redirected to the **Connect** > **End User Connectivity** > **Virtual Private Network** page.

Download an ASA Configuration File with ASDM

Provides instructions for completing the Download an ASA Configuration File with ASDM workflow in Cisco Secure Access. We strongly recommend this method of downloading an ASA configuration file.

We **strongly** recommend this method of downloading an ASA configuration file. If you don't have ASDM installed already, see Cisco ASA General Operations ASDM Configuration Guide and install it prior to the steps in the proocedure below.

If you must use CLI to upload the configuration file, see Download an ASA Configuration File with CLI on page 1147.

Procedure

---

1. Open the ASDM dashboard and enter the IP or FQDN of the ASA, and a username and password for the admin account.
2. In the ASDM dashboard, navigate to **Tools** > **Backup Configuration** and uncheck all options but **Running Configuration**.
3. Click **Browse Local** and select where to save this file locally. Click **Select File** and then Backup. The file is saved as `running-config.cfg`.

What to do next

Download the ASA XML file before you continue with the remainder of the procedure.

Download an ASA Configuration File with CLI

Provides instructions for completing the Download an ASA Configuration File with CLI workflow in Cisco Secure Access. The preferred method of downloading an ASA configuration file is with the ASDM dashboard.

The preferred method of downloading an ASA configuration file is with the ASDM dashboard.

For users who opt for the CLI method of downloading,follow the procedure below. See Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.19 for more information about CLI commands in ASA devices.

> **Note**
>
> Be sure to identify the correct profile in the procedure below; the VPN XML profiles are specified as AnyConnect client profiles and could be mistaken as non-XML files.

Procedure

1. Open an SSH Client like Putty and then enter the IP/FQDN of the ASA and the username/ password of an account with admin privileges.
2. Execute the enable command and enter the admin password if prompted.
3. Enter the `show running-config` command to display the actively running configuration.
4. Manually copy the entire output and save it locally.

What to do next

Download the ASA XML file before you continue with the remainder of the procedure.

Download the ASA XML File

Describes Download the ASA XML File in Cisco Secure Access. The VPN XML profile can be obtained from the VPN endpoint in the Secure Client folder, with the exact location depending on your operating system.

The VPN XML profile can be obtained from the VPN endpoint in the Secure Client folder, with the exact location depending on your operating system. Refer to the "Locations to Predeploy the Cisco Secure Client Profiles" chapter of the Cisco Secure Client Administrator Guide, Release 5.1 for detailed folder locations.

Choose **one** of the following procedures to download the XML file from your ASA device. Do not do both procedures.

Download the ASA XML File with ASDM

1. Log into the ASDM dashboard.
2. Navigate to **Configuration** > **Remote Access** > **Network (Client) Access** > **Secure Client Profile.** to identify the correct locations and filenames.
3. Check the Profile Location column and ensure the Profile Usage is set to AnyConnect VPN Profile.
4. Navigate to **Tools** > **File Management**.
5. At the top, select **File Transfer**, then choose **Between Local Device** and **Flash**.
6. On the left, select the directory where you want to export the file.
7. On the right, select the appropriate VPN XML profile file as identified above.
8. Click the left arrow button in the center to transfer the file.
9. Complete the upload wizard with step 4.

Download the ASA XML File with CLI

1. Open an SSH Client like Putty and then enter the IP/FQDN of the ASA and the username/ password of an account with admin privileges.
2. Run the command `show running-config webvpn`.
3. Locate the Anyconnect profiles subcommand; note that the command needs to include both the location and the filename . For example, if you see `anyconnect profiles VPN_Profile disk0:/secure_client_profile.xml` then **disk0:/secure_client_profile.xml** is the file you need., where "disk0:/" is the location and "secure_client_profile.xml" is the filename.
4. Display the file with the `more [profile location]:/[name].xml` command.
5. Copy the output and save it as a .xml file. Do not include command prompt when you copy.
6. Complete the upload wizard with step 4.

Manage VPN Settings

Describes Manage VPN Settings in Cisco Secure Access. Administrators can prevent end users from manually entering any VPN headend on the Cisco Secure Client by unchecking the Allow Manual Host Entry check box.

Administrators can prevent end users from manually entering any VPN headend on the Cisco Secure Client by unchecking the **Allow Manual Host Entry** check box. This ensures that end users can only select the VPN headend explicitly defined in the VPN profile configuration, thereby helping to prevent any risk of data exfiltration. Note that enabling this option also allows your remote access VPN configuration to process traffic that would otherwise be dropped due to the DF Bit setting on your system. For example, if a device's MTU is higher than the VPN headend's effective MTU, meaning the device is configured to process a maximum byte-size a data packet can be and the VPN has a smaller MTU size, packets that do not match the VPN headend size are dropped despite the device's MTU allowance. With this option, packets are fragmented and processed within the range of the VPN.

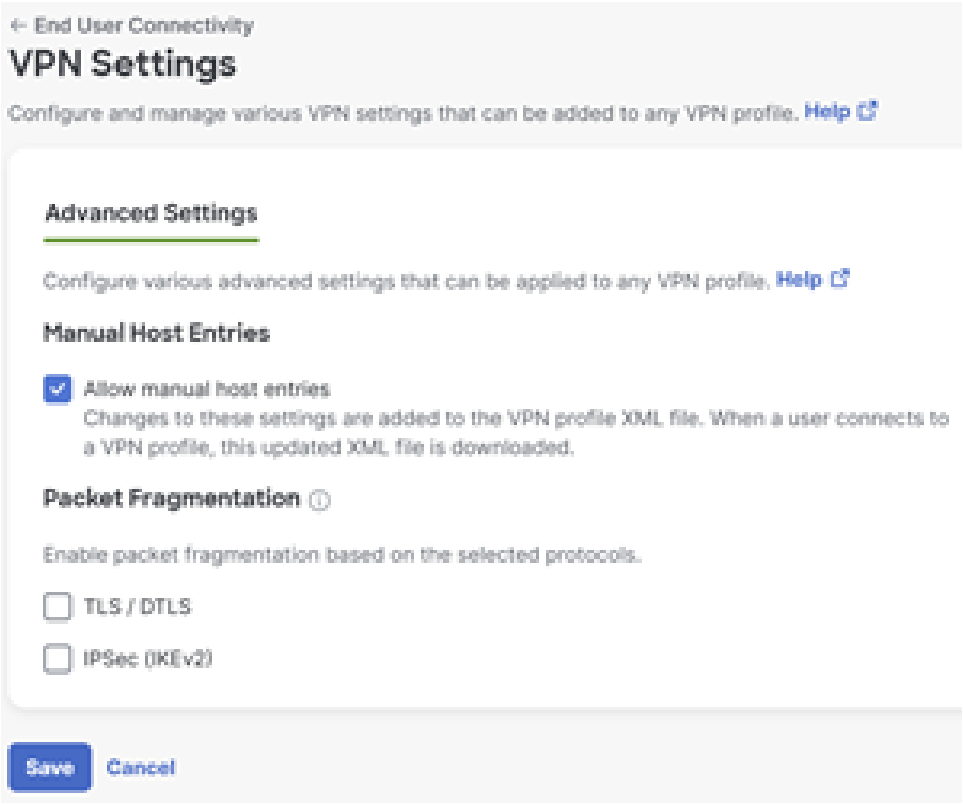
Manage Manual Host Entries for VPN Profiles

Provides instructions for completing the Manage Manual Host Entries for VPN Profiles workflow in Cisco Secure Access. This setting applies to all VPN profiles crated for the current organization.

This setting applies to all VPN profiles crated for the current organization. To restrict or allow end users from manually creating any unsolicited VPN profiles, perform the following steps:

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. In the VPN Profiles section, click **Settings** and then select **VPN Settings**.
3. View the **Allow manual host entries** option. To restrict manual host entries from end users, uncheck this option. To allow manual host entries from end users and allowing fragmentation for packets that are larger than the VPN headend value, leave this option checked and proceed to the next step.



4. If you have "Manual Host Entries" enabled, check the appropriate **Packet Fragmentation** protocols this option is applied to once deployed. Allowing fragmentation at this level breaks down packets that are too large for the VPN headend's configured MTU for analysis instead of dropping them.
5. Click **Save**.

Manage Machine Tunnels

Machine tunnels ensure connectivity to the corporate entwork whenever the client system is powered up, whether or not a VPN connection has been established.

A Secure Access VPN machine tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts that require corporate network connectivity also benefit from this feature. For this tunnel to be created without user interaction, certificate-based authentication is used.

About the VPN Machine Tunnel

The Secure Access machine tunnel allows administrators to have the Cisco Secure Client connected without user intervention prior to when the user logs in. Secure Access machine tunnel is triggered when the endpoint is off-premises and disconnected from a user-initiated VPN. The Secure Access VPN machine tunnel is transparent to the end user and disconnects automatically when the user initiates VPN.

The Secure Client VPN agent service is automatically started upon system boot-up. The Secure Client VPN agent uses the VPN profile to detect that the machine tunnel feature is enabled. If the machine tunnel feature is enabled, the agent launches the management client application to initiate a machine tunnel connection. The management client application uses the host entry from the VPN profile to initiate the connection. Then the VPN tunnel is established as usual, with one exception: no software update is performed during a machine tunnel connection since the machine tunnel is meant to be transparent to the user.

The user initiates a VPN tunnel via the Secure Client, which triggers the machine tunnel termination. Upon machine tunnel termination, the user tunnel establishment continues as usual.

The user disconnects the VPN tunnel, which triggers the automatic re-establishment of the machine tunnel.

For information about viewing connection events filtered by machine tunnel, see View the Remote Access Log Report.

Limitations

- User interaction is not supported.
- Certificate-based authentication through Machine Certificate Store (Windows) is only supported.
- Strict Server Certificate checking is enforced.
- A private proxy is not supported.
- A public proxy is not supported (ProxyNative value is supported on platforms where Native Proxy settings are not retrieved from the browser).
- Secure Client Customization Scripts are not supported.

Add a Machine Tunnel and Configure General Settings

Provides instructions for completing the Add a Machine Tunnel and Configure General Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

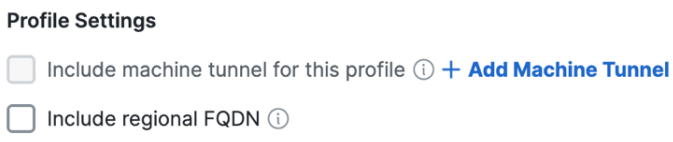
This section describes how to configure Secure Access as the VPN gateway and accept connections from the Secure Client through the VPN machine tunnel.

Before you begin

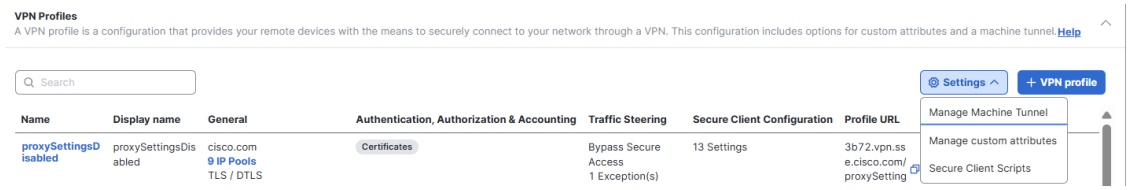
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Navigate to **VPN Profiles** and configure the general settings for the machine tunnel.
   a) Click **+VPN profile**, navigate to **Profile Settings**, and then click **+Add Machine Tunnel**.



   b) Click **Settings**, and then choose **Manage Machine Tunnel** from the drop-down.



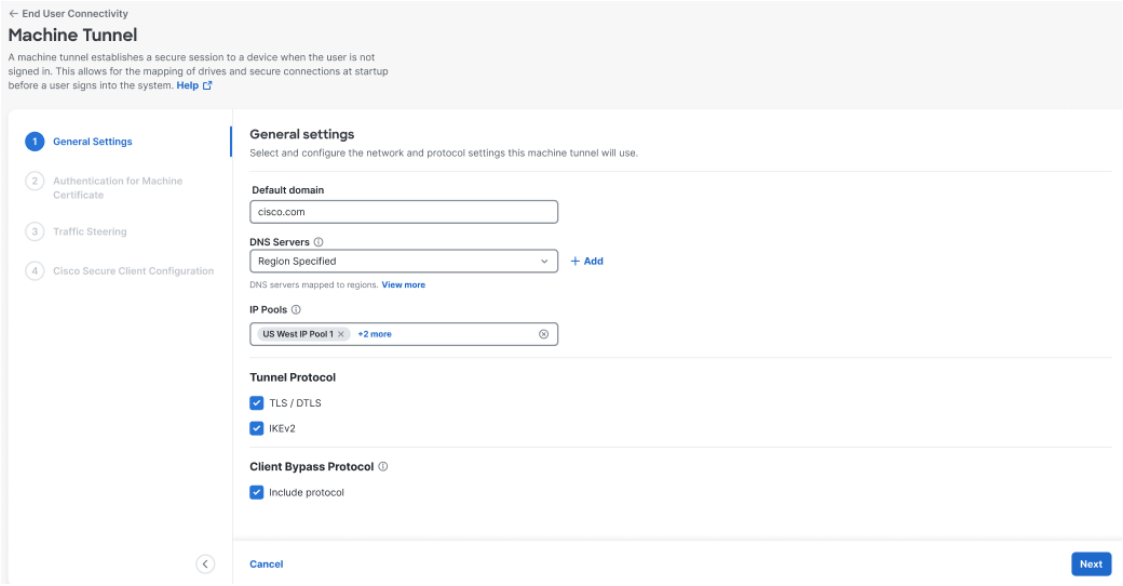
3. Enter the **Default domain**.
4. The **DNS Server** mapped through the **Manage Regions and IP Pools** page is set as the default server. You can accept the default DNS server, choose another DNS server from the drop-down, or click **+ Add** to add a new DNS server pair. Selecting another DNS server or adding a new DNS server overwrites this default server.

5. Select one IP pool per region from the **IP Pools** drop-down. VPN profiles must have at least one IP pool assigned in each region for a valid configuration.
6. Select the **Tunnel Protocol** that this machine tunnel will use.

> **Note**
>
> Select at least one protocol.

   - TLS/DTLS
   - IPSec (IKEv2)

7. Optionally, check **Include protocol** to enforce client bypass protocol.



Configure Authentication for Machine Certificate

Provides instructions for completing the Configure Authentication for Machine Certificate workflow in Cisco Secure Access. The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session.

The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session. For this tunnel to be created without user interaction, certificate-based authentication is used.

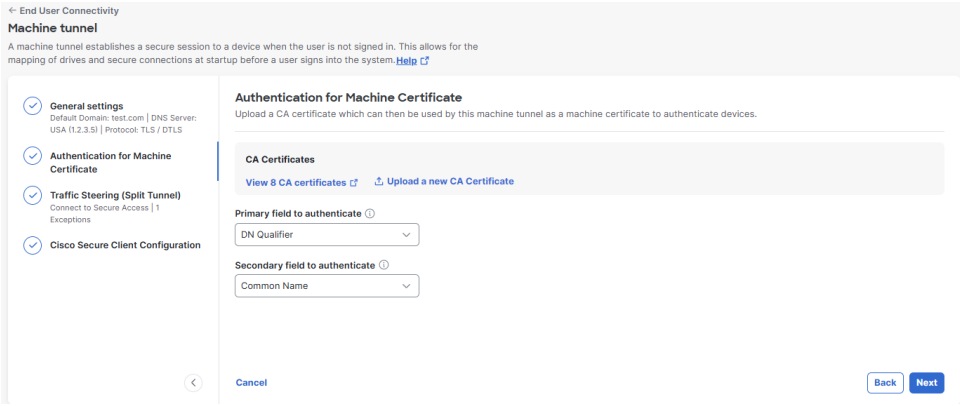
Set up the authentication for the machine certificate.

Procedure

1. Choose CA certificates from the list or click **Upload CA certificates**.

   These certificates can be used by the machine tunnel as a machine certificate to authenticate devices.

   Upload your organization's signed CA root certificate. For more information, see VPN Certificates for User and Device Authentication.



2. Select the certificate-based authentication fields.
   a) For **Primary field to authenticate**, choose the certificate field that contains the device name (computer name).

      Secure Access uses the device name as the machine tunnel identifier. The format of the computer name must match the format of the chosen device identifier. For more information, see Authenticate Device Identity with Active Directory.

   b) (Optional) For **Secondary field to authenticate**, choose a secondary attribute to authenticate to Active Directory endpoint devices.

      You cannot choose the same value for the primary and secondary authentication fields.

3. Click **Next**.

Configure Traffic Steering (Split Tunnel)

Provides instructions for completing the Configure Traffic Steering (Split Tunnel) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

For **Traffic Steering (Split Tunnel)**, you can configure a machine tunnel to maintain a full tunnel connection to Secure Access, or configure it to use a split tunnel connection to direct traffic through the VPN only if necessary.

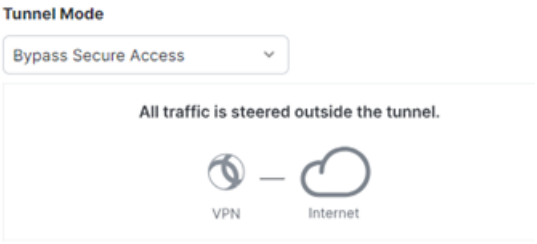
Procedure

---

1. For **Tunnel Mode**, choose either:
   - **Connect to Secure Access** to direct all traffic through the tunnel; or,



   - **Bypass Secure Access** to direct all traffic outside the tunnel.



2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel.
   a) Click **+Add**.
   b) In the search bar, enter the name of a Network Object or a Network Object Group in the search bar, click **Select sources** and then select the same on the **Select sources tab**.
   c) Click the **Add a source**, and then enter comma-separated IPs, domains, and network spaces.
   d) Click **Save**.
3. For **DNS Mode**, you can accept the default mode or, depending on your selection, choose to **Tunnel all DNS** traffic or **Split DNS** traffic.

   When **Split DNS** is chosen, DNS names matching the configured **DNS Names** will be routed over the encrypted Secure Client connection for resolution. Any that do not match the configured **DNS Names** are routed via the local physical interface for the resolution.

   > **Note**
   >
   > At this time, **Split DNS** is only available for **Bypass Secure Access** tunnel mode.

4. Click **Next**, and then configure the Cisco Secure Client.

Define the Cisco Secure Client Configuration

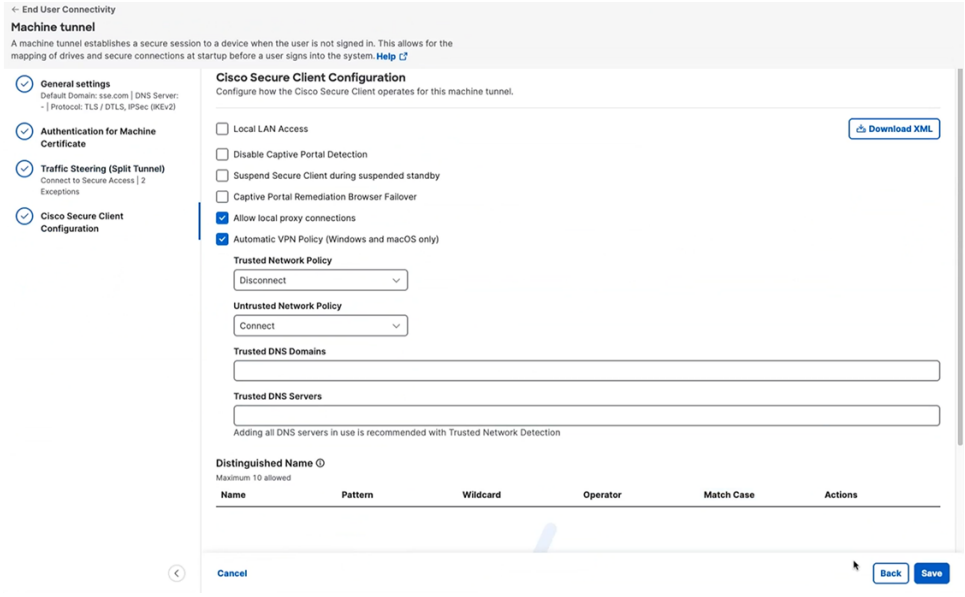
Provides instructions for completing the Define the Cisco Secure Client Configuration workflow in Cisco Secure Access. Review the options presented on the Cisco Secure Client Configuration tab.

You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN machine tunnel.

Procedure

---

1. Review the options presented on the **Cisco Secure Client Configuration** tab.



2. Configure the options that are specific to your machine tunnel.

   - **Local LAN Access**–Allows the user complete access to the local LAN connected to the remote computer during the VPN session to Secure Access.

     > **Note**
     >
     > Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network.

   - **Disable Captive Portal Detection**–When Cisco Secure Client receives a certificate with a common name that does not match the Secure Access name, a captive portal is detected. This behavior prompts the user to authenticate. Some users using self signed certificates may want to enable connection to corporate resources behind an HTTP captive portal and should thus mark the **Disable Captive Portal Detection** checkbox. The administrator can also determine if they want the option to be user configurable and mark the checkbox accordingly. If user configurable is selected, the checkbox appears on the Preferences tab of the Cisco Secure Client UI.
   - **Suspend Secure Client during suspended standby**– (Windows Only) Available only for devices that support Connected Standby. During Connected Standby, the operating system throttles system process, which can impact how packets are processed. With this option, you can disable VPN traffic when the system enters Connected Standby mode. The feature is disabled by default.
   - **Captive Portal Remediation Browser Failover**–Allows the end user to use an external browser (after closing the Cisco Secure Client browser) for captive portal remediation.
   - **Allow Local Proxy Connections**–By default, Cisco Secure Client lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network components on some antivirus software.
   - **Automatic VPN Policy (Windows and macOS only)**–Enables Trusted Network Detection allowing Cisco Secure Client to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

- **Trusted Network Policy**–Action Cisco Secure Client automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
  - Disconnect (Default)–Disconnects the VPN connection upon the detection of the trusted network.
  - Connect–Initiates a VPN connection upon the detection of the trusted network.
  - Do Nothing–Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - Pause–Cisco Secure Client suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, Cisco Secure Client resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
- **Untrusted Network Policy**–Cisco Secure Client starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
  - Connect (Default)–Initiates the VPN connection upon the detection of an untrusted network.
  - Do Nothing–Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
- **Trusted DNS Domains**–DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *".cisco.com*.

  Note

  Wildcards *('*')* are **not** supported for DNS suffixes.

- **Trusted DNS Servers**–DNS server addresses (IP addresses separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1.

  Note

  Wildcards *('*')* are **not** supported for DNS server addresses.

Distinguished Name–Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates. When you add multiple Distinguished Names, each certificate is checked against all entries, and all of them must match.

Note

A maximum of 10 distinguished names are allowed.

- **Name**–The distinguished name (DN) to use for matching:
  - CN–Subject Common Name
  - C–Subject Country

- DC–Domain Component
- DNQ–Subject Dn Qualifier
- EA–Subject Email Address
- GENQ–Subject Gen Qualifier
- GN–Subject Given Name
- I–Subject Initials
- L–Subject City
- N–Subject Unstruct Name
- O–Subject Company
- OU–Subject Department
- SN–Subject Sur Name
- SP–Subject State
- ST–Subject State
- T–Subject Title
- ISSUER-CN–Issuer Common Name
- ISSUER-DC–Issuer Component
- ISSUER-SN–Issuer Sur Name
- ISSUER-GN–Issuer Given Name
- ISSUER-N–Issuer Unstruct Name
- ISSUER-I–Issuer Initials
- ISSUER-GENQ–Issuer Gen Qualifier
- ISSUER-DNQ–Issuer Dn Qualifier
- ISSUER-C–Issuer Country
- ISSUER-L–Issuer City
- ISSUER-SP–Issuer State
- ISSUER-ST–Issuer State
- ISSUER-O–Issuer Company
- ISSUER-OU–Issuer Department
- ISSUER-T–Issuer Title
- ISSUER-EA–Issuer Email Address

3. Click **Save**.

What to do next

You need to associate the machine tunnel with remote access VPN for users and their devices.

- Establish a machine tunnel VPN using certificate-based authentication against device identities from Active Directory. For more information, see Authenticate Device Identity with Active Directory.

Authenticate Device Identity with Active Directory

Describes Authenticate Device Identity with Active Directory in Cisco Secure Access. Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs).

Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs). Once integrated with Secure Access, you can protect and monitor the connections for the users and devices to internet and private destinations by configuring Access rules in the organization's policy.

Note

We recommend you use certificate-based authentication to register device identities with Active Directory.

Configure Active Directory Endpoint Device Management

Provides instructions for completing the Configure Active Directory Endpoint Device Management workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Active Directory integration in Secure Access includes the option to provision endpoint devices from an on-premise Active Directory domain controller (DC).

Before you begin

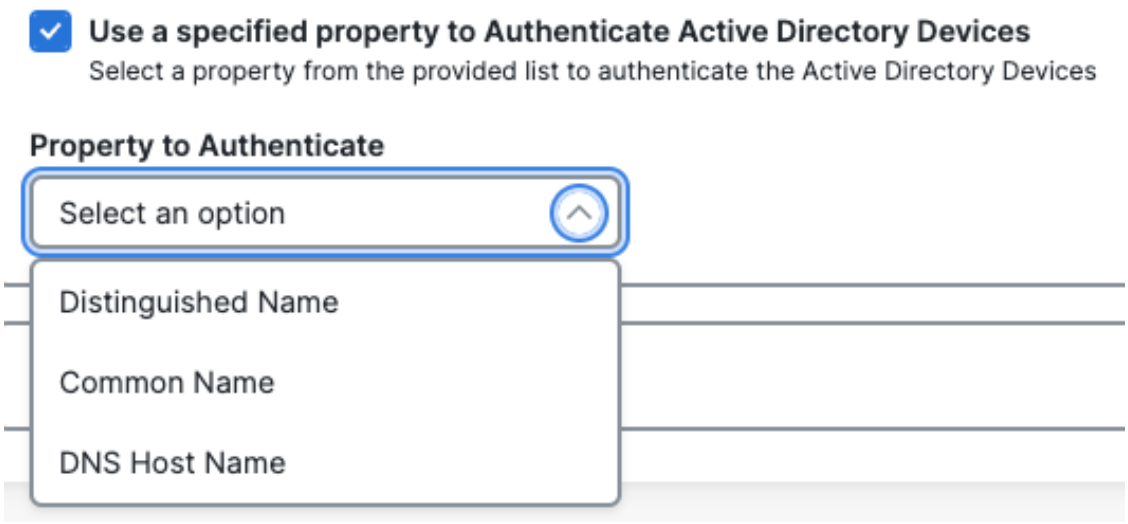
- Full Admin user role. For more information, see Manage Accounts.
- Endpoint device integration requires devices provisioned by an on-premise Active Directory domain controller (DC) and Cisco AD Connector version 1.14.4 or newer. For more information, see Connect Active Directory to Secure Access and Configure Updates on AD Connector.
- A configured machine tunnel applied to a VPN profile. For more information, see Manage Machine Tunnels.

Note

Make a note of the primary attribute for Active Directory certificate-based authentication. For more information, see Add a Machine Tunnel.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and click **Configuration management**.
2. On the **Configurations** tab, navigate to **Directories**, and then expand **Active Directory**.
3. Check the box at the bottom of your Active Directory integration menu to **Use a specified property to Authenticate Active Directory Devices**.



4. Select a **Property to Authenticate** from the list of Active Directory machine attributes for certificate-based authentication.

   Secure Access supports the **Distinguished Name**, **Common Name**, and **DNS Host Name** attributes. For more information see, Manage Machine Tunnels.

   When selecting the **Property to Authenticate** option, we recommend:

   - For the computer names in the FQDN format, choose **DNS Host Name**.
   - For the computer name in the short-format, choose **Common Name**.

5. After making changes to the AD integration, restart the AD Connector to trigger a full synchronization of AD Users, Groups, and Endpoint Devices.

   For more information, see Restart the Active Directory Connector.

What to do next

Secure Access has a single Access policy, which consists of policy rules and settings. Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization.

Secure Access supports configuring security controls for sources and destinations (resources) on private and internet access rules. Once authenticated in Active Directory, user devices are available as sources in private access and internet access rules. You can select all endpoint devices in the organization, all existing and future AD devices, or individual AD devices.

Migrate AD User for Machine Tunnel to Identity Endpoint

Migrate AD User provisioned for a machine tunnel to an identity endpoint.

Secure Access provides the option to configure a remote access VPN machine (RA VPN) machine tunnel in an organization. You can set up the machine tunnel using a device and single-machine certificate for all identities in the organization. You can also configure unique certificates for various identity endpoints in the organization.

If your organization provisioned an AD User for a machine tunnel in Secure Access, you must remove this AD User and provision an identity endpoint. For information about machine tunnels, see Manage Machine Tunnels.

Best Practices: Deploying Identity Endpoints for Machine Tunnels

- We recommend that you provision an identity endpoint for the machine tunnel through the Secure Access AD Connector or Secure Access Identities Registration API.
  - For information about the Secure Access AD Connector, see Manage Active Directory Integration.
  - For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.
- Because of potential security vulnerabilites, do not provision AD Users for machine tunnels or surrogates of AD devices.
- Before onboarding identities, we recommend that you remove all AD Users configured as machine tunnels or surrogates of AD devices in your system and Secure Access.
- If you are unable to remove an AD User with a machine tunnel, contact Cisco Support.
- Follow one of the recommended methods to migrate an AD User provisioned as a machine tunnel or surrogate of an AD device to an identity endpoint.

Migrate AD User for Machine Tunnel: Provisioned with CSV Import

If you previously imported a CSV file in Secure Access that included a single AD User for a machine tunnel, you must migrate the AD User to an identity endpoint.

Follow these steps to remove the AD User for the machine tunnel in Secure Access and provision an identity endpoint.

1. Delete the User Authentication profile for the AD User or upload an empty CSV file to Secure Access.

   For information about User Authentication profiles, see Manage User Authentication Profiles.
2. Confirm that Secure Access removed the AD User provisioned for the machine tunnel.
3. Provision the new identity endpoint using either the Secure Access AD Connector or Secure Access Identities Registration API.
   - For information about the Secure Access AD Connector, see Manage Active Directory Integration.
   - For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.
4. Confirm that you added the new identity endpoint in Secure Access.

Migrate AD Users and an AD User for Machine Tunnel: Provisioned with CSV Import

If you previously imported a CSV file in Secure Access that included AD Users and a specific AD User for a machine tunnel, you must migrate the AD Users to identity endpoints.

Follow these steps to import the AD Users, remove the AD User for the machine tunnel, and then provision a new identity endpoint for the machine tunnel.

1. Upload a new CSV file that excludes the AD User provisioned for the machine tunnel.

   For more information, see Import Users and Groups from CSV File.
2. Confirm that Secure Access removed the AD User provisioned for the machine tunnel.
3. Provision the new identity endpoints using either the Secure Access AD Connector or Secure Access Identities Registration API.
   - For information about the Secure Access AD Connector, see Manage Active Directory Integration.

- For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.

4. Confirm that you added the new identity endpoints in Secure Access.

Migrate AD User for Machine Tunnel: Provisioned with AD Connector

If you previously provisioned an AD User for a machine tunnel in Secure Access through the AD Connector, you must migrate the AD User to an identity endpoint.

Follow these steps to migrate the AD User for the machine tunnel to an identity endpoint.

1. Delete the AD User provisioned for the machine tunnel in Secure Access.
2. Provision the new identity endpoint using the AD Connector. For information about the Secure Access AD Connector, see Manage Active Directory Integration.
3. Add the User Authentication profile for the identity endpoint in Secure Access.

   For information about User Authentication profiles, see Manage User Authentication Profiles.
4. Use the AD Connector to resync the identity endpoints in the organization.
5. Confirm that you added the identity endpoints in Secure Access.

Manage Machine Tunnels

Machine tunnels ensure connectivity to the corporate entwork whenever the client system is powered up, whether or not a VPN connection has been established.

A Secure Access VPN machine tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts that require corporate network connectivity also benefit from this feature. For this tunnel to be created without user interaction, certificate-based authentication is used.

About the VPN Machine Tunnel

The Secure Access machine tunnel allows administrators to have the Cisco Secure Client connected without user intervention prior to when the user logs in. Secure Access machine tunnel is triggered when the endpoint is off-premises and disconnected from a user-initiated VPN. The Secure Access VPN machine tunnel is transparent to the end user and disconnects automatically when the user initiates VPN.

The Secure Client VPN agent service is automatically started upon system boot-up. The Secure Client VPN agent uses the VPN profile to detect that the machine tunnel feature is enabled. If the machine tunnel feature is enabled, the agent launches the management client application to initiate a machine tunnel connection. The management client application uses the host entry from the VPN profile to initiate the connection. Then the VPN tunnel is established as usual, with one exception: no software update is performed during a machine tunnel connection since the machine tunnel is meant to be transparent to the user.

The user initiates a VPN tunnel via the Secure Client, which triggers the machine tunnel termination. Upon machine tunnel termination, the user tunnel establishment continues as usual.

The user disconnects the VPN tunnel, which triggers the automatic re-establishment of the machine tunnel.

For information about viewing connection events filtered by machine tunnel, see View the Remote Access Log Report.

Limitations

- User interaction is not supported.

- Certificate-based authentication through Machine Certificate Store (Windows) is only supported.
- Strict Server Certificate checking is enforced.
- A private proxy is not supported.
- A public proxy is not supported (ProxyNative value is supported on platforms where Native Proxy settings are not retrieved from the browser).
- Secure Client Customization Scripts are not supported.

Add a Machine Tunnel and Configure General Settings

Provides instructions for completing the Add a Machine Tunnel and Configure General Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

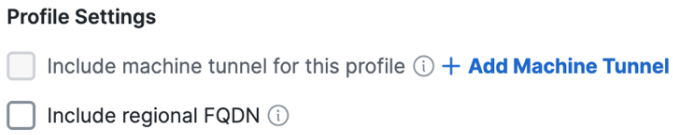
This section describes how to configure Secure Access as the VPN gateway and accept connections from the Secure Client through the VPN machine tunnel.

Before you begin

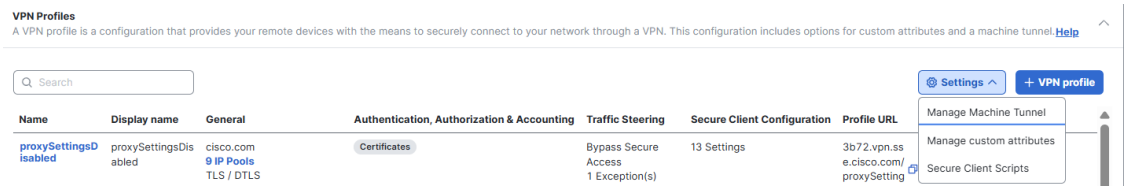
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Navigate to **VPN Profiles** and configure the general settings for the machine tunnel.
   a) Click **+VPN profile**, navigate to **Profile Settings**, and then click **+Add Machine Tunnel**.



   b) Click **Settings**, and then choose **Manage Machine Tunnel** from the drop-down.

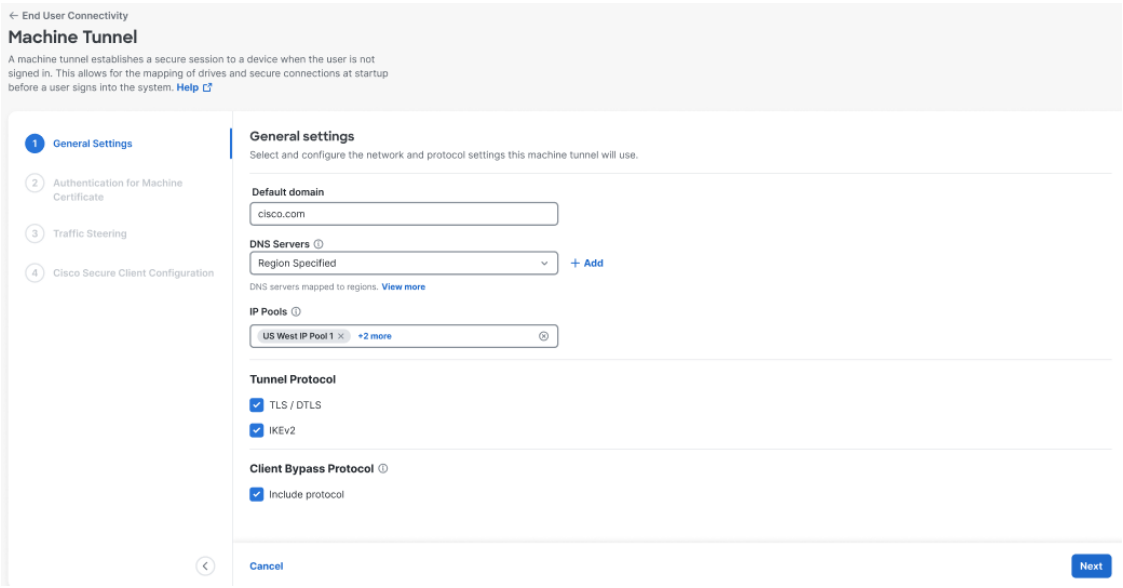


3. Enter the **Default domain**.
4. The **DNS Server** mapped through the **Manage Regions and IP Pools** page is set as the default server. You can accept the default DNS server, choose another DNS server from the drop-down, or click **+ Add** to add a new DNS server pair. Selecting another DNS server or adding a new DNS server overwrites this default server.
5. Select one IP pool per region from the **IP Pools** drop-down. VPN profiles must have at least one IP pool assigned in each region for a valid configuration.
6. Select the **Tunnel Protocol** that this machine tunnel will use.

> **Note**
>
> Select at least one protocol.

- TLS/DTLS
- IPSec (IKEv2)

7. Optionally, check **Include protocol** to enforce client bypass protocol.



Configure Authentication for Machine Certificate

Provides instructions for completing the Configure Authentication for Machine Certificate workflow in Cisco Secure Access. The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session.

The machine tunnel is transparent to the end user and disconnects automatically when the user initiates a VPN session. For this tunnel to be created without user interaction, certificate-based authentication is used.

Set up the authentication for the machine certificate.

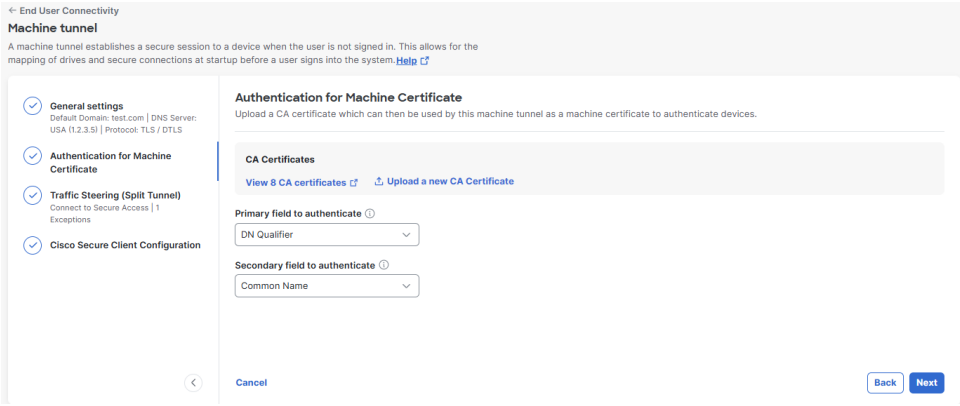
Procedure

---

1. Choose CA certificates from the list or click **Upload CA certificates**.

   These certificates can be used by the machine tunnel as a machine certificate to authenticate devices.

   Upload your organization's signed CA root certificate. For more information, see VPN Certificates for User and Device Authentication.



2. Select the certificate-based authentication fields.
   a) For **Primary field to authenticate**, choose the certificate field that contains the device name (computer name).

      Secure Access uses the device name as the machine tunnel identifier. The format of the computer name must match the format of the chosen device identifier. For more information, see Authenticate Device Identity with Active Directory.

   b) (Optional) For **Secondary field to authenticate**, choose a secondary attribute to authenticate to Active Directory endpoint devices.

      You cannot choose the same value for the primary and secondary authentication fields.

3. Click **Next**.

Configure Traffic Steering (Split Tunnel)

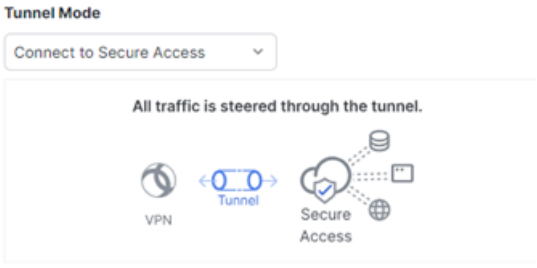
Provides instructions for completing the Configure Traffic Steering (Split Tunnel) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

For **Traffic Steering (Split Tunnel)**, you can configure a machine tunnel to maintain a full tunnel connection to Secure Access, or configure it to use a split tunnel connection to direct traffic through the VPN only if necessary.

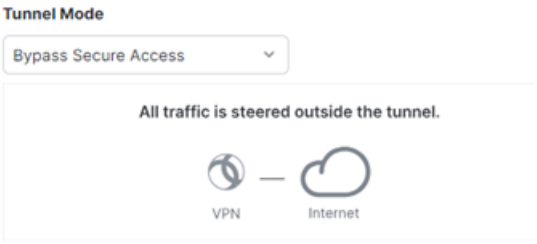
Procedure

---

1. For **Tunnel Mode**, choose either:
   - **Connect to Secure Access** to direct all traffic through the tunnel; or,



   - **Bypass Secure Access** to direct all traffic outside the tunnel.



2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel.
   a) Click **+Add**.
   b) In the search bar, enter the name of a Network Object or a Network Object Group in the search bar, click **Select sources** and then select the same on the **Select sources tab**.
   c) Click the **Add a source**, and then enter comma-separated IPs, domains, and network spaces.
   d) Click **Save**.
3. For **DNS Mode**, you can accept the default mode or, depending on your selection, choose to **Tunnel all DNS** traffic or **Split DNS** traffic.

   When **Split DNS** is chosen, DNS names matching the configured **DNS Names** will be routed over the encrypted Secure Client connection for resolution. Any that do not match the configured **DNS Names** are routed via the local physical interface for the resolution.

   > **Note**
   >
   > At this time, **Split DNS** is only available for **Bypass Secure Access** tunnel mode.

4. Click **Next**, and then configure the Cisco Secure Client.

Define the Cisco Secure Client Configuration

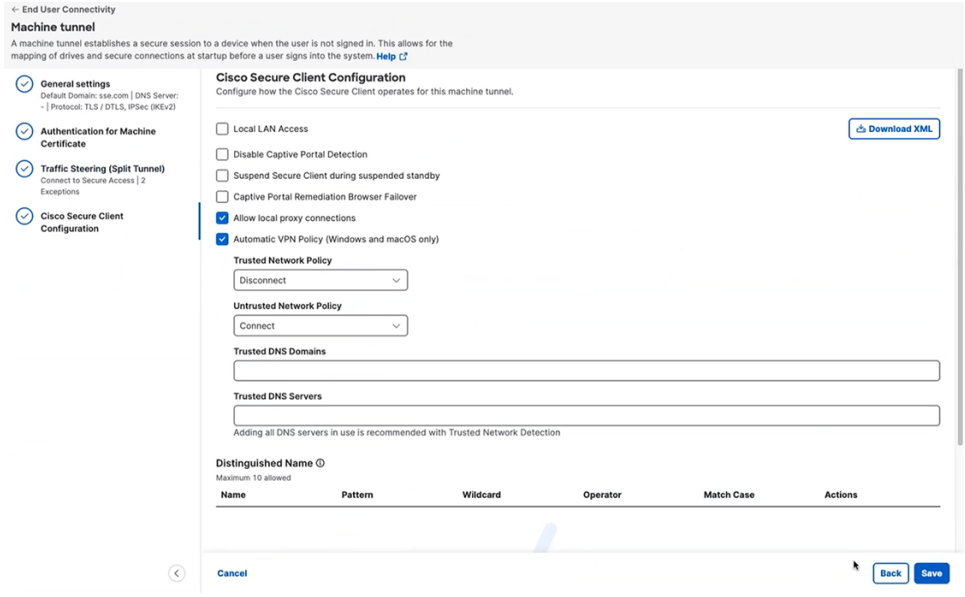
Provides instructions for completing the Define the Cisco Secure Client Configuration workflow in Cisco Secure Access. Review the options presented on the Cisco Secure Client Configuration tab.

You can modify a subset of Cisco Secure Client settings based on the needs of a particular VPN machine tunnel.

Procedure

---

1. Review the options presented on the **Cisco Secure Client Configuration** tab.



2. Configure the options that are specific to your machine tunnel.

   - **Local LAN Access**–Allows the user complete access to the local LAN connected to the remote computer during the VPN session to Secure Access.

     > **Note**
     >
     > Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network.

   - **Disable Captive Portal Detection**–When Cisco Secure Client receives a certificate with a common name that does not match the Secure Access name, a captive portal is detected. This behavior prompts the user to authenticate. Some users using self signed certificates may want to enable connection to corporate resources behind an HTTP captive portal and should thus mark the **Disable Captive Portal Detection** checkbox. The administrator can also determine if they want the option to be user configurable and mark the checkbox accordingly. If user configurable is selected, the checkbox appears on the Preferences tab of the Cisco Secure Client UI.
   - **Suspend Secure Client during suspended standby**– (Windows Only) Available only for devices that support Connected Standby. During Connected Standby, the operating system throttles system process, which can impact how packets are processed. With this option, you can disable VPN traffic when the system enters Connected Standby mode. The feature is disabled by default.
   - **Captive Portal Remediation Browser Failover**–Allows the end user to use an external browser (after closing the Cisco Secure Client browser) for captive portal remediation.
   - **Allow Local Proxy Connections**–By default, Cisco Secure Client lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network components on some antivirus software.
   - **Automatic VPN Policy (Windows and macOS only)**–Enables Trusted Network Detection allowing Cisco Secure Client to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

- **Trusted Network Policy**–Action Cisco Secure Client automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
  - Disconnect (Default)–Disconnects the VPN connection upon the detection of the trusted network.
  - Connect–Initiates a VPN connection upon the detection of the trusted network.
  - Do Nothing–Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - Pause–Cisco Secure Client suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, Cisco Secure Client resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
- **Untrusted Network Policy**–Cisco Secure Client starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
  - Connect (Default)–Initiates the VPN connection upon the detection of an untrusted network.
  - Do Nothing–Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
- **Trusted DNS Domains**–DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *".cisco.com*.

  Note

  Wildcards *('*')* are **not** supported for DNS suffixes.

- **Trusted DNS Servers**–DNS server addresses (IP addresses separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1.

  Note

  Wildcards *('*')* are **not** supported for DNS server addresses.

Distinguished Name–Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates. When you add multiple Distinguished Names, each certificate is checked against all entries, and all of them must match.

Note

A maximum of 10 distinguished names are allowed.

- **Name**–The distinguished name (DN) to use for matching:
  - CN–Subject Common Name
  - C–Subject Country

- DC–Domain Component
- DNQ–Subject Dn Qualifier
- EA–Subject Email Address
- GENQ–Subject Gen Qualifier
- GN–Subject Given Name
- I–Subject Initials
- L–Subject City
- N–Subject Unstruct Name
- O–Subject Company
- OU–Subject Department
- SN–Subject Sur Name
- SP–Subject State
- ST–Subject State
- T–Subject Title
- ISSUER-CN–Issuer Common Name
- ISSUER-DC–Issuer Component
- ISSUER-SN–Issuer Sur Name
- ISSUER-GN–Issuer Given Name
- ISSUER-N–Issuer Unstruct Name
- ISSUER-I–Issuer Initials
- ISSUER-GENQ–Issuer Gen Qualifier
- ISSUER-DNQ–Issuer Dn Qualifier
- ISSUER-C–Issuer Country
- ISSUER-L–Issuer City
- ISSUER-SP–Issuer State
- ISSUER-ST–Issuer State
- ISSUER-O–Issuer Company
- ISSUER-OU–Issuer Department
- ISSUER-T–Issuer Title
- ISSUER-EA–Issuer Email Address

3. Click **Save**.

What to do next

You need to associate the machine tunnel with remote access VPN for users and their devices.

- Establish a machine tunnel VPN using certificate-based authentication against device identities from Active Directory. For more information, see Authenticate Device Identity with Active Directory.

Authenticate Device Identity with Active Directory

Describes Authenticate Device Identity with Active Directory in Cisco Secure Access. Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs).

Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs). Once integrated with Secure Access, you can protect and monitor the connections for the users and devices to internet and private destinations by configuring Access rules in the organization's policy.

> **Note**
>
> We recommend you use certificate-based authentication to register device identities with Active Directory.

Configure Active Directory Endpoint Device Management

Provides instructions for completing the Configure Active Directory Endpoint Device Management workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Active Directory integration in Secure Access includes the option to provision endpoint devices from an on-premise Active Directory domain controller (DC).

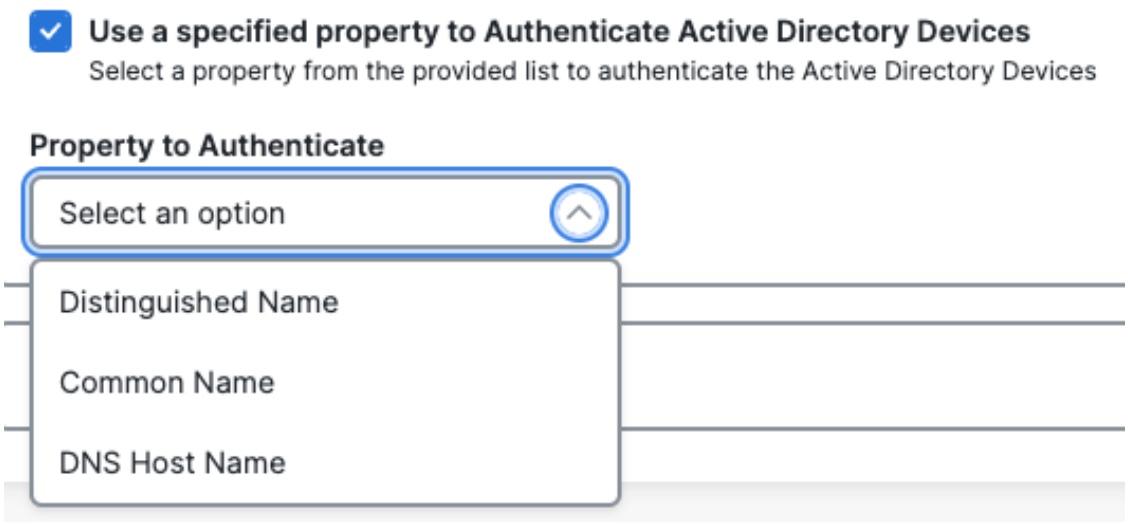
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Endpoint device integration requires devices provisioned by an on-premise Active Directory domain controller (DC) and Cisco AD Connector version 1.14.4 or newer. For more information, see Connect Active Directory to Secure Access and Configure Updates on AD Connector.
- A configured machine tunnel applied to a VPN profile. For more information, see Manage Machine Tunnels.

> **Note**
>
> Make a note of the primary attribute for Active Directory certificate-based authentication. For more information, see Add a Machine Tunnel.

Procedure

1. Navigate to **Connect** > **Users, Groups, and Endpoint Devices**, and click **Configuration management**.
2. On the **Configurations** tab, navigate to **Directories**, and then expand **Active Directory**.
3. Check the box at the bottom of your Active Directory integration menu to **Use a specified property to Authenticate Active Directory Devices**.



4. Select a **Property to Authenticate** from the list of Active Directory machine attributes for certificate-based authentication.

   Secure Access supports the **Distinguished Name**, **Common Name**, and **DNS Host Name** attributes. For more information see, Manage Machine Tunnels.

   When selecting the **Property to Authenticate** option, we recommend:

   - For the computer names in the FQDN format, choose **DNS Host Name**.
   - For the computer name in the short-format, choose **Common Name**.

5. After making changes to the AD integration, restart the AD Connector to trigger a full synchronization of AD Users, Groups, and Endpoint Devices.

   For more information, see Restart the Active Directory Connector.

What to do next

Secure Access has a single Access policy, which consists of policy rules and settings. Your private access and internet policy rules and the default policy rules control the access and security of your resources and protect the traffic in your organization.

Secure Access supports configuring security controls for sources and destinations (resources) on private and internet access rules. Once authenticated in Active Directory, user devices are available as sources in private access and internet access rules. You can select all endpoint devices in the organization, all existing and future AD devices, or individual AD devices.

Migrate AD User for Machine Tunnel to Identity Endpoint

Migrate AD User provisioned for a machine tunnel to an identity endpoint.

Secure Access provides the option to configure a remote access VPN machine (RA VPN) machine tunnel in an organization. You can set up the machine tunnel using a device and single-machine certificate for all identities in the organization. You can also configure unique certificates for various identity endpoints in the organization.

If your organization provisioned an AD User for a machine tunnel in Secure Access, you must remove this AD User and provision an identity endpoint. For information about machine tunnels, see Manage Machine Tunnels.

Best Practices: Deploying Identity Endpoints for Machine Tunnels

- We recommend that you provision an identity endpoint for the machine tunnel through the Secure Access AD Connector or Secure Access Identities Registration API.
  - For information about the Secure Access AD Connector, see Manage Active Directory Integration.
  - For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.
- Because of potential security vulnerabilites, do not provision AD Users for machine tunnels or surrogates of AD devices.
- Before onboarding identities, we recommend that you remove all AD Users configured as machine tunnels or surrogates of AD devices in your system and Secure Access.
- If you are unable to remove an AD User with a machine tunnel, contact Cisco Support.
- Follow one of the recommended methods to migrate an AD User provisioned as a machine tunnel or surrogate of an AD device to an identity endpoint.

Migrate AD User for Machine Tunnel: Provisioned with CSV Import

If you previously imported a CSV file in Secure Access that included a single AD User for a machine tunnel, you must migrate the AD User to an identity endpoint.

Follow these steps to remove the AD User for the machine tunnel in Secure Access and provision an identity endpoint.

1. Delete the User Authentication profile for the AD User or upload an empty CSV file to Secure Access.

   For information about User Authentication profiles, see Manage User Authentication Profiles.
2. Confirm that Secure Access removed the AD User provisioned for the machine tunnel.
3. Provision the new identity endpoint using either the Secure Access AD Connector or Secure Access Identities Registration API.
   - For information about the Secure Access AD Connector, see Manage Active Directory Integration.
   - For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.
4. Confirm that you added the new identity endpoint in Secure Access.

Migrate AD Users and an AD User for Machine Tunnel: Provisioned with CSV Import

If you previously imported a CSV file in Secure Access that included AD Users and a specific AD User for a machine tunnel, you must migrate the AD Users to identity endpoints.

Follow these steps to import the AD Users, remove the AD User for the machine tunnel, and then provision a new identity endpoint for the machine tunnel.

1. Upload a new CSV file that excludes the AD User provisioned for the machine tunnel.

   For more information, see Import Users and Groups from CSV File.
2. Confirm that Secure Access removed the AD User provisioned for the machine tunnel.
3. Provision the new identity endpoints using either the Secure Access AD Connector or Secure Access Identities Registration API.
   - For information about the Secure Access AD Connector, see Manage Active Directory Integration.

- For information about the Secure Access Identities Registration API, see Cisco Secure Access Identities Registration API.

4. Confirm that you added the new identity endpoints in Secure Access.

Migrate AD User for Machine Tunnel: Provisioned with AD Connector

If you previously provisioned an AD User for a machine tunnel in Secure Access through the AD Connector, you must migrate the AD User to an identity endpoint.

Follow these steps to migrate the AD User for the machine tunnel to an identity endpoint.

1. Delete the AD User provisioned for the machine tunnel in Secure Access.
2. Provision the new identity endpoint using the AD Connector. For information about the Secure Access AD Connector, see Manage Active Directory Integration.
3. Add the User Authentication profile for the identity endpoint in Secure Access.

   For information about User Authentication profiles, see Manage User Authentication Profiles.
4. Use the AD Connector to resync the identity endpoints in the organization.
5. Confirm that you added the identity endpoints in Secure Access.

Manage Application-Based Remote Access VPN (Per App VPN)

For mobile devices that run on Android or iOS, you can restrict the applications that traverse the VPN tunnel using Per App VPN.

When a remote user establishes a VPN connection from a mobile device using Secure Client, all the traffic including traffic from personal applications is routed through the VPN. For mobile devices that run on Android or iOS, you can restrict the applications that traverse the VPN tunnel. This application-based remote access VPN is called Per App VPN.

To use Per App VPN, you must perform the following actions:

1. Install and configure a third-party Mobile Device Manager (MDM) server.
2. Define the list of approved applications that can go over the VPN tunnel in the MDM server.
3. Deploy the Per App configurations from the MDM server to the mobile devices.
4. Configure Per App VPN on the managed headend threat defense.

When an MDM-managed mobile device connects to the VPN using Secure Client, the client validates the applications before tunneling the traffic. The Per App policy configured on Secure Access performs this validation.

Benefits

Limit VPN traffic over the corporate network and free up resources of the VPN headend. You can:

- Limit applications such as Netflix, Facebook, and YouTube over the VPN.
- Allow trusted cloud applications such as Outlook, and Webex over the VPN.
- Optimize traffic.
- Minimize latency.
- Protect the corporate VPN tunnel from unapproved malicious applications on the mobile device.

Manage Custom Attributes

Describes Manage Custom Attributes in Cisco Secure Access. Custom attributes are used by the Cisco Secure Client to configure features such as Per App VPN and split tunneling.

Custom attributes are used by the Cisco Secure Client to configure features such as Per App VPN and split tunneling. You can create the Secure Client custom attributes objects from the VPN Profiles dashboard, add the objects to a VPN profile, and associate the VPN profile with a remote access VPN to enable the features for the VPN clients.

Secure Access supports the following features using the custom attribute objects:

- **Split Exclude Failover**– The split Exclude Failover feature helps allow traffic through a VPN tunnel when a lack of network connectivity prevents its routing outside the tunnel.
- **Per App VPN** –The Per App VPN feature helps identify an app and tunnel only applications allowed by the Secure Access administrator over the VPN.
- **Bypass Virtual Subnets** –The Bypass Virtual Subnets feature helps resolve connectivity issues with virtual machine-based subsystems.

Split Exclude Failover

By default, the VPN tunnel implicit security (filtering) blocks access via the tunnel to any destinations in the exception list unable to be routed outside the tunnel because of a lack of network connectivity.

To avoid this, create a **Split Exclude Failover** custom attribute set to **true**. And add this attribute to a remote access VPN group profile. This allows split exclude failover for destinations in exception list to route traffic through the VPN tunnel when a lack of network connectivity prevents its routing outside the tunnel.

> **Note**
>
> Mobile platforms do not support split exclude failover custom attributes.

Per App VPN

When you use Cisco Secure Client AnyConnect to establish a VPN connection from a mobile device, all the traffic including the traffic from personal applications is routed through the VPN.

If you instead want to route corporate applications only through the VPN, so that non-corporate traffic is excluded from the VPN, you can use Per App VPN to select which applications should be tunneled through the VPN.

You configure Per App VPN using the **perapp** AnyConnect custom attribute. Adding this attribute to a remote access VPN group profile automatically limits the tunnel to the explicitly identified applications. Traffic from all other applications is automatically excluded from the tunnel.

Configuring Per App VPN has the following main benefits:

- Performance–It limits traffic in the VPN to the traffic that needs to go to the corporate network. Thus, you free up resources at the head end of the RA VPN.
- Protection–Because only traffic from approved applications is allowed, it protects the corporate tunnel from unapproved malicious applications that a user might unwittingly install on the mobile device. Because these applications are not included in the tunnel, traffic from them is never sent to the head end.

The Mobile Device Manager (MDM) running on the mobile endpoint enforces the Per App VPN policy on the applications.

Bypass Virtual Subnets

If you experience connectivity issues with virtual machine-based subsystems, such as Windows Subsystem for Linux (WSL2) or VMware Fusion VM, when the AnyConnect VPN is active on the host (Windows 10 or macOS 11 (and later), you can configure local LAN split/exclude tunneling restricted to only virtual adapter subnets.

About Cisco Secure Client on Mobile Devices

Describes About Cisco Secure Client on Mobile Devices in Cisco Secure Access. Cisco Secure Client on mobile devices is similar to Cisco Secure Client on Windows, macOS, and Linux platforms.

Cisco Secure Client on mobile devices is similar to Cisco Secure Client on Windows, macOS, and Linux platforms. The Cisco Secure Client (including AnyConnect) Administrator Guide provides device information, configuration information, support information, as well as other administrative tasks specific to Cisco Secure Client for mobile devices.

Because Secure Access supports custom attributes on Android and iOS devices, you should review the following sections of the Administrator Guide:

- Cisco Secure Client on Android Devices
- Cisco Secure Client on Apple iOS Devices

In particular, pay close attention to the following guidelines and limitations for each supported platform. As always, you should consult the latest Cisco Secure Client (including AnyConnect) Administrator Guide for the most up-to-date information.

Guidelines and Limitations for Secure Client AnyConnect on Android

Describes Guidelines and Limitations for Secure Client AnyConnect on Android in Cisco Secure Access. The Secure Firewall ASA does not provide distributions and updates for AnyConnect for Android.

- The Secure Firewall ASA does not provide distributions and updates for AnyConnect for Android. They are available on Google Play. The APK (package) file for the latest version is also posted on Cisco.com.
- AnyConnect for Android supports only the Network Visibility Module and Umbrella; it does not support any other Secure Client modules.
- The Android device supports no more than one AnyConnect profile, which is the last one received from a headend. However, a profile can consist of multiple connection entries.
- If users attempt to install AnyConnect on devices that are not supported, they receive the pop-up message Installation Error: Unknown reason -8. This message is generated by the Android OS.
- With users who have AnyConnect in a widget on their home screen, the AnyConnect services are automatically started (but not connected) regardless of the "Launch at startup" preference.
- AnyConnect for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.
- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the AnyConnect Send Log button. As a workaround, use the native utilities on Windows and macOS to decompress Secure Client log files.
- DHE Incompatibility—With the introduction of DHE cipher support in AnyConnect, incompatibility issues result in Cisco Secure Firewall ASA versions before ASA 9.2. If you are using DHE ciphers with Secure Firewall ASA releases earlier than 9.2, you must disable DHE ciphers on those Secure Firewall ASA versions.
- Because AnyConnect is a networking VPN application, it requires background operation to function; therefore, you should never add AnyConnect to the deep sleep list.

Guidelines and Limitations for Secure Client AnyConnect on Apple iOS

Describes Guidelines and Limitations for Secure Client AnyConnect on Apple iOS in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

AnyConnect for Apple iOS supports only features that are related to remote VPN access such as:

- AnyConnect can be configured by the user (manually), by the AnyConnect VPN Client Profile, generated by the Apple Configurator Utility (http://www.apple.com/support/iphone/enterprise), or using an Enterprise Mobile Device Manager.
- The Apple iOS device supports no more than one AnyConnect VPN client profile. The contents of the generated configuration always match the most recent profile. For example, you connect to vpn.example1.com and then to vpn.example2.com. The AnyConnect VPN client profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it reduces battery life of the device. Increasing the update interval value mitigates this issue.

Apple iOS Connect On-Demand Considerations:

- VPN sessions, which are automatically connected as a result of iOS On-Demand logic and have Disconnect on Suspend configured, are disconnected when the device sleeps. After the device wakes up, On-Demand logic will reconnect the VPN session when it is necessary again.
- AnyConnect collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which AnyConnect can misreport mobile posture information if the user relies on iOS Connect On-Demand feature to make a connection initially, or after device information, such as the OS version has changed.

Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs. Hence:

- Using the new extension framework in AnyConnect 4.0.07x (and later) causes the following changes in behavior from legacy AnyConnect 4.0.05x: AnyConnect considers traffic for tunnel DNS server to be tunneled, even if it is not in split-include network.
- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x (or later). Cisco AnyConnect 4.0.07x (or 4.6.x and later) is a separate app, installed with a different name and icon.
- The different versions of AnyConnect can co-exist on the mobile device, but this is not supported by Cisco. The behavior may not be as expected if you attempt to connect while having both versions of AnyConnect installed. Make sure you have only one AnyConnect app on your device, and it is the appropriate version for your device and environment.
- Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.
- Current MDM profiles will not trigger the new app. EMM vendors must support VPNType (VPN), VPNSubType (com.cisco.anyconnect) and ProviderType (packet-tunnel). For integration with ISE, they must be able to pass the UniqueIdentifier to AnyConnect since AnyConnect no longer has access to this in the new framework. Consult your EMM vendor for how to set this up; some may require a custom VPN type, and others may not have support available at release time.

Using the New Extension Framework in AnyConnect 4.0.07x and later causes the following changes in behavior from Legacy AnyConnect 4.0.05x:

- The Device ID sent to the head end is no longer the UDID in the new version, and it is different after a factory reset unless your device is restored from a backup made by the same device.

- You may use MDM deployed certificates, as well as certificates imported using one of the methods available in AnyConnect: SCEP, manually through the UI, or via the URI handler. The new version of AnyConnect can no longer use certificates imported via email or any other mechanism beyond these identified ones.
- When creating a connection entry using the UI, the user must accept the iOS security message displayed.
- A user-created entry with the same name as a downloaded host entry from the AnyConnect VPN profile will not be renamed until it disconnects, if it is active. Also, the downloaded host connection entry will appear in the UI after this disconnect, not while it remains connected.
- AnyConnect considers traffic for tunnel DNS server to be tunneled even if it is not in split-include network.

Define Custom Attributes

Describes Define Custom Attributes in Cisco Secure Access and explains Prerequisites, Supported Platforms, and Limitations. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

A custom attribute has a type and a named value. The type of the attribute is defined first, then one or more named values of this type can be defined. You create the Secure Client custom attribute objects from the VPN Profiles dashboard, add the objects to a VPN profile, and associate the VPN profile with a remote access VPN to enable the features for the VPN clients.

This topic describes how to define and apply Secure Client custom attributes to your organization's VPN profiles.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For Per App VPN, ensure that you have:
  - Set up an MDM server and enrolled each mobile device to the MDM server.
  - For more information, see the MDM documentation. We recommend that you configure the applications that can traverse the VPN tunnel in the MDM server. This configuration simplifies the headend configuration.
- Downloaded and installed the Cisco AnyConnect Enterprise Application Selector from the Cisco Software Download Center to your local host. You need this tool to define the Per App VPN policy.

Supported Platforms

- Per App VPN is supported for mobile devices running:
  - Android
  - iOS
- Bypass Virtual Subnet is supported for devices running:
  - Windows 10 (and later)
  - macOS 11 (and later)

Limitations

See the following sections for information about the limitations for deploying Secure Client custom attribute objects in Secure Access:

- Guidelines and Limitations for Secure Client AnyConnect on Android
- Guidelines and Limitations for Secure Client AnyConnect on Apple iOS

Define Per App VPN Custom Attributes

Describes Define Per App VPN Custom Attributes in Cisco Secure Access. To define custom attributes for Per App VPN applications, download the Policy Tool for Android and Apple iOS devices to generate application IDs and assign Per App VPN custom attributes to Secure Access VPN profiles.

To define custom attributes for Per App VPN applications, download the Policy Tool for Android and Apple iOS devices to generate application IDs and assign Per App VPN custom attributes to Secure Access VPN profiles.

Step 1 - Determine the Application IDs for Mobile Applications

Provides instructions for completing the Step 1 – Determine the Application IDs for Mobile Applications workflow in Cisco Secure Access. To configure the list of allowed applications on the headend, you must determine the application IDs for each application on each type of endpoint.

To configure the list of allowed applications on the headend, you must determine the application IDs for each application on each type of endpoint.

The application ID, or the bundle ID in iOS, is a reverse DNS name. You can use an asterisk as a wildcard. For example, . indicates all applications, com.cisco.* indicates all Cisco applications.

To determine the application IDs:

Android

Procedure

1. In a web browser, go to Google Play (https://play.google.com/store/).
2. Click the **Apps** tab.
3. Click an application that you want to allow in the VPN tunnel.
4. The application ID is part of the URL.
5. Copy the string after the 'id=' parameter.

   For Microsoft Remote Desktop, the URL is:https://play.google.com/store/apps/details?id=com.microsoft.rdc.androidx, and the app id is com.microsoft.rdc.androidx.

What to do next

> **Note**
>
> For applications that are not available on Google Play, download a package name viewer application to extract the app ID.

iOS

1. In a web browser, go to Apple App Store (https://www.apple.com/in/app-store/).
2. In the search results, search for an application.

   The application ID is part of the URL.
3. Copy the number after the 'id' string.

   For Facebook, the URL is:https://apps.apple.com/in/app/facebook/id284882215 and the application ID is 284882215.
4. Open a new browser window, and add the number to the end of the following URL: https://itunes.apple.com/lookup?id=

For Facebook the URL is https://itunes.apple.com/lookup?id=284882215.

5. Download the text file, usually named `1.txt`.
6. Open the file in a text editor, and search for 'bundleId'. For Facebook, the 'bundleId' is "com.facebook.Facebook". Use this bundle ID as the app ID.

Once you have your list of application IDs, you can define the custom attributes for the mobile device as described in the following steps.

Step 2 - Create a Base64 Encoded String for Each Mobile Application

Provides instructions for completing the Step 2 - Create a Base64 Encoded String for Each Mobile Application workflow in Cisco Secure Access. Create a base64 encoded string for each app using the Cisco Secure Client Enterprise Application Selector Tool.

Create a base64 encoded string for each app using the Cisco Secure Client Enterprise Application Selector Tool.

Procedure

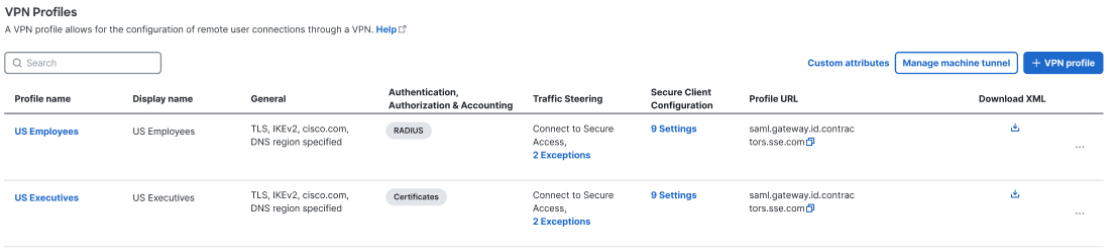
1. Download the Cisco Secure Client Enterprise Application Selector Tool from here .
2. Open the Application Selection Tool and select the mobile platform from the drop-down menu located on the upper left, either **Android** or **iOS**.
3. Add a rule by entering the following options:
   a. **Friendly Name**–Enter something meaningful.
   b. **App ID**–Enter the name of the mobile application.
   c. The rest of the fields are optional.
4. On the menu bar, click on **Policy** > **View Policy**. The encoded base64 rule is displayed in its encrypted format.
5. Select and copy the policy string, and save it to use later when you create Secure Client custom attribute objects.

Step 3 - Create a Custom Attribute Object

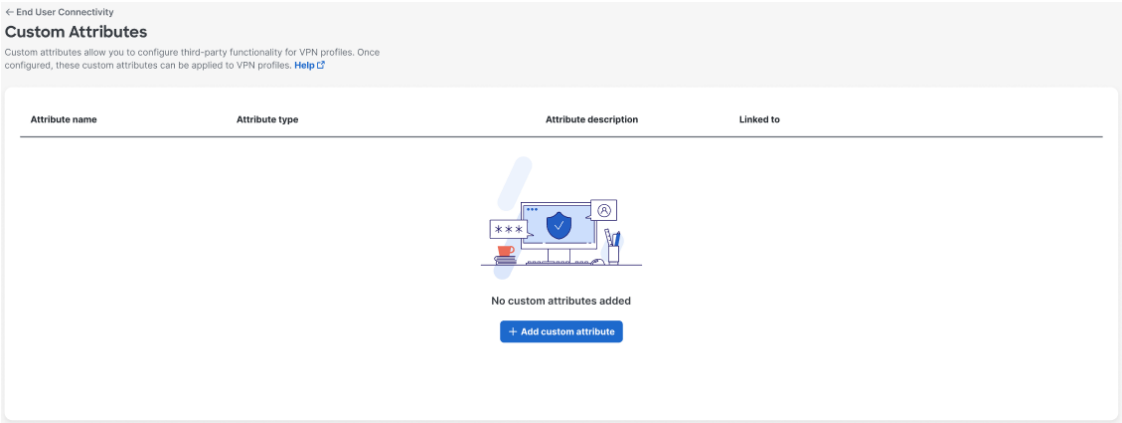
Provides instructions for completing the Step 3 - Create a Custom Attribute Object workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Virtual Private Network .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **Custom attributes**.



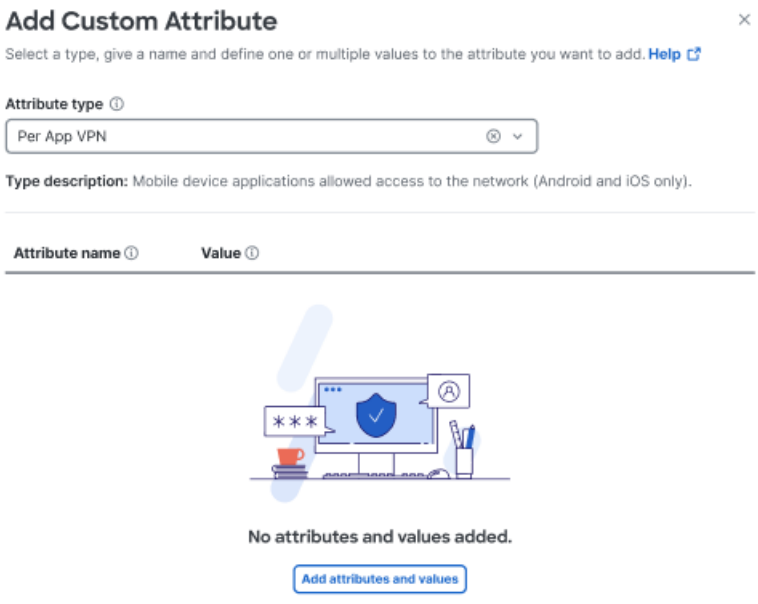
3. Click **+ Add custom attribute** to configure an attribute for a third-party application for a mobile device.



4. From the **Add Custom Attributes** drawer, choose **Per App VPN** from the **Attribute type** drop-down.



5. Click **Add attributes and values** to configure your custom attributes.

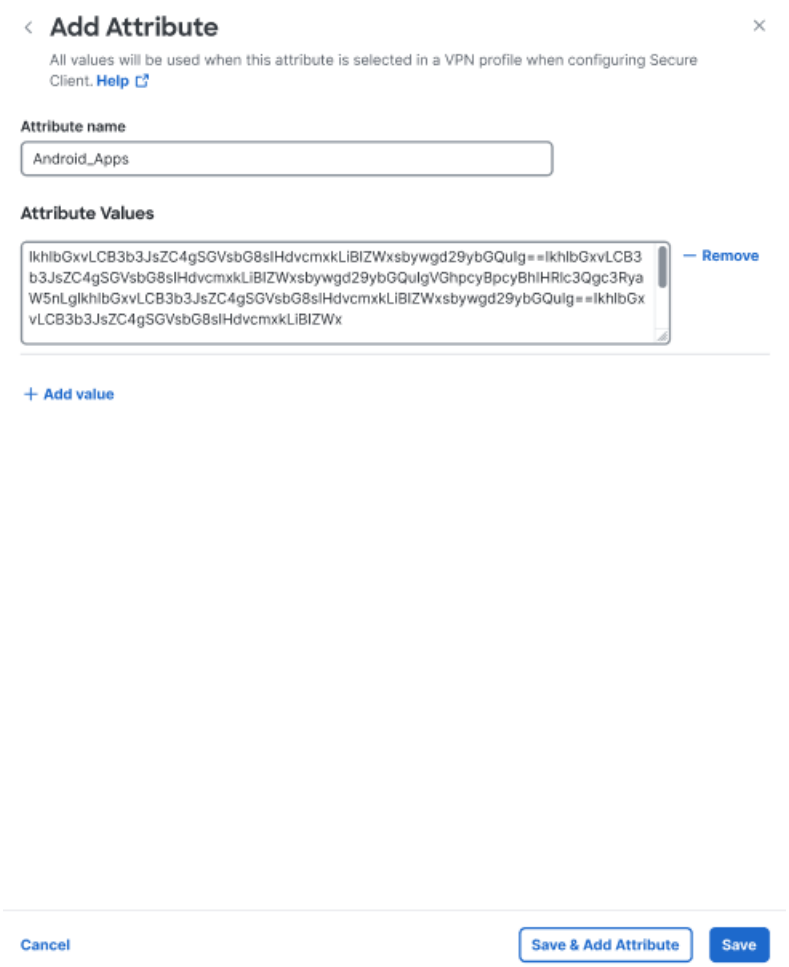


6. Configure the following options:

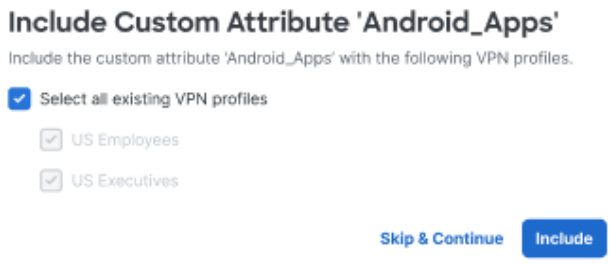
   a. **Attribute name**–Enter a unique name for the attribute. For example, *Android_Apps* or *Apple_iOS_Apps*.

   b. **Attribute Values**–Add one or more values by copying the base64 format from the policy tool and pasting it here. Each value cannot exceed 420 characters. If your value exceeds this length, click **+ Add value** to add multiple values for the additional value content. The configured values are concatenated before being sent to the Cisco Secure Client.

      All values added to an attribute will be used when that attribute is assigned to a VPN profile.

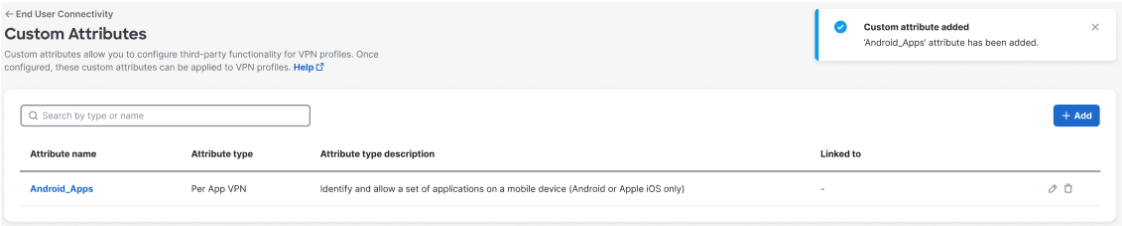


c. Click **Save** when you are finished with this attribute. If you have active VPN profiles, you'll be presented with the option to selectively add the attribute to VPN profile.



d. Click **Include** to add the attribute to VPN profiles, or click **Skip & Continue**.

e. Click **Save & Add Attribute** to add the attribute to the dashboard. Once saved, you can come back to **Edit** or **Delete** the attribute.



7. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** > **Custom attributes** to view the table of available custom attributes.

Define Bypass Virtual Subnets Custom Attributes

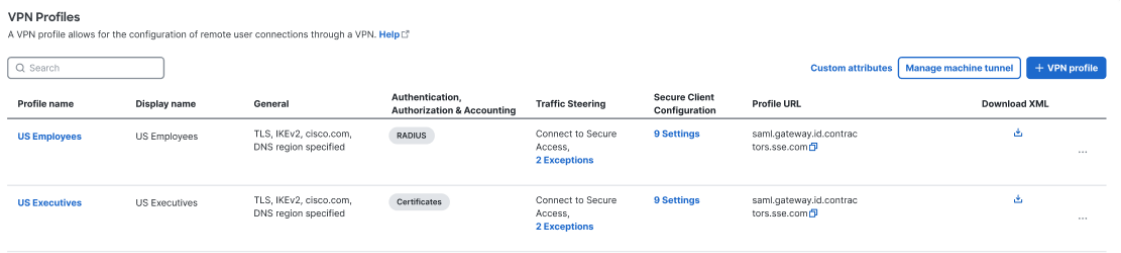
Provides instructions for completing the Define Bypass Virtual Subnets Custom Attributes workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

If you experience connectivity issues with Windows Subsystem for Linux (WSL2) or VMware Fusion VM when the AnyConnect VPN is active on the host (Windows 10 or macOS 11 (and later), follow these steps to configure Local LAN split exclude tunneling restricted to only virtual adapter subnets.

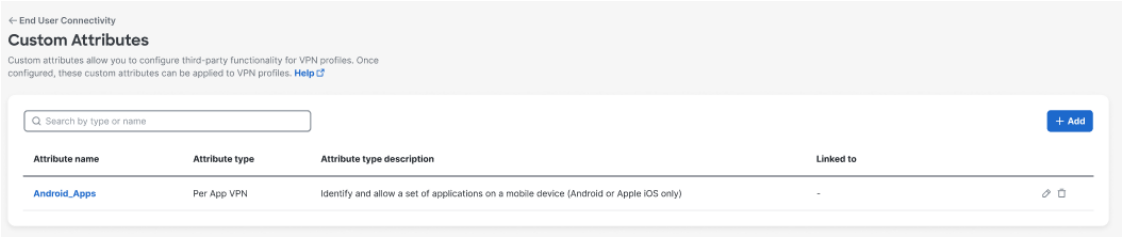
> **Note**
>
> Enable the **Local LAN Access** option when using the **Bypass Virtual Subnets Custom Attributes** feature.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For **VPN Profiles**, click **Custom attributes**.



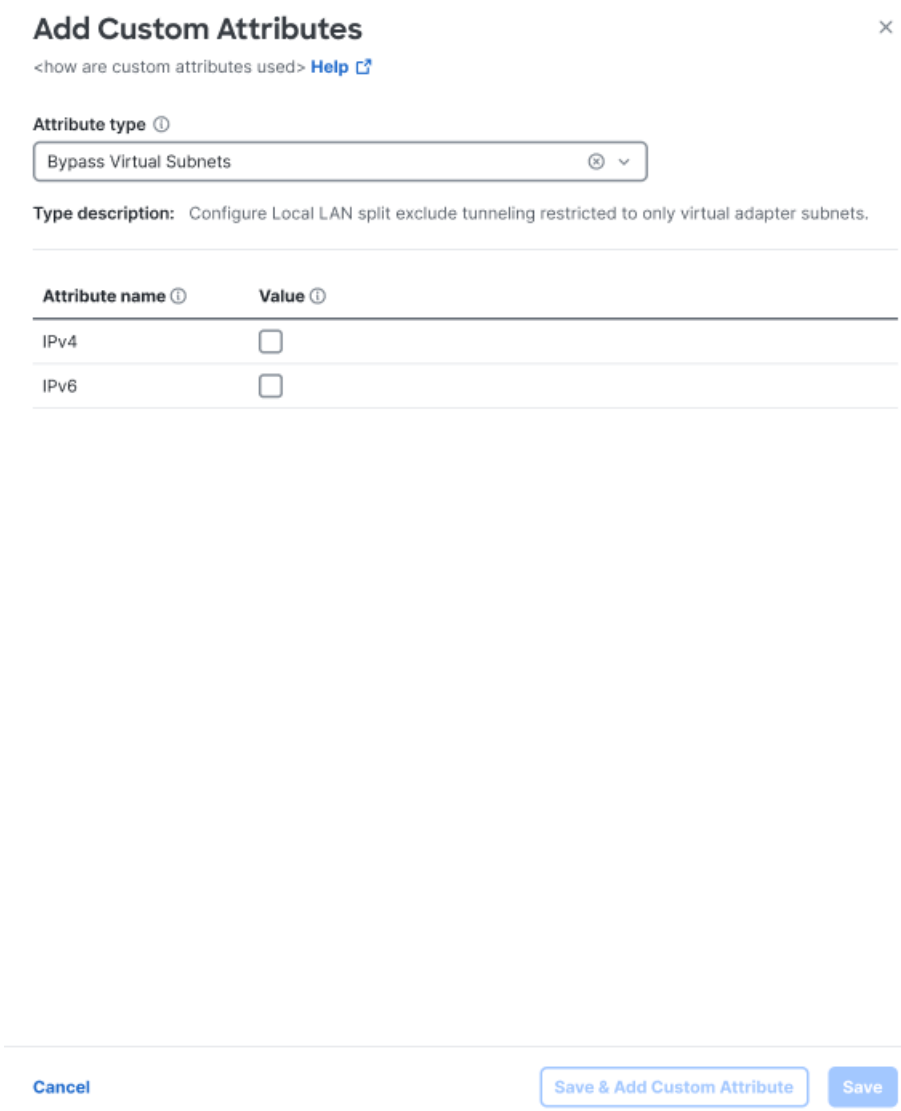
3. Click **+ Add** to configure an attribute for a third-party application for a mobile device.



4. From the **Add Custom Attributes** drawer, choose **Bypass Virtual Subnets** from the **Attribute type** drop-down.

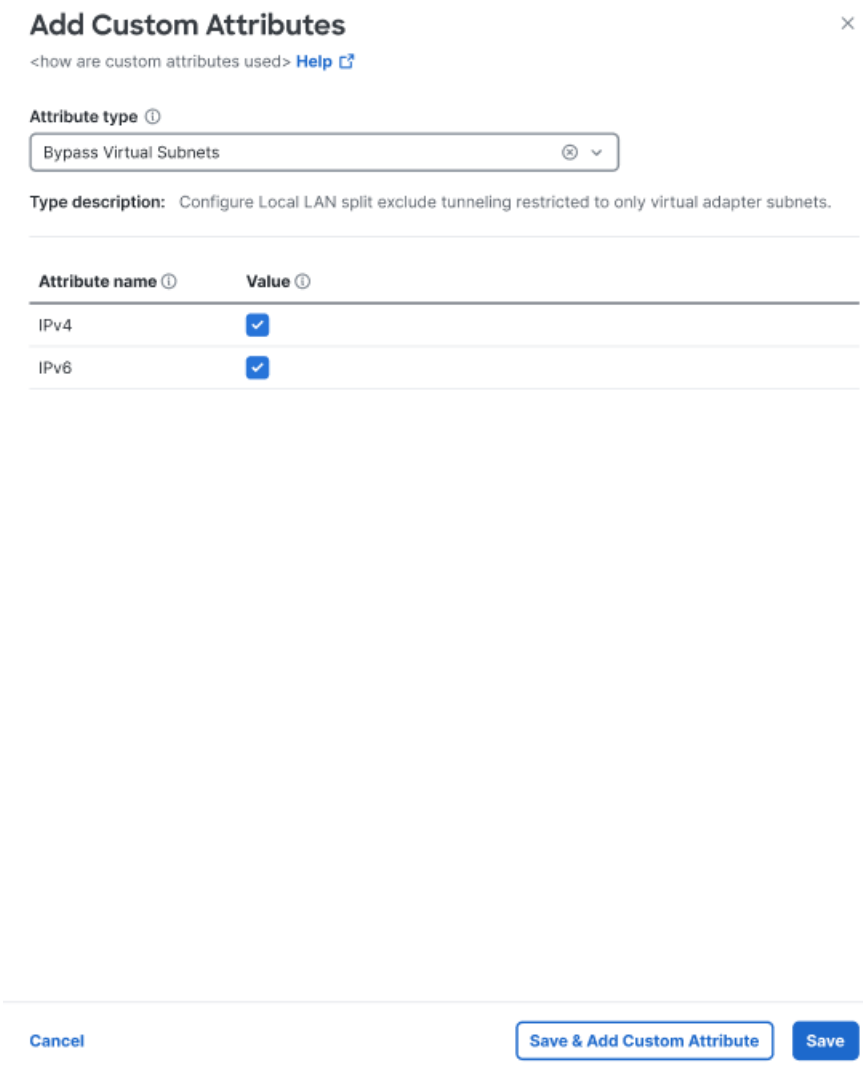


5. Click **Add attributes and values** to configure your custom attributes.

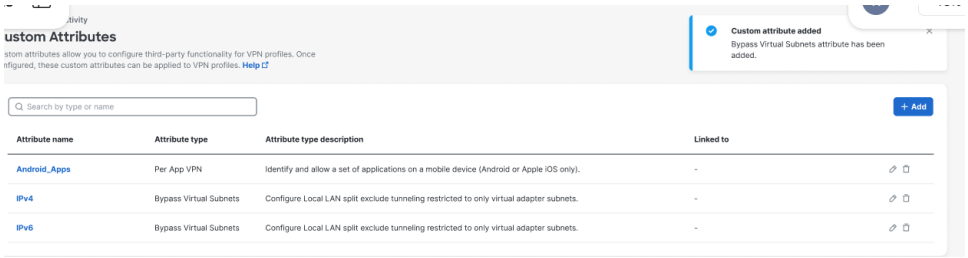


6. Choose from the following options:
   a. **IPv4**–Select IPv4 to bypass virtual subnets for only IPv4 traffic.
   b. **IPv6**–Select IPv6 to bypass virtual subnets for only IPv6 traffic.

      You can choose either or both of these options.
   c. Click **Save** if you need to come back to this attribute at a later time; click **Save & Add Attribute** if you are finished.



7. Navigate to Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** > **Custom attributes** to view the table of available custom attributes.



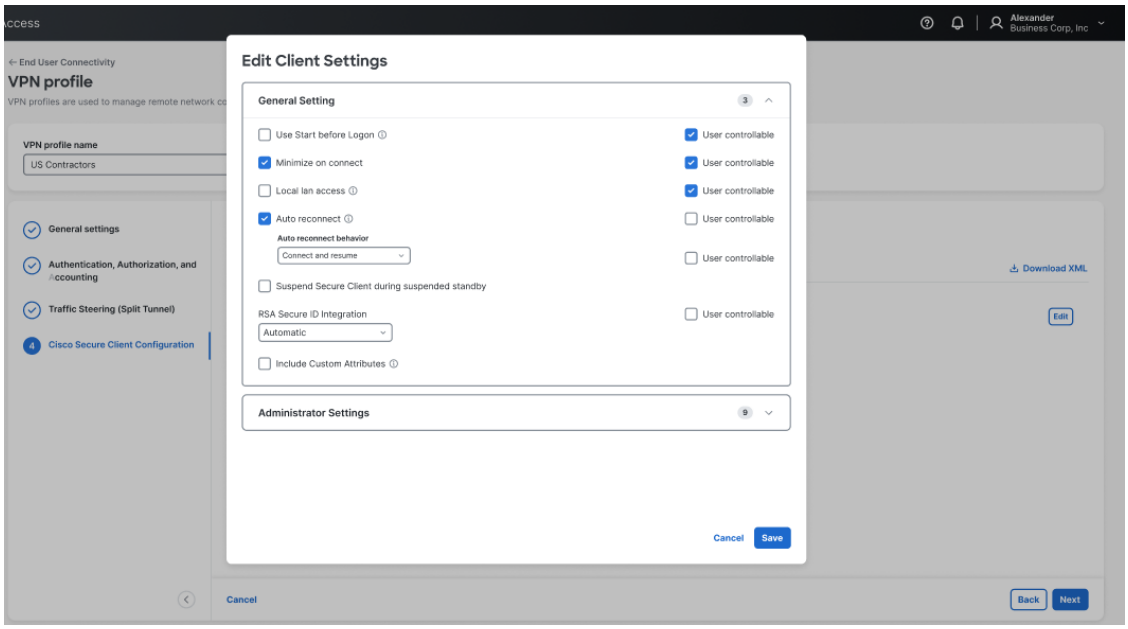
Edit Cisco Secure Client Settings

Provides instructions for completing the Edit Cisco Secure Client Settings workflow in Cisco Secure Access. You can modify Cisco Secure Client settings to attach a previously created custom attribute type and name to a VPN profile via Connect End User Connectivity Virtual Private Network .

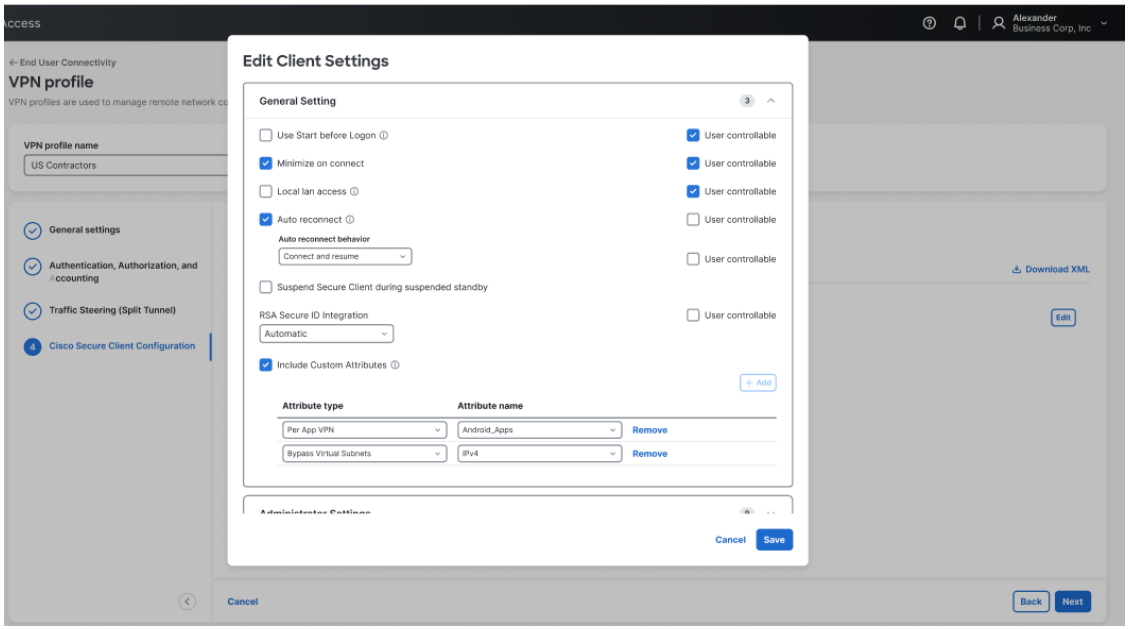
You can modify Cisco Secure Client settings to attach a previously created custom attribute type and name to a VPN profile via **Connect** > **End User Connectivity** > **Virtual Private Network**.

Procedure

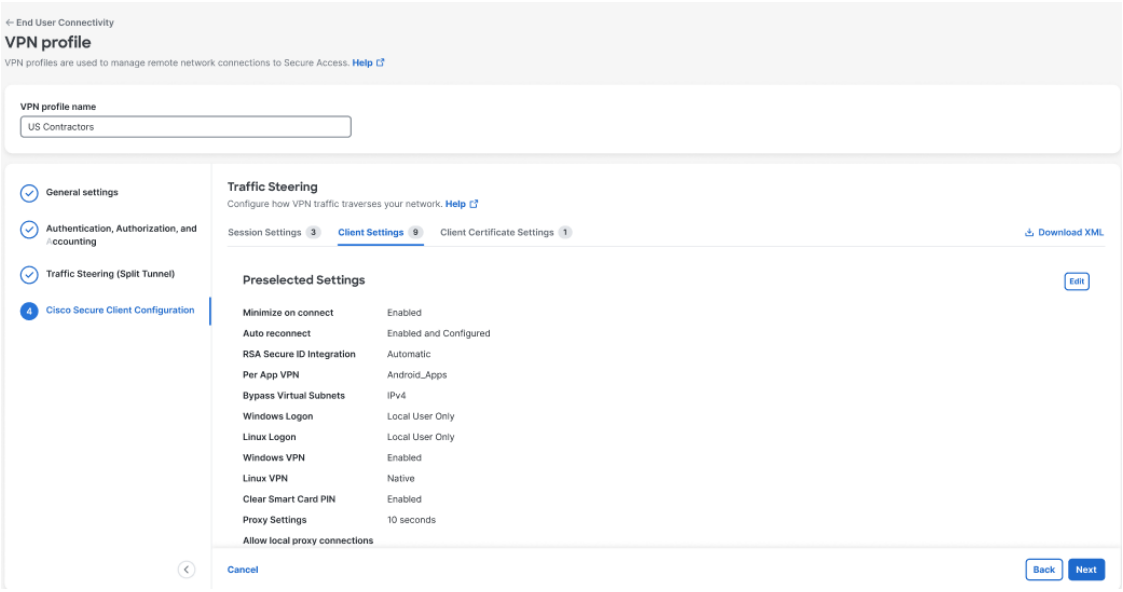
1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Choose a profile from the **VPN Profiles** list, click the ellipses **...** and choose **Edit**.
3. Click through the profile to the **Cisco Secure Client Configuration**.
4. Click the **Client Settings** tab then click **Edit** to modify client-specific settings. See The Cisco Secure Client Profile Editor for complete information about Cisco Secure Client settings.



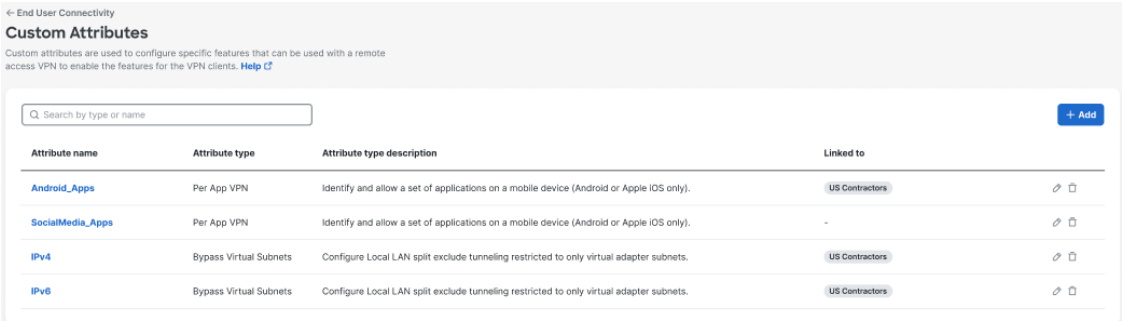
5. Check **Include Custom Attributes** and add the desired attributes to the VPN profile.



6. Click **Save**.



7. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network** and click **Custom attributes** to view the custom attributes available to VPN profiles from the **Custom Attributes** dashboard, which also includes which VPN profiles have assigned attributes in the **Linked to** column.



Manage Secure Client Scripts

Platform-specific Secure Client scripts enable you to automate the connection process, configure network settings, mount network drives, or enforce security policies.

Secure Access supports the upload and management of platform-specific Secure Client scripts that are used to automate the connection process, such as connecting to or disconnecting from a VPN. This functionality can be used for tasks such as configuring network settings, mounting network drives, or enforcing security policies.

Several types of files make up the Cisco Secure Client deployment:

- AnyConnect VPN, which is included in the Cisco Secure Client package.
- Modules that support extra features, which are included in the Cisco Secure Client package.
- Client profiles that configure Cisco Secure Client and the extra features, which you create.
- Language files, images, scripts, and help files, if you wish to customize or localize your deployment.
- ISE posture and the compliance module (OPSWAT).

For complete information on how to write and deploy scripts for Cisco Secure Client, see the *Customize and Localize Cisco Secure Client and Installer* chapter of the Cisco Secure Client (including AnyConnect) Administrator Guide.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- General understanding about how to write scripts and run them from the command line of the targeted endpoint to test them; for more information see the *Customize and Localize Cisco Secure Client and Installer* chapter of the Cisco Secure Client (including AnyConnect) Administrator Guide.

Guidelines and Limitations

Describes Guidelines and Limitations in Cisco Secure Access. There are some guidelines and platform limitations of which you should be aware when deploying scripts for Cisco Secure Client.

There are some guidelines and platform limitations of which you should be aware when deploying scripts for Cisco Secure Client.

- **Platform Support** – The scripting feature is available across multiple platforms, including Windows, macOS, and Linux-64. Be aware that Secure Client scripting is not compatible with macOS devices with Apple silicon chips, such as the M1 and M2. **Only macOS devices with Intel chips are compatible**.
- **Trigger Events** – Scripts can be set to run during events like VPN connection or disconnection.
- **Customization** – Administrators can create custom scripts tailored to their organization's specific requirements.
- **Security** – It is crucial to ensure scripts are secure and have the proper permissions to prevent misuse or security vulnerabilities.
- **Global deployment** – This feature is available on a global level for the entire organization, in all regions. For more detailed instructions about this feature and configuration, see Configure Secure Client Scripts.

Enable Secure Client Scripts

Provides instructions for completing the Enable Secure Client Scripts workflow in Cisco Secure Access. You enable the Secure Client scripts feature in the VPN profile, under the Cisco Secure Client settings.

You enable the Secure Client scripts feature in the VPN profile, under the Cisco Secure Client settings.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. Under **VPN Profiles**, choose a profile to edit.
3. Click **Cisco Secure Client Configuration** in the left panel.
4. Under **Client Settings**, check **Enable Secure Client Scripts**.
   a. Optionally, check **Terminate Script on Next Event** to enables Secure Client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running *On Connect* script if the VPN session ends and terminates a running *On Disconnect* script if Cisco Secure Client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the *On Connect* or *On Disconnect* script launched, and all their script descendants. On macOS and Linux, the client terminates only the *On Connect* or *On Disconnect* script; it does not terminate child scripts.
   b. **Enable Post SBL on Connect Script**, enabled by default, lets the client launch the *On Connect* script (if present) if SBL (Start Before Login) establishes the VPN session. The *On Connect* script is not launched from the SBL GUI but may be launched from the second GUI after login, depending on the *PostSBLScriptingBehavior*

preference; on Windows, it can mimic logon scripts, so administrators might suppress it in SBL mode to avoid redundancy. For more information, see About Start Before Login.

Upload Secure Client Scripts

Provides instructions for completing the Upload Secure Client Scripts workflow in Cisco Secure Access. This topic describes how to upload and manage the scripts that will run when Secure Client scripting is enabled.

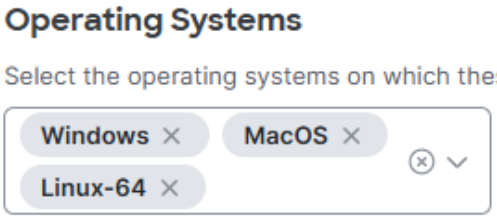
This topic describes how to upload and manage the scripts that will run when Secure Client scripting is enabled.

Procedure

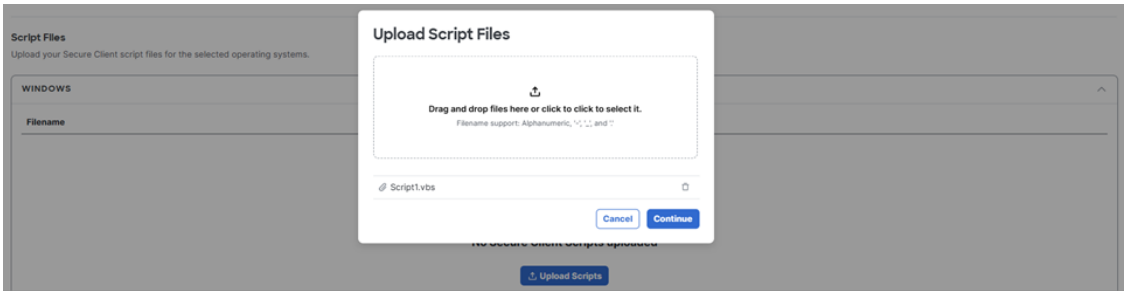
1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. In the **VPN Profiles** page, click **Settings** and choose **Secure Client Scripts** from the **Settings** drop-down.
3. Click **Upload Scripts**.
4. Under **Operating Systems**, select the operating systems on which these uploaded Secure Client scripts files will run. Supported options are:
   - Windows
   - macOS (Only macOS devices with Intel chips are compatible)
   - Linux-64

   Note

   You can select any or all options.

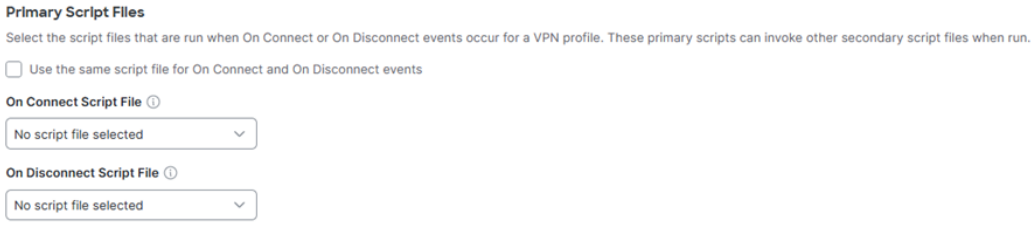
   

5. Under **Script Files**, upload your Secure Client script files for the selected operating systems.
   a. For a selected operating system, Windows for example, expand the applicable operating system pane and click **Upload Scripts**.
   b. In the **Upload Script Files** modal, you can drag and drop files there, or you can click to browse to a file location to select it.



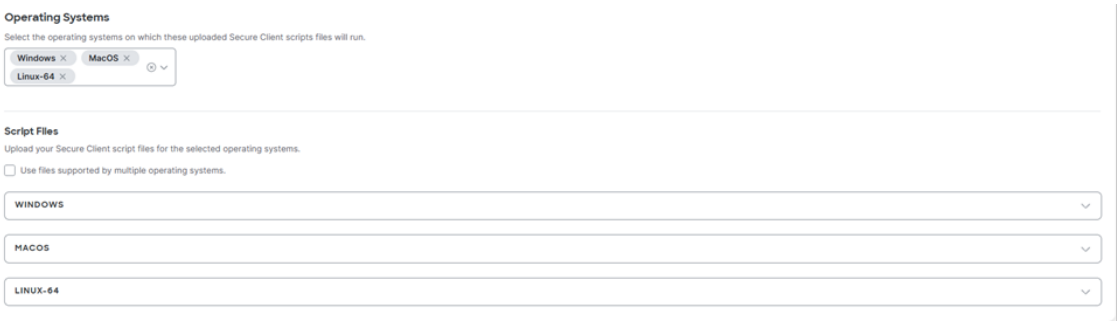
c. Optionally, you can designate a script as a primary file to run when *On Connect* or *On Disconnect* events occur. A primary script runs for a selected action and operating system. A primary script can be written to invoke more scripts.

1. Check **Use the same script file for On Connect and On Disconnect events** to simplify script selection.
2. Alternately, select a script for **On Connect Script File** and/or **On Disconnect Script File**.

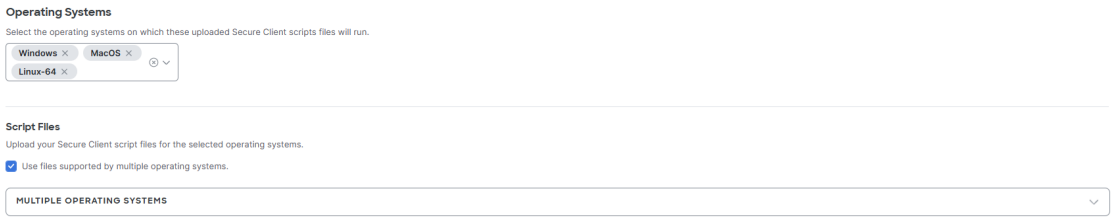


d. For multiple operating systems:

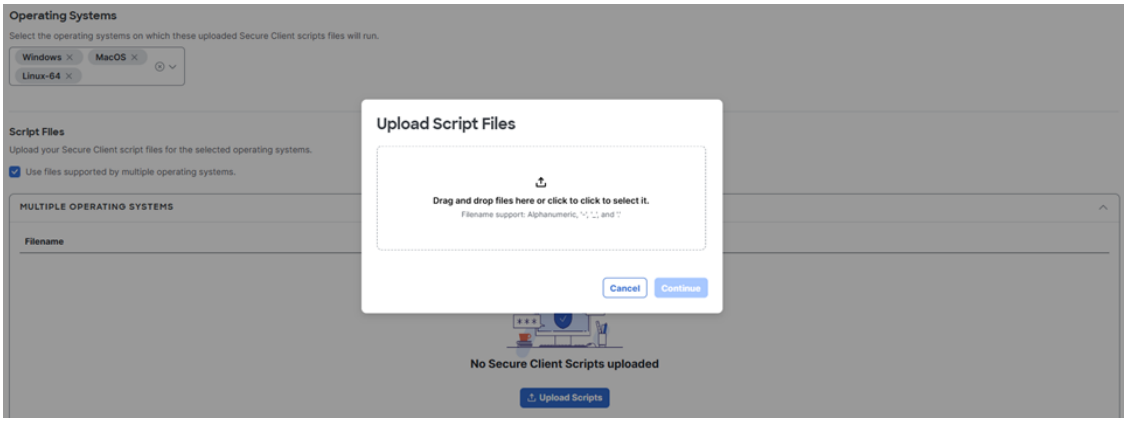
1. Select the operating systems on which scripts will run, then expand each operating system to upload scripts for that OS.



2. To use scripts that support multiple operating systems, check **Use files supported by multiple operating systems**, expand the multiple operating systems pane, and click **Upload Scripts**.



3. In the **Upload Script Files** modal, you can drag and drop files there, or you can click to browse to a file location to select it.



e. Click **Continue** to upload the scripts.

6. Click **Save** when you are finished to return to the listing page.

Manage VPN Connection Posture Profiles

Describes Manage VPN Connection Posture Profiles in Cisco Secure Access. Posture profiles define requirements for user devices when accessing resources and the network.

Posture profiles define requirements for user devices when accessing resources and the network.

Profiles in this list apply when users access specific resources using VPN. The VPN client must be installed on the end-user device. Requirements are checked when the device connects to the network.

VPN Posture Attributes

- Operating System
- Endpoint security agent
- Windows registry entries
- Firewall
- Disk encryption
- Files
- Processes
- Certificates

Add a VPN Connection Posture Profile

Provides instructions for completing the Add a VPN Connection Posture Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure a VPN connection posture profile to define posture requirements for end-user devices connecting to the network using VPN. The VPN client must be installed on the end-user device, and Secure Access checks the requirements when the device connects to the network.

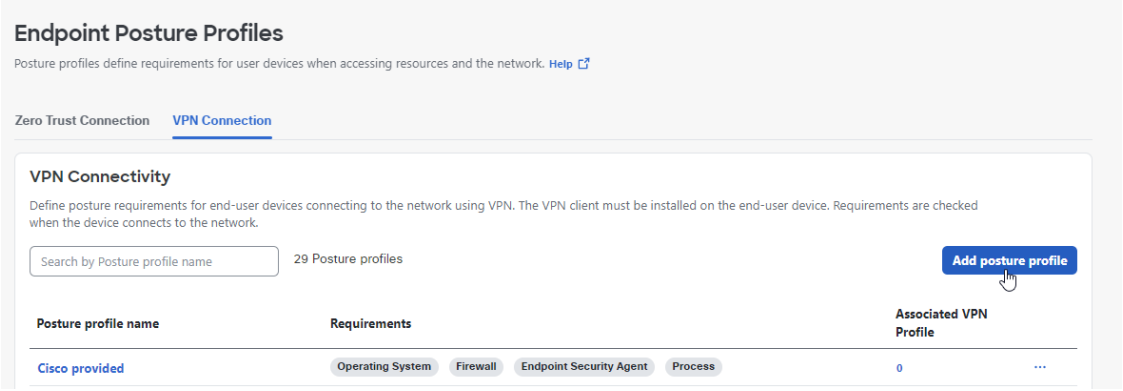
> **Note**
>
> Each requirement is optional. Configure requirements in any order. Endpoints must meet all conditions of any configured requirement.

Before you begin

- Full Admin role in Secure Access. For more information, see Manage Accounts.

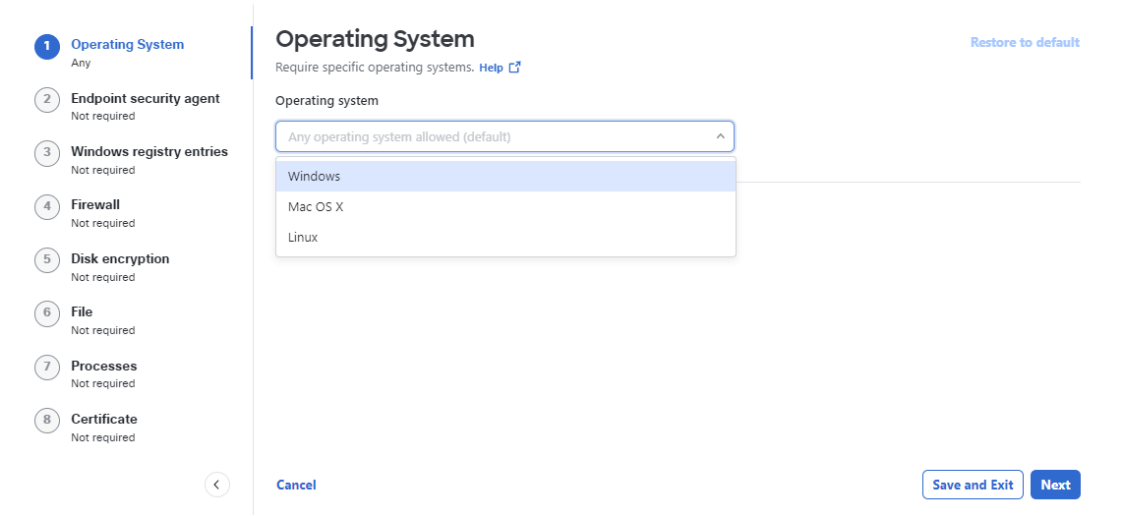
Procedure

1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.
2. For **VPN Connection**, click **Add Posture Profile**.



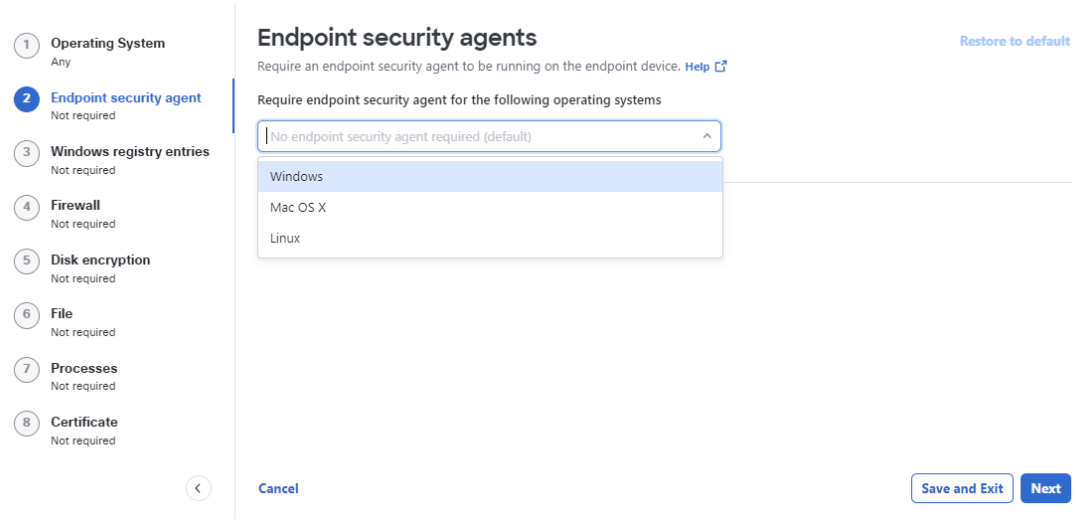
3. Give your posture profile a good descriptive **Name**.
4. For the **Operating System** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint security agents.

   For more information, seee Supported Operating Systems.



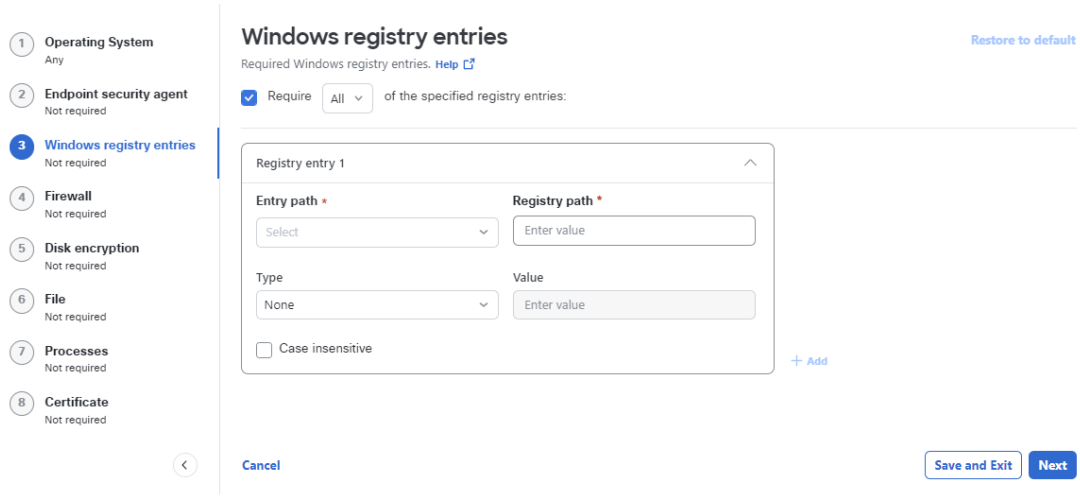
5. For the **Endpoint security agent** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select Windows registry entries.

   For more information, see Endpoint Security Agents.



6. For the **Windows registry entries** option, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint firewalls.

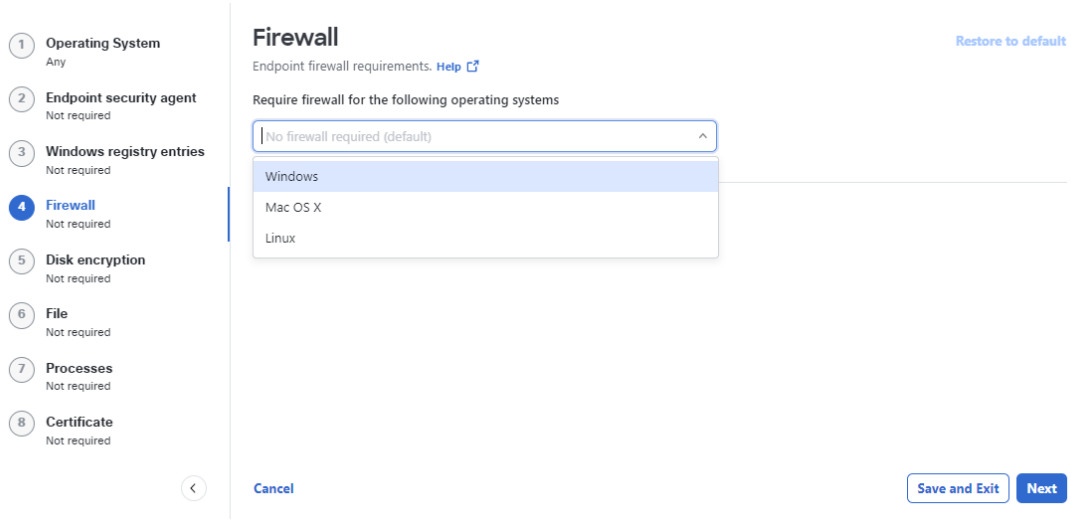
   For more information, see Windows Registry Entries.



> **Note**
>
> The posture check for the Registry Path only requires the navigation path to the directory containing the registry. The key name of the registry should **not** be included in the registry path.

7. For the **Firewall** option, choose the firewall for your profile. Click **Save and Exit** or **Next** to select disk encryption.

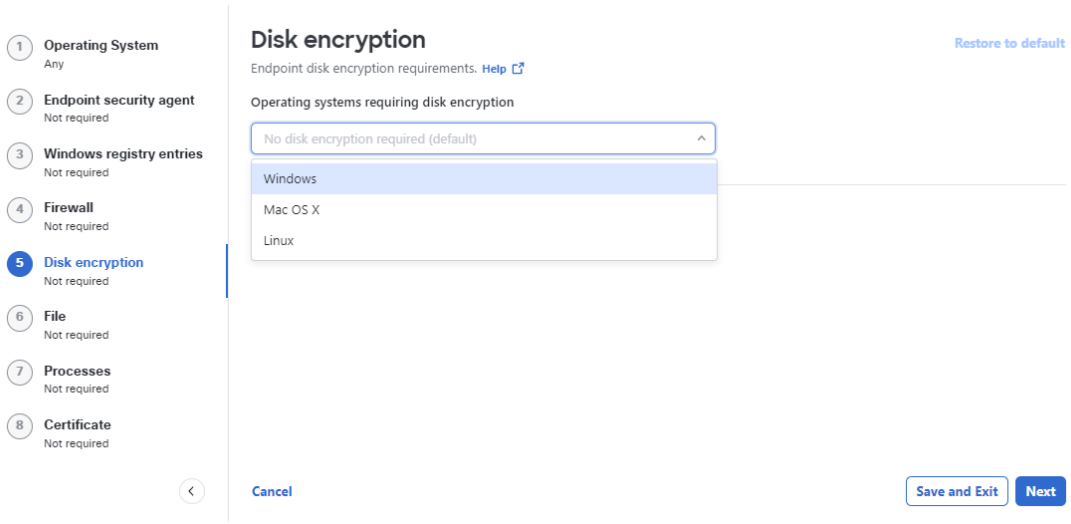
   For more information, see Firewall Requirements.



8. For the **Disk encryption** option, choose the disk encryption package(s) for your profile. Click **Save and Exit** or **Next** to configure any OS file requirements.

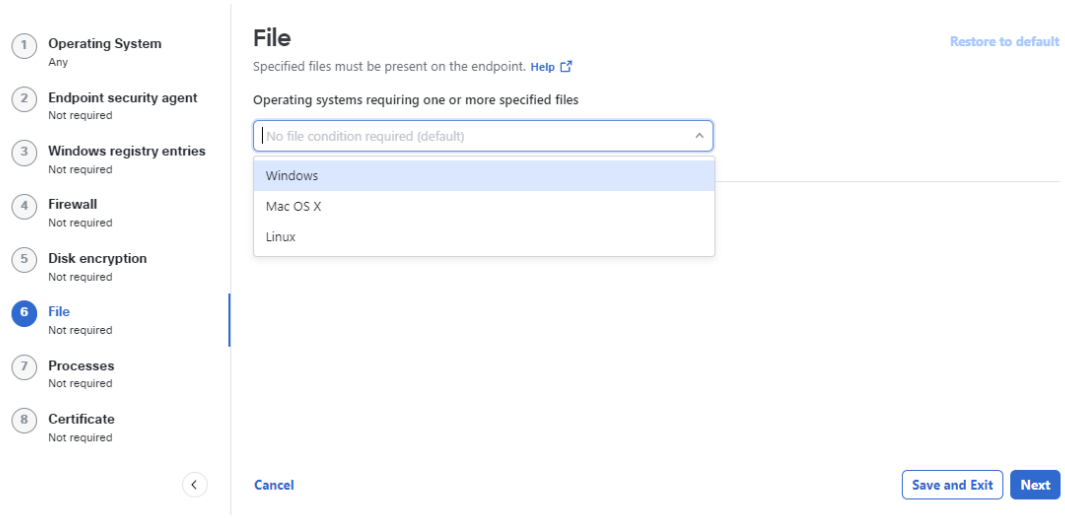
   For more information, see Disk Encryption.

> **Note**
>
> By default the disk encryption check only detects for the presence of disk encryption software but does not require that particular disk drives are encrypted. On a Windows platform it is possible to require that the default C:\ drive is encrypted. Reach out to your Cisco team for assistance.



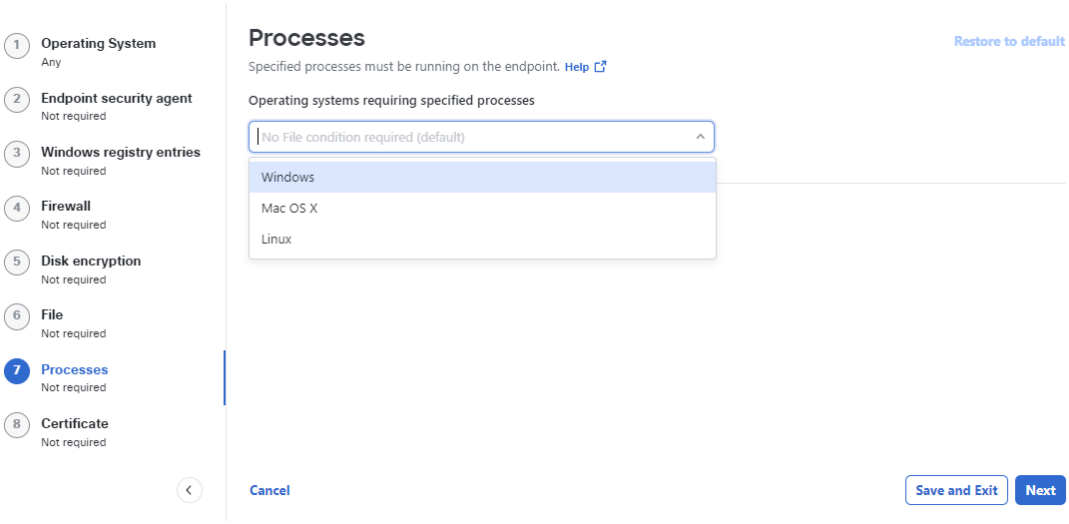
9. For the **File** option, specify any files that are required for the operating system. Click **Save and Exit** or **Next** to configure any OS process requirements.

   For more information, see File Requirements.



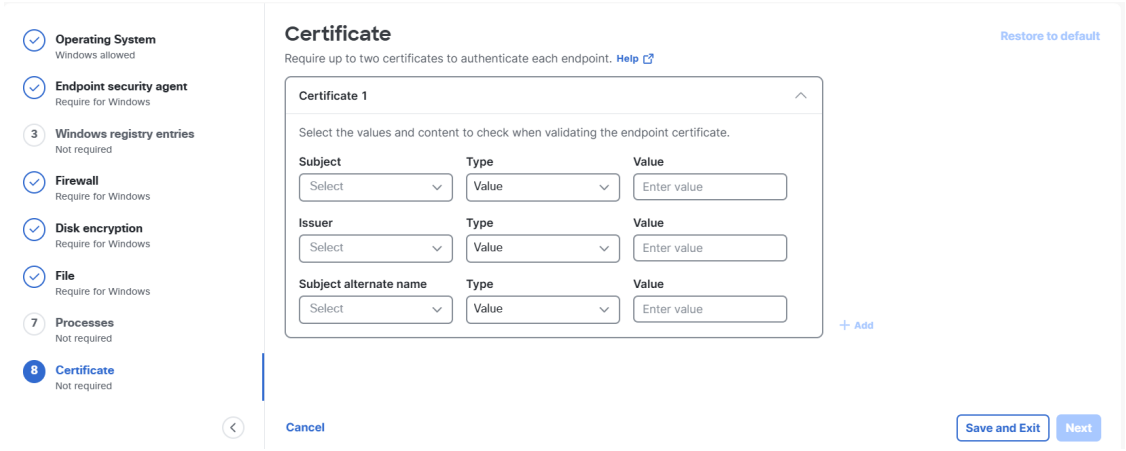
10. For the **Processes** option, specify any process that are required for the operating system. Click **Save and Exit** or **Next** to configure any endpoint certificates.

    For more information, see Process Requirements.



11. For the **Certificate** option, specify up to two certificates to authenticate each endpoint. Click **Save and Exit** or **Next** to return to the OS requirements.

    For more information, see Certificate Requirements.



> **Note**
>
> If you select **SAML attribute name** as a certificate type with the intention of using this profile in a VPN profile, the subject name must match the group attribute statement in your SAML application configuration.

12 Review and finalize the profile.

Manage Proxy Chaining

Deploy proxy-chaining for easier migration or proxy transparency for registered networks that do not use tunnels.

You can deploy proxy-chaining in your environment for easier migration or proxy transparency. Cisco Secure Access supports proxy-chain traffic on **Registered Networks only**. Since the **X-Forwarded-For (XFF)** HTTP header is not available for traffic sent through network tunnels, Cisco recommends that you do not send proxy-chain traffic through tunnels.

The Cisco Secure Access secure web gateway (SWG) leverages FQDN anycast routing to forward web traffic to the most optimal data center. If you use Secure Access DNS resolvers and your on-premises proxy supports an FQDN-based upstream proxy definition, use the **organization-specific FQDN anycast endpoint.**

Using the organization-specific FQDN pattern allows Cisco Secure Access to apply improved data center selection logic for your tenant. This helps reduce sub-optimal routing and improves connection reliability and performance. The improvement is especially beneficial for customers using reserved IPs and in environments where DNS-based steering is unavailable or inactive.

Network Requirements

- Configure your on-premises upstream proxy settings for FQDN anycast and **HTTP 80/443** on:
  - `swg-url-proxy-https-<org-id>.sseproxy.qq.opendns.com`
  - For instructions on finding your organization ID, refer to Find Your Organization ID.
- If you explicitly allowlist FQDNs in firewalls or ACLs, add the new organization-specific FQDN to avoid blocked connections.
- If you use a PAC file or proxy chain with the legacy FQDN hardcoded, update it to the new organization-specific FQDN to benefit from the improved reliability.

- Add a **Registered Network** in Secure Access that matches the public IP of your on-premises proxy NAT IP address. For more information, refer to Manage Registered Networks.
- Route the required URLs directly to the internet, not to the Secure Access secure web gateway. For more information, refer to Secure Access SAML Identity Provider Domains.
- If you use SAML authentication for single sign-on (SSO), send requests for `id.sse.cisco.com` to the Secure Access secure web gateway, not directly to the internet. For more information, refer to Secure Access SAML Gateway Services.

> **Note**
>
> The legacy FQDN below continues to work after your organization is enabled for the new pattern, but Cisco recommends updating hardcoded configurations to take advantage of the enhancement:
>
> - Legacy FQDN: `swg-url-proxy-https-sse.sigproxy.qq.opendns.com`

Forwarded-For (XFF) Configuration

Describes Forwarded-For (XFF) Configuration in Cisco Secure Access. You can configure the X-Forwarded-For (XFF) request header by using an on-premises proxy or a browser plugin such as Firefox's Simple Modify Headers plugin.

You can configure the X-Forwarded-For (XFF) request header by using an on-premises proxy or a browser plugin such as Firefox's **Simple Modify Headers** plugin.

When configured, the XFF header sets the internal IP address for traffic on a Registered Network (an egress IP). You must add these Registered Networks as sources in your internet access rules. Then, for traffic on the Registered Networks, the Activity Search report includes the internal IP addresses.

> **Note**
>
> Cisco Secure Access does not require the XFF header for deploying proxy chaining.

On-Premises XFF Header Configuration (No Plug-In)

For information about configuring the X-Forwarded-For (XFF) request header, see your proxy documentation.

Guidelines

To write the XFF header on HTTPS packets, configure internal clients for an explicit proxy and HTTPS decryption.

- Configure internal clients to forward web traffic to the proxy's internal network interface or a PAC file.
- For transparent proxy deployments, the proxy must provide Man-in-the-Middle (MitM) decryption.
- For HTTPS decryption to work correctly, import your Secure Access root certificate to your proxy. For more information, see Manage Certificates. Also, refer to your proxy documentation.

> **Note**
>
> If you are not using XFF headers (and instead using SAML or only external IP addresses to identify sources), you only have to enable HTTPS decryption on the proxies deployed in your cloud environments.

Browser Plugin XFF Header Configuration (No Proxy Chaining)

The browser plug-in approach is not scalable for production deployments and should be used for testing and troubleshooting only.

37 Zero Trust Access

Topics:

- Manage Client-Based Zero Trust Access in Secure Access
- Pre-login and Post-login Authentication to your Cisco Secure Client
- Traffic Steering for Zero Trust Access Client-Based Connections
- Manage User Trust Profile Zero Trust Access
- Manage Zero Trust Access Posture Profiles

Provides an overview of Zero Trust Access in Cisco Secure Access, including Manage Client-Based Zero Trust Access in Secure Access, Traffic Steering for Zero Trust Access Client-Based Connections, and Manage User Trust Profile Zero Trust Access. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Client-Based Zero Trust Access in Secure Access

Describes Manage Client-Based Zero Trust Access in Secure Access. Zero Trust Access means that no one is trusted by default, whether inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.

Zero Trust Access means that no one is trusted by default, whether inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. Enrolling in Zero Trust Access implies an enhanced level of security that reduces the attack surface by ensuring that only authenticated and authorized users and devices can access specific resources. This method aligns well with cloud adoption, remote work, and mobile device usage by securing access regardless of location.

Important

Customers that are new to ZTA now experience the broad match policy enforcement model to provide a more consistent, reliable, and efficient security enforcement experience. This update streamlines our infrastructure to ensure greater system stability while establishing a unified foundation for future platform enhancements.

Cisco Secure Client supports Zero Trust Access to private resources and internet resources from user devices. To use the Secure Client with Zero Trust Access on a supported device, a user must enroll in Zero Trust Access on the Secure Client. Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, SaaS apps, and internet resources protected by Secure Access. Secure Client is configured with various software modules. A Secure Client module may require the deployment of a certain profile to run module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Secure Client on an organization's user devices. For more information about the Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

What is ZTA and How Does it Compare to VPN?

Describes What is ZTA and How Does it Compare to VPN in Cisco Secure Access. Zero Trust Access (ZTA) and VPN share some similarities despite have independent purposes.

Zero Trust Access (ZTA) and VPN share some similarities despite have independent purposes. Both allow for remote access and encryption that allow for enhanced security. See the following benefits that come with enabling ZTA:

- Zero Trust Access is enabled for each private resource.
- Remote users connect to specific private resources rather than to an entire network, minimizing risk surface area.
- An attacker who breaches a device or zero-trust connection cannot glean information about your internal network.
- You can allow authorized users of unmanaged devices to connect to specific resources without granting them access to your network. You will enable browser-based zero trust access for those resources, then distribute a dummy URL to those users, so the real address is not exposed. This solution lets you securely provide browser-based access to end users such as:
  - Contractors, vendors, trainers, outside legal counsel, and others.
  - Employees on leave.
- End-users' endpoint/device posture is evaluated continuously to verify that the end-user device meets requirements. Posture can be assessed each time they access a resource, rather than just once when they join the network.
- When access to a resource is blocked, client-based users see a block page rather than a browser time-out error.
- Simpler setup and faster performance than VPN.
- Remote users can connect to internal resources in situations where they cannot use VPN. For example, an employee who is visiting a customer or vendor site can connect.
- Users do not need to log in separately to the network before they can access resources configured for zero trust access.

- After a user with a managed device has completed initial setup of Cisco Secure Client, the user has the same experience accessing a resource whether in the office or working remotely.

So why are they different and what would you need them for?

Zero Trust Network Access (ZTNA) provides access only to specific authorized applications, not the entire network, reducing the attack surface whereas VPN grants users access to the entire network or a network segment once connected, which can expose broad resources.

Furthermore, ZTA is mostly a clientless function that is accessible with just a web browser. It also hides applications from the internet, enforces least privilege access, and continuously assesses device posture and user context, enhancing security with direct connection to applications across the web and cloud or data centers; VPN primarily creates client-to-tunnels that can expose the network unnecessarily.

We strongly recommend utilizing VPN for environments with broad network access and network segmentation is limited. See the following scenarios where enabling VPN might be more beneficial:

- To allow end users to connect to all resources on the network that are not configured to disallow VPN access.
- To enable connections to private destinations that are not configured as private resources.
- To enforce some endpoint requirements that are not currently available in client-based zero-trust posture profiles.
- While transitioning your organization to Zero Trust Access.

Zero Trust Access Use Cases

Describes Zero Trust Access Use Cases in Cisco Secure Access. To allow these users to access the resource, use the solutions described on this page to ensure that the egress IP address associated with their devices is within your organization's IP address space.

To allow these users to access the resource, use the solutions described on this page to ensure that the egress IP address associated with their devices is within your organization's IP address space. Read through the following use cases and required licenses for a full explanation of functionality.

Multi-site Environments

If you organization has multiple Active Directory sites then the IP address of the client (the LDAP source IP) can affect the resultant selection of AD Site and therefore the selected domain controllers. Consider the IP address of the client in different deployment modes:

- **Network Tunnels** - In Network Tunnel mode the client IP will be affected by NAT. The source IP will be replaced with an IP address from the CGNAT IP address range. Therefore clients will typically be associated with the “Default Site” in Active Directory. The Domain Controllers in the default site must be accessible in the Access Policy.
- **Resource Connectors** - In Resource Connector mode the client IP will be affected by NAT. The source IP will be the Resource Connector IP address. The IP address of the resource connector(s) should be assigned to an appropriate AD Site in Active Directory Sites & Services. The Domain Controllers in this site must be accessible in the Access Policy.

> **Note**
>
> While you can sustain multiple site environments note that having duplicate destinations associated with a resource connector may affect mobile functionality with Secure Private Access.

Allow Zero Trust Access connections with private access

In short, this is a client-based ZTA method that enables users to securely access private applications without needing to install a client. When you configure a Private Resource, Secure Access automatically adds an entry for each configured

resource address for client-based zero-trust access to the Traffic Steering page to direct end-user traffic to the resource. With this scenario you can support the following environments:

- Allow private access of private resources over ZTA.
- Allow internet destinations to be defined as private resources and access those internet destinations over resources connectors.

> **Note**
>
> You **must** have a private access license.

Allow Zero Trust Access connections with secure internet access

Secure internet access ensures safe, policy-driven internet connectivity for users anywhere. This case protects access to internet and SaaS resources, while private access secures internal applications and resources. Review the following supported use cases for this scenario:

- Disable ZTA at the profile level to prevent ZTA from intercepting or examining any traffic with an internet destination.
- Use ZTA for all traffic with an internet destination for examination.
- Use ZTA to intercept traffic for specific internet destination, as specified with an exception.

Note that mobile platforms currently **do not** support secure internet access steering that uses "all" as a wildcard for internet destinations.

See Traffic Steering for Zero Trust Access Client-Based Connections for more information.

> **Note**
>
> You **must** have an internet access license.

Block Experience with ZTA

Describes both blocked activity and block HTTPS pages with Zero Trust Access in Cisco Secure Access. Blocked traffic and resulting events generate events that can be examined or acted upon; also, you can block specific URLs and websites with either a rule or security profile configured to block within your access policy but ZTA does not enforce block actions at the DNS level.

Default Block Action

ZTA blocks traffic through a combination of traffic steering, rules attributed to the access policy, and enforcement modes. Where traffic steering and interception determines if ZTA should handle a traffic request before the request is authorized, either by a destination match or exclusion configured as part of your traffic steering, the access policy evaluates if traffic should be permitted post-interception based on explicit rules, matching criteria in rules, or specific rule order.

Intercepted traffic that doesn't explicitly match any custom access policy rules is default blocked by the system policy. This specific case triggers a ZTA remediation flow to evaluate and identify the reason for denied access. If this occurs for multiple requests simultaneously, the system can experience overwhelming load due to the expensive nature of the remediation flow. In such a scenario, remediation is throttled at an organization level during this increased window and a generic `Access was blocked by the default rule` block reason is reported in the Activity Search logs.

Block Enforcement Pages

You can block specific URLs and websites with either a rule or security profile configured to **block** within your access policy but ZTA does not enforce block actions at the DNS level. This generates a blank web page instead of the expected block page.

To block HTTPS pages with a ZTA security profile, you must Configure End-User Notifications so the Decryption setting is set to **End-User Notification Only**.

Cached Block Verdict Types for ZTA

The Zero Trust Access module caches blocked verdicts to reduce the load from client interception and cloud enforcement.

Table 16: Blocked Verdict Types and Cache Intervals

Block Type	Verdict Cache Interval	Verdict Cache Scope
Geolocation-based	5 minutes	Global
No matching access policy rule	1 minute	Global
Explicit block rule	5 minutes	Process
Time-based	1 minute	Global
DNS errors	1 minute	Global
Resource matching or definition issue	5 minutes	Global
General policy and posture based blocks	30 seconds	Process

This function is only available on desktop platforms running Client version 5.1.17 and later. For more information about supported features on desktop and mobile platforms, see Zero Trust Access Requirements and Limitations on page 1207.

Regional Static IP for Client-based ZTA for Edgev2

For users implementing client-based ZTA on an Edge v2 infrastructure, a fixed public IP address tied to a specific geographic cloud region might be required. Predictable IPs like this can improve operational efficiency and reliability for distributed operations. This applies the two following use cases:

- Organizations without a default route per region.
- Organizations with a default route and a restrictive firewall that does not support FQDN-based rules. Any IP range must be added to the Access Control List (ACL).

Refer to the following table for available IP addresses per region.

Table 17:

Device	Device Identifier in Secure Access	IPv6	IPv4
bom1	csc-aps1-1-0	2603:5001:3030:6::/64	163.129.198.90/32, 163.129.198.91/32, 163.129.198.92/32, 163.129.198.93/32, 163.129.198.94/32, 163.129.198.95/32, 163.129.198.114/32, 163.129.198.115/32, 163.129.198.116/32, 163.129.198.117/32, 163.129.198.118/32, 163.129.198.119/32
den3	csc-usc1-1-1	2603:5000:3080:6::/64	163.129.226.90/32, 163.129.226.91/32, 163.129.226.92/32, 163.129.226.93/32, 163.129.226.94/32, 163.129.226.95/32, 163.129.226.114/32, 163.129.226.115/32, 163.129.226.116/32, 163.129.226.117/32, 163.129.226.118/32, 163.129.226.119/32
dfw2	csc-usc1-1-0	2603:5000:3060:6::/64	163.129.203.90/32, 163.129.203.91/32, 163.129.203.92/32, 163.129.203.93/32, 163.129.203.94/32, 163.129.203.95/32, 163.129.203.114/32, 163.129.203.115/32, 163.129.203.116/32, 163.129.203.117/32, 163.129.203.118/32, 163.129.203.119/32
iad1	csc-use1-1-1	2603:5000:3020:3::/64	151.186.85.64/32, 151.186.85.65/32, 151.186.85.66/32, 151.186.85.67/32, 151.186.85.68/32, 151.186.85.69/32, 151.186.85.70/32, 151.186.85.71/32, 151.186.85.72/32, 151.186.85.73/32, 151.186.85.74/32, 151.186.85.75/32

Device	Device Identifier in Secure Access	IPv6	IPv4
jed2	csc-mec2-1-0	2603:5002:3000:3::/64	151.186.109.90/32, 151.186.109.91/32, 151.186.109.92/32, 151.186.109.93/32, 151.186.109.94/32, 151.186.109.95/32, 151.186.109.114/32, 151.186.109.115/32, 151.186.109.116/32, 151.186.109.117/32, 151.186.109.118/32, 151.186.109.119/32
kix1	csc-apne1-1-1	2603:5001:3010:6::/64	151.186.121.90/32, 151.186.121.91/32, 151.186.121.92/32, 151.186.121.93/32, 151.186.121.94/32, 151.186.121.95/32, 151.186.121.114/32, 151.186.121.115/32, 151.186.121.116/32, 151.186.121.117/32, 151.186.121.118/32, 151.186.121.119/32
lax2	csc-usw1-1-0	2603:5000:3000:3::/64	151.186.93.90/32, 151.186.93.91/32, 151.186.93.92/32, 151.186.93.93/32, 151.186.93.94/32, 151.186.93.95/32, 151.186.93.114/32, 151.186.93.115/32, 151.186.93.116/32, 151.186.93.117/32, 151.186.93.118/32, 151.186.93.119/32
lhr1	csc-euw2-1-0	2603:5002:3030:6::/64	163.129.222.90/32, 163.129.222.91/32, 163.129.222.92/32, 163.129.222.93/32, 163.129.222.94/32, 163.129.222.95/32, 163.129.222.114/32, 163.129.222.115/32, 163.129.222.116/32, 163.129.222.117/32, 163.129.222.118/32, 163.129.222.119/32

Device	Device Identifier in Secure Access	IPv6	IPv4
maa1	csc-aps1-1-1	2603:5001:3020:6::/64	163.129.194.90/32, 163.129.194.91/32, 163.129.194.92/32, 163.129.194.93/32, 163.129.194.94/32, 163.129.194.95/32, 163.129.194.114/32, 163.129.194.115/32, 163.129.194.116/32, 163.129.194.117/32, 163.129.194.118/32, 163.129.194.119/32
man2	csc-euw2-1-1	2603:5002:3040:6::/64	163.129.234.90/32, 163.129.234.91/32, 163.129.234.92/32, 163.129.234.93/32, 163.129.234.94/32, 163.129.234.95/32, 163.129.234.114/32, 163.129.234.115/32, 163.129.234.116/32, 163.129.234.117/32, 163.129.234.118/32, 163.129.234.119/32
mia2	csc-use1-1-0	2603:5000:3030:3::/64	151.186.81.64/32, 151.186.81.65/32, 151.186.81.66/32, 151.186.81.67/32, 151.186.81.68/32, 151.186.81.69/32, 151.186.81.99/32, 151.186.81.100/32, 151.186.81.101/32, 151.186.81.102/32, 151.186.81.103/32, 151.186.81.104/32
nrt3	csc-apne1-1-0	2603:5001:3000:6::/64	151.186.117.90/32, 151.186.117.91/32, 151.186.117.92/32, 151.186.117.93/32, 151.186.117.94/32, 151.186.117.95/32, 151.186.117.114/32, 151.186.117.115/32, 151.186.117.116/32, 151.186.117.117/32, 151.186.117.118/32, 151.186.117.119/32

Device	Device Identifier in Secure Access	IPv6	IPv4
ord2	csc-use2-1-0	2603:5000:3070:6::/64	163.129.215.90/32, 163.129.215.91/32, 163.129.215.92/32, 163.129.215.93/32, 163.129.215.94/32, 163.129.215.95/32, 163.129.215.114/32, 163.129.215.115/32, 163.129.215.116/32, 163.129.215.117/32, 163.129.215.118/32, 163.129.215.119/32
ruh1	csc-mec2-1-2	2603:5002:3020:6::/64	151.186.126.90/32, 151.186.126.91/32, 151.186.126.92/32, 151.186.126.93/32, 151.186.126.94/32, 151.186.126.95/32, 151.186.126.114/32, 151.186.126.115/32, 151.186.126.116/32, 151.186.126.117/32, 151.186.126.118/32, 151.186.126.119/32
sjc6	csc-usw1-1-1	2603:5000:3010:3::/64	151.186.89.64/32, 151.186.89.65/32, 151.186.89.66/32, 151.186.89.67/32, 151.186.89.68/32, 151.186.89.69/32, 151.186.89.98/32, 151.186.89.99/32, 151.186.89.100/32, 151.186.89.101/32, 151.186.89.102/32, 151.186.89.103/32

Zero Trust Access with Captive Portal Detection

Describes Zero Trust Access with Captive Portal Detection in Cisco Secure Access. ZTA rules configured for Internet Access execute traffic interception that can hinder captive portal detection performed by the OS and remediation by the user.

ZTA rules configured for Internet Access execute traffic interception that can hinder captive portal detection performed by the OS and remediation by the user. For rules configured to **Use ZTA to secure all internet destinations** intercept all traffic by default. To allow for OS remediation to happen, the ZTA agent must detect captive portals itself and disable interception while the endpoint is in that condition.

The ZTA agent's Captive Portal Detection Service is responsible for detecting changes in endpoint captive portal conditions and starts when there is a network change. It detects by probing the following HTTP urls per platform:

- Windows: http://www.msftconnecttest.com/connecttest.txt

Response: "Microsoft Connect Test" with Status Code 200

- macOS and iOS: http://captive.apple.com

  Response: "<HTML><HEAD><TITLE>Success</TITLE></HEAD><BODY>Success</BODY></HTML>" with Status Code 200

- Android: http://connectivitycheck.gstatic.com/generate_204 Empty

  Response with Status Code 204

If the expected response is received, then it's deemed that the endpoint is **not** behind a captive portal. Otherwise if the initial probe times out (two seconds for DNS, two seconds for the remainder) or is otherwise inconclusive, probes will be retried at lower frequency until a response is received. If the initial probe returns any HTTP response that does not match the expected response, then it's deemed that the endpoint is behind a captive portal. The service then continues to probe frequently until it detects that the OS has remediated and the endpoint is no longer behind a captive portal.

> **Note**
>
> Captive portal detection service requires a network change debounce timeout that is shorter than the current 5 second default.

When endpoint is etected behind a captive portal, the ZTA agent disables interception for all `ProxyConfigs` to avoid intercepting captive portal remediation traffic. Interception resumes when it's detected that the endpoint is no longer behind a captive portal.

Zero Trust Access Logs

Describes Zero Trust Access Logs in Cisco Secure Access. When a Zero Trust Access request passes through the different services in Secure Access, various scenarios or configurations generate a variety of logs.

When a Zero Trust Access request passes through the different services in Secure Access, various scenarios or configurations generate a variety of logs. See the following explanations on how to investigate and process the logs created:

ZTA With Secure Private Access (SPA) Using Private Resources

- Zero Trust Access client-based logs for policy enforcement, verdicts and block reasons, as well as any handling issues that prevented enforcing at all.
- Firewall logs in case a security feature (IPS, Security profiles, DLP) is enabled for your Zero Trust Access traffic and is so passed through the firewall service for enforcement.

ZTA With Secure Internet Access (SIA) Using Internet Destinations

- Zero Trust Access client-based logs for request handling and any issues that come up for it, as well as global posture enforcement details in case of a posture block.
- Firewall or Secure Web Gateway (SWG) logs for the outcome of the Secure Access SIA stack policy evaluation, after Zero Trust Access as the headend has handed off the traffic for enforcement.
- DNS logs for the internet DNS resolution that happens at the Zero Trust Access proxy (which is done against the Secure Access resolvers).

These logs can be viewed in either the Activity Search Logs or the S3 Logs.

Zero Trust Access Requirements and Limitations

Describes Zero Trust Access Requirements and Limitations in Cisco Secure Access. Zero Trust Access has the following requirements that you must establish or confirm prior to enabling and configuring your environment.

Zero Trust Access has the following requirements that you must establish or confirm prior to enabling and configuring your environment.

Requirements

Secure Access requires at least the following minimum versions for supported platforms:

Table 18: Minimum Required Version for Supported OS

Supported Operating System	Required Minimum Version
Windows	10 11
macOS	11 12 13 13.3 **Note** See Cisco Secure Client (including AnyConnect) Administrator Guide
iOS	17.2
Linux	x64 **Note** IPv6-only is not supported on Ubuntu 24.0.4.
Android	12 with Knox 3.10; this version only supports KSP registration. 14 with Knox 3.11; this version supports unmanaged Knox and managed Knox with KSP only. 16 with Knox 3.12; this version supports unmanaged Knox and managed Knox with or without KSP.
ChromeOS	Android version (10)

To support the functionality in the table below, your devices must follow the following version minimums:

- Windows and Linux devices must support Trusted Platform Module (TPM) 2.0.
- Mac devices must support Secure Enclave.

Some functionality is reliant on the version of the managing platform. Review the table below for an overview of what functionality is supported per platform, and what version of Cisco Secure Client you must run to successfully utilize these functions.

Table 19: Table of supported ZTA Functionality and Required Versioning - Desktop

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
SAML Enrollment	Windows MacOS Linux	All versions.
Zero Touch Enrollment	Windows MacOS Linux	5.1.9+
Certificate-based Enrollment	Windows MacOS Linux	5.1.9+
Step-up Authentication	Windows MacOS Linux	All versions.
Trusted Network Detection (Secure Internet Access and Secure Private Access)	Windows MacOS Linux	5.1.10+ **Note** Virtual interface detection is only supported with version 5.1.13 and later.
Trusted Network Detection (DNS Server or DNS Domain)	Windows MacOS Linux	5.1.10+
Posture Profiles	Windows MacOS Linux	All versions.
Posture Profiles with DNS-over-HTTPS (DoH)	Windows MacOS Linux	5.1.8+
Posture Profiles with Duo Desktop	Windows MacOS Linux	All versions.
Posture Profile with Duo Desktop	Windows MacOS	All versions.

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
Pause ZTA with Cisco Secure Client	Windows MacOS Linux	5.1.13+
Custom ZTA Profiles	Windows MacOS	All versions.
Traffic Steering: Secure Private Access	Windows MacOS Linux	All versions.
Traffic Steering: Secure Private Access (DNS)	Windows MacOS Linux	5.1.16+
Traffic Steering: Secure Internet Access for specific internet destinations	Windows MacOS Linux	All versions.
Traffic Steering: Secure Internet Access for all internet destinations	Windows MacOS 26.5+ Linux	5.1.11+ MacOS requires 5.1.18+
Traffic Steering: Universal ZTNA (cloud or local)	Windows MacOS Linux	5.1.11+
Traffic Steering: Universal ZTNA (local only)	Windows MacOS Linux	5.1.11+
Network Location Objects	Windows MacOS Linux	5.1.19+
Cached Block Verdict Types	Windows MacOS Linux	5.1.17+

Table 20: Table of supported ZTA Functionality and Required Versioning - Mobile (Generic Android, iOS , ChromeOS)

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
SAML Enrollment	iOS Android ChromeOS	All versions.
Certificate Enrollment	iOS Android ChromeOS	5.1.19+ For more information about MDM enrollment and recommended configuration guidelines, see Configure iOS Settings in Mobile Device Manager (MDM) on page 1964and Configure Android Settings in MDM on page 1967 respectively.
Step-up Authentication	Android ChromeOS	All versions.
Posture Profiles	iOS Android ChromeOS	All versions.
Custom ZTA Profiles	iOS Android ChromeOS	All versions.
Traffic Steering: Secure Private Access	iOS Android ChromeOS	All versions.
Traffic Steering: Secure Internet Access for specific internet destinations	iOS Android ChromeOS	All versions.

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
Traffic Steering: Secure Internet Access for all internet destinations	iOS Android ChromeOS	iOS 26.5 **Note** Trusted server probes do not support certificate hash checks; only the first probe URL is used.
Trusted Network Detection (Secure Internet Access and Secure Private Access)	iOS Android ChromeOS	All versions. **Note** iOS does not support virtual interface detection, and multiple interface evaluation matches network fingerprint rules against a single OS-preferred adapter.
Pause ZTA with Cisco Secure Client	Android ChromeOS	All versions.

Note

For information on known issues in Client compatibility see the Secure Client Release Notes.

Table 21: Table of supported ZTA Functionality and Required Versioning - Android (Samsung)

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
Posture Profiles with DNS-over-HTTPS (DoH)	Android (Samsung)	(5.1.15+)*
Pause ZTA with Cisco Secure Client	Android (Samsung)	(5.1.18+)*
Traffic Steering: Secure Private Access (DNS)	Android (Samsung)	(5.1.15+)*
Traffic Steering: Secure Internet Access for all internet destinations	Android (Samsung)	(5.1.15+)*
Traffic Steering: Universal ZTNA (cloud or local)	Android (Samsung)	(5.1.15+)*

ZTA Functionality	Supported Platforms	Minimum Secure Client Version Required
Traffic Steering: Secure Private Access (Full)	Android (Samsung)	(5.1.15+)*
Trusted Network Detection (DNS Server or DNS Domain)	Android (Samsung)	(5.1.15+)*
Trusted Network Detection SPA	Android (Samsung)	(5.1.15+)*
Trusted Network Detection (Trusted Server)	Android (Samsung)	(5.1.15+)*

*: Requires Samsung device with Knox 3.13+.

For more information on Windows and MacOS support, see Get Started with Cisco Secure Client on Windows and MacOS Devices.

For network and client requirements, see Network Requirements for Zero Trust Access.

Limitations for Zero Trust Access

Consider the following limitations before you start utilizing Zero Trust Access:

- You can create a maximum of 100,000 rules per ZTA profile.
- You are limited to 20,000 private resources per organization.
- Users with MacOS as their platform need to note the following:
  - Only a single TND rule with either domains, DNS servers, or trusted server configuration is supported. The multiple TND rules, or a single TND rule with a combination of domains, DNS servers, and trusted servers, do not work.
  - TNDs with probe behave differently than other platforms, as Apple does not pause traffic if the request sent to the probe URL result is not an `HTTP 200 OK` response.
- You must have the appropriate licenses available. See Use Cases (/link) for more information.
- You must have the Cisco Secure Client installed.
- You must be enrolled for Zero Trust Access functionality.
- If both the client-based zero trust and VPN options are enabled for the resource:
  - If the client is installed on the user device and enrolled for zero trust access, the connection uses client-based zero trust access. Otherwise, the connection uses VPN.
  - If a client that is enabled for zero trust access cannot reach a resource that is configured for client-based zero trust access, the system does not attempt to connect using VPN
- If a private resource is not configured in Secure Access but the VPN client is installed on the end-user device, the user can access the resource using VPN if:
  - A profile with VPN traffic steering routes traffic to the applicable network address space.
  - A private access profile allows traffic to the applicable network address space.
- If a user accesses a resource with their browser using the address configured in a private resource for that purpose, the connection will always use browser-based zero trust access, even if Cisco Secure Client is installed.

- If a private access profile allows traffic to a destination that is not configured as a private resource, for example the destination is entered directly in a private access profile: Traffic may use zero trust access if the traffic steering for the destination has been added to the list on the **Connect** > **End User Connectivity** > **Zero Trust** page. See Manage Branch Connections for more information.

Post Zero Trust Access Enrollment Action Items

Describes Post Zero Trust Access Enrollment Action Items in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

After you've enrolled in ZTA, we strongly recommend the following action items to ensure total security and performance:

- Cisco Secure Client Overview
- Configure Timeout Intervals for ZTA Sessions
- Network Authentication for ZTA
- Create and Add a Private Resource
- Configure Client-Based Zero Trust Access for Private Destinations
- Manage Zero Trust Access profiles
- Get Started With Private Access Rules
- Manage User Authentication Profiles
- Manage Threat Defense Devices for Universal Zero Trust Network Access

Pre-login and Post-login Authentication to your Cisco Secure Client

Configure login authnetication with ZTA and the Cisco Secure client for when you either want to authenticate the user and device before or after the user logs in.

Traffic Steering for Zero Trust Access Client-Based Connections

Describes Traffic Steering for Zero Trust Access Client-Based Connections in Cisco Secure Access. DNS Steering selectively directs matching DNS requests based on configured domains to a customer-defined private resolution path where you can resolve matching queries by using one or more specified internal DNS servers.

DNS Steering selectively directs matching DNS requests based on configured domains to a customer-defined private resolution path where you can resolve matching queries by using one or more specified internal DNS servers.

> **Note**
>
> Successful application connectivity still depends on follow-up hostname resolution, policy coverage, and reachability of the returned endpoints through the intended ZTA path. DNS Steering affects how queries are routed, not the DNS records themselves or their authoritative source.

We strongly encourage you to utilize DNS Steering when an applications depends on DNS records to resolve interal services like the following:

- When the client must discover a service endpoint before connecting.

- When the service records exist only in internal DNS.
- When DNS responses return target hostnames that require additional A, AAAA, or CNAME lookups and subsequent connections.
- When the same user population is already using ZTA and you want to reduce VPN dependence for discovery-based workflows.

In Cisco Secure Access, Zero Trust traffic steering rules apply only for Client-based Zero Trust Access (ZTA) connections to internal destinations that are configured as private resources. When you configure a Private Resource, Secure Access automatically adds an entry for each configured resource address for Client-based ZTA to the Zero Trust Traffic Steering page, in order to direct end-user traffic to the resource.

View the traffic steering rules, but in most cases you should not edit the rules on the **End User Connectivity** > **Zero Trust** page. For more information, see Best Practices.

Use Cases for DNS Steering

Important

If you edit entries that were automatically added to this page when you configured a Private Resource, the traffic steering rules for the resource are not updated when you make future edits to the Private Resource configuration page.

If you change the destination address on the Zero Trust Traffic Steering page, the original Private Resource will not have a traffic steering rule and Client-based ZTA connections to that resource will not occur even if configured in the resource.

AD Controller Discovery

Discover an appropriate domain controller over ZTA without requiring a full VPN connection solely for private DNS resolution. The client sends the service discovery request to the private resolution path, receives domain controller hostnames from internal DNS, and then proceeds with normal identity traffic to the returned hosts.

There may be other enterprise applications that rely on internal discovery records can find the correct service endpoint without requiring users to know the final hostname in advance. Internal discovery records are resolved through the intended private DNS path, allowing the application to continue with its normal connection logic after discovery completes.

Kerberos Dependent Authentication

Identity workflows that depend on Kerberos service discovery while working remotely through ZTA after sign-in. DNS steering preserves that discovery path for supported post-login workflows prior to authentication.

LDAP Directory Lookups

Enterprise applications that use LDAP often rely on DNS service records to locate directory services without hardcoding individual server names. By locating the internal DNS and then connecting to the returned directory server, you can steer the relevant discovery namespace allows this pattern to work over ZTA.

Best Practices

Describes Best Practices in Cisco Secure Access. We recommend the following as best practices and further explanations on how to configure a Zero Trust Access profile.

We recommend the following as best practices and further explanations on how to configure a Zero Trust Access profile.

Private Resources in ZTA

In general, you should not add destinations directly to the Zero Trust traffic steering page. Instead, add a Private Resource. For more information, see Add a Private Resource.

- The private resource address to edit must be configured as a wildcard fully-qualified domain name (FQDN).

- You should not edit entries on the zero-trust traffic steering page, except for the following purpose:

  Edit entries on the Zero Trust traffic steering page if you have configured the access address for a Private Resource as a wildcard FQDN of the format **.example.com* and you want to exclude specified subdomains from Client-based ZTA. For example, you might want to exclude your company's public URL, www.example.com, from Zero Trust Access.

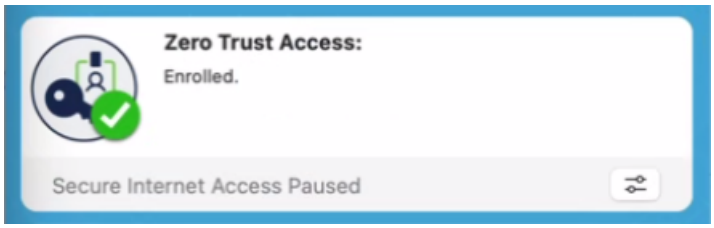
  For instructions, see Using Wildcards to Configure Traffic Steering for Private Destinations.

Pause ZTA with Cisco Secure Client

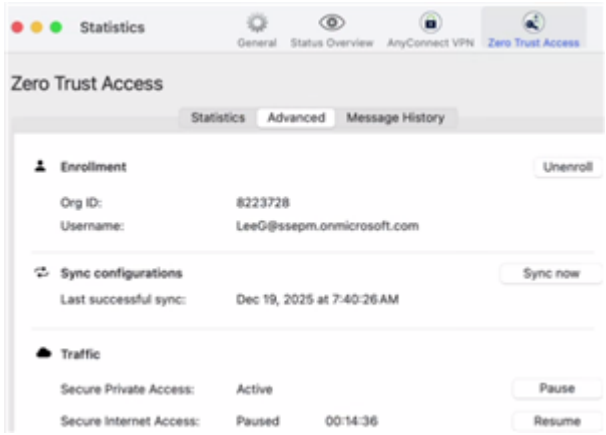
You can configure a ZTA profile to either permanently or temporarily pause ZTA enforcement and still utilize the traffic steering configured for a specific profile with the **Enable Cisco Secure Client end user pause** function. This allows you to independently configure pause settings for both secure internet access and secure private access; each of these options are available when editing or creating a ZTA profile. This allows you to investigate access concerns more effectively and allows you to control when and how the ZTA enforcement is active or not.

> **Note**
>
> You can enable the pause functionality for both Secure Private Access and Secure Internet Access independently of each other; both of these configurable settings are available in their respective steps when editing or creating a profile.

Once enabled in the profile and added to the access policy you can monitor and confirmed the enrolled or un-enrolled state of the pause function from the Cisco Secure Client application on your desktop.



Based on the different combinations of configurations available between pausing ZTA and enabling, or not enabling, Secure Internet Access within your profile then the messaging in your Client window may differ depending on the configuration you created. To view the specifics of the profile being enforced, open the Secure Client window on your desktop and click the connection icon for the Zero Trust Access module to view the advanced settings.



If traffic is paused by Trusted Network Detection, this action overrides the **Enable Cisco Secure Client end user pause** setting in your ZTA profile.

> **Note**
>
> If you update the Client version or restart the agent application on your laptop, the **Pause** function restarts as well.

Limits: Zero Trust Traffic Steering Rules

Describes Limits: Zero Trust Traffic Steering Rules in Cisco Secure Access. Secure Access allows a maximum number of Zero Trust traffic steering rules.

Secure Access allows a maximum number of Zero Trust traffic steering rules. For more information, see Limitations and Range Limits.

> **Note**
>
> Custom Zero Trust Access profiles created with the process described below contain traffic steering configurations that only impact the users or groups of users included in the custom profile and its impact on processing traffic is dependent on its priority amongst other profiles.

Windows or macOS

For Zero Trust connectivity on Windows or macOS, Secure Access recommends at most 25K traffic steering rules for the organization.

The organization can reduce the number of Zero Trust steering rules by using wildcards. For more information, see Using Wildcards to Configure Traffic Steering for Private Destinations.

If the organization has 100K Zero Trust traffic steering rules, Secure Access displays a notification.

iOS

For Zero Trust connectivity on iOS, Secure Access recommends at most 1K traffic steering rules for the organization.

If the organization has 5K Zero Trust steering rules, Secure Access displays a notification.

Android: Samsung, Chrome and Generic

For Zero Trust connectivity on Android, Secure Access recommends at most 1K traffic steering rules for the organization.

If the organization has 10K Zero Trust steering rules, Secure Access displays a notification and prevents the addition of more traffic steering rules.

Manage the DNS Steering Rule in a Zero Trust Access Profile

Provides instructions for completing the Manage the DNS Steering Rule in a Zero Trust Access Profile workflow in Cisco Secure Access. Beware of the following requirements or limitations: You must run Secure Client version 5.1.16 or newer to utilize this function.

DNS Steering is derived from destination lists and steering rules that determine where DNS queries are sent. These destinations can be private or public DNS servers or specific IP addresses or domain names that the DNS queries should be directed to. The steering destination is the endpoint for these DNS queries dictated by the steering policy. This is particularly useful in scenarios configured for secure private access where or private DNS resolution over ZTA and allows for the secure handling of private DNS resolution over Zero Trust Access (ZTA) by using established resolution paths such as internal DNS servers and RCGs. It supports all DNS record types, with particular emphasis on the common use case of SRV and discovery records.

You must create a DNS Steering Destination and then attach the destination to a ZTA profile; you cannot add or created a destination within the ZTA profile procedure. This enables effective control and monitoring of DNS-based traffic flows within the network environment. How these rules are configured affect the action made against traffic based on what traffic matches the rule and how the rules within the profile are ordered.

> **Note**
>
> Wildcard matching in DNS traffic steering destinations does not include exact-domain matching; it can represent only one token and cannot represent multiple tokens. When you add a domain like google.com to an allow list, it implicitly allows all subdomains like *.google.com, but if you want to block only a specific subdomain such as news.google.com, you must add the entire FQDN.

Use the following procedure to add, edit, or delete a DNS destination in the DNS settings tab of the ZTA profile.

Before you begin

Beware of the following requirements or limitations:

- You must run Secure Client version 5.1.16 or newer to utilize this function. Check the **About** icon inside your Cisco Secure Client module to view the Secure Client UI version.
- You must have the complete FQDN of the DNS destination set ready prior to creating a rule. This includes **domain name**, **DNS Server 1 IP address**, and an optional **DNS Server 2** for failover purposes. If you opt to use a Resource Connector Group (RCG), enter that information in place of the the domain servers.
- By adding a DNS destination and attaching it to a ZTA profile, the profile intercepts all DNS types that match the value you enter. If matching values are intercepted, the associated traffic is forwarded to the designated proxy.

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. In the **Zero Trust Access** tab of the window, click **ZTA Settings**.
3. In the ZTA Settings page, switch to the **DNS Steering** tab and click **+ DNS Steering Destination** to add a new destination.

   > **Note**
   >
   > To edit an existing DNS steering destination, click the edit icon for the destination you want to edit.
   >
   > To delete an existing DNS steering destination, click the delete icon for the destination. This completely removes the destination as a configurable destination from your organization.

4. Manually enter the domain you want as the **Destination**. This field specifies the FQDN that DNS queries are directed to.
5. Select one of the following options as your **Resolution Path**:
   - **DNS Server**: This option is ideal if you want to confirm the earliest possible checkpoint in a connection event without compromising aspects of your device that might not support ZTA or cannot guarantee security, such as laptop cameras or legacy systems. Expand the drop-down menu to select a DNS Server. If there are none available, click **+ Add** to add one. You must provide a **domain name**, **DNS Server 1 IP address**, and an optional **DNS Server 2** for failover purposes.

- **Resource Connection groups**: This option is preferable for secure, high-performance access to private applications with built in high availability, load balancing across multiple connectors, and a simplified network configuration. Expand the drop-down menu and select one of the connector groups available. To remove a connector group from the list once you've added one, simply click the remove icon next to the connector name.

> **Note**
>
> Resource connectors do not support some special characters such as "_"; we strongly recommend using an established DNS Server as the resolution path in your end target includes the special character.

6. (Optional) Assign the destination to a ZTA profile. Expand the **ZTA Profiles** drop-down menu and select a pre-existing profile.
7. Click **Save**.

What to do next

If you opt to not attach the DNS Steering Destination to a ZTA profile in step 7 of this procedure, create you ZTA profile and attach the steering destination. For more information see Add a Zero Trust Access Profile on page 1219.

If you are implementing Kerberos authentication wit Active Directory (AD), we **strongly** recommend adding the AD DNS SRV recorcd names to the DNS Steering you just created. For more information from Microsoft, see How to verify that SRV DNS records have been created for a domain controller for more information. Microsoft documents specific SRV DNS records for you, see 6.3.2.3 SRV Records specifically for more information.

Add a Zero Trust Access Profile

Provides instructions for completing the Add a Zero Trust Access Profile workflow in Cisco Secure Access. Zero Trust Access profiles provides distinct access experiences for different users and groups.

Zero Trust Access profiles provides distinct access experiences for different users and groups. You can view, edit, and delete the profiles for private and internet access.

Wildcard matching in ZTA profiles does not include exact-domain matchinng; it can represent only one token and cannot represent multiple tokens. When you add a domain like google.com to an allow list, it implicitly allows all subdomains like *.google.com, but if you want to block only a specific subdomain such as news.google.com, you must add the entire FQDN as your DNS steering destination.

Important

Be aware of the ZTA limitations when creating a profile. See Limitations and Range Limits for more information. You **must** be a **Full Admin** to proceed with this procedure. See Manage Accounts for more information.

Zero Trust Access profiles are an ordered list where the order of profiles determines their priority. The last profile in the list is always the Default ZTA Profile. A user's Zero Trust Access client receives settings from the first matching Zero Trust Access profile in profile order. The profile must match both the user's membership and the endpoint operating system. Default profile includes all users in the org and all client Zero Trust Access enabled private and internet resources . Use the following procedure to modify the user's access:

Procedure

---

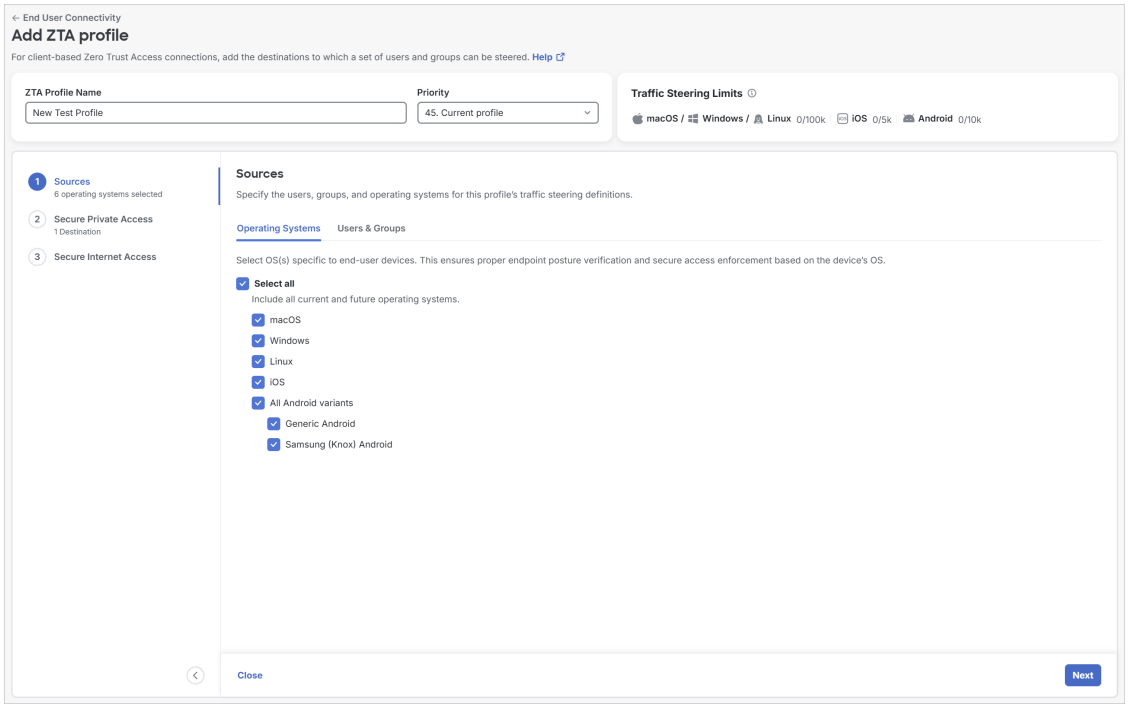
1. Navigate to **Connect** > **End User Connectivity**.

2. Click the **Zero Trust** tab.
3. To create a new profile, click **+ ZTA profile**.
4. Enter a unique **ZTA profile name** and select the rule priority that this profile will execute in. Note that this profile may not get triggered with incoming traffic if a rule with a higher priority is executed.
5. In the Sources section, configure both endpoint and user matching criteria:
   - **Operating Systems** – Select the endpoint operating systems that this Zero Trust Access profile applies to.

     Note

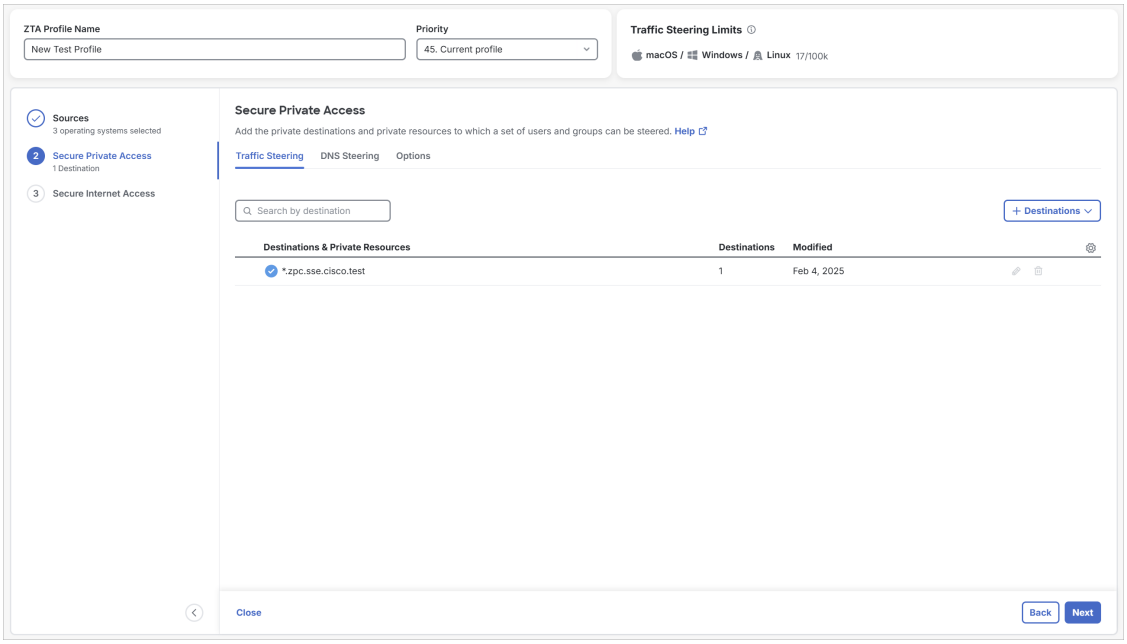
     To use specific operating systems in combination with DNS Steering and Use ZTA to secure all internet destinations , the user must run Cisco Secure Client 5.1.18 or later. For older clients, you must select all operating systems or remove these steering options.

   - **Users & Groups** – Click **+Users and groups** to add the users or groups that this Zero Trust Access profile applies to.

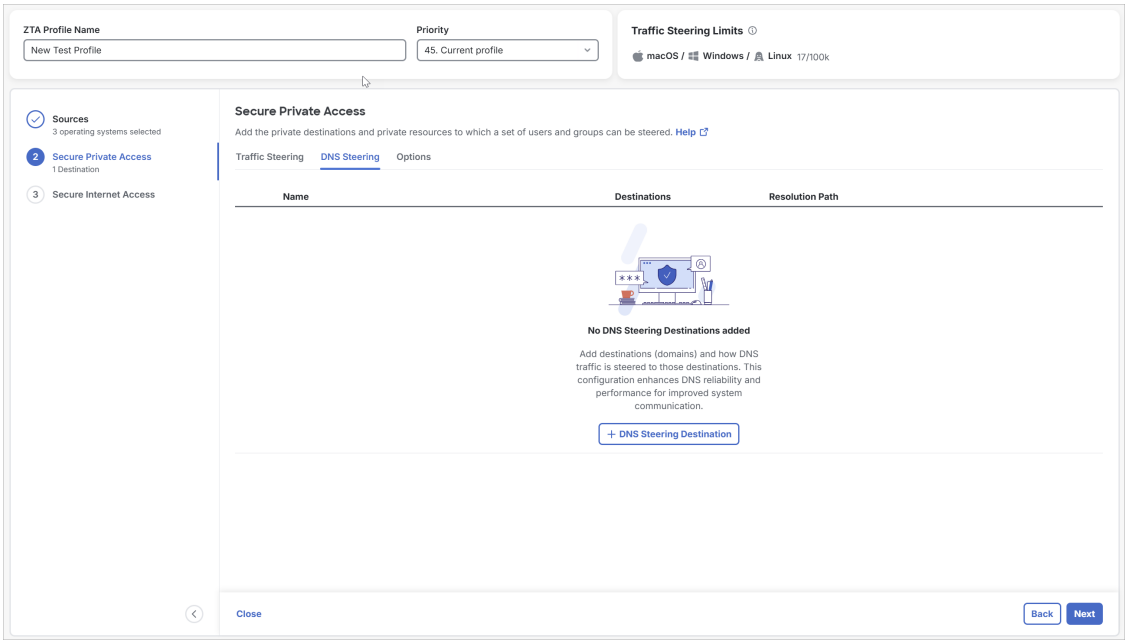


6. Click **Next**.
7. In the **Secure Private Access** window, click through the following tabs:
   - **Traffic Steering** – Click **+Destinations** to map in a destination for your rule. You can opt to add either a **Destination** or a **Private Resource**; you can also upload or download a CSV file to managed your exclusions. You must create the DNS destination outside of this ZTA profile. See Manage the DNS Steering Rule in a Zero Trust Access Profile for more information. There is no character-limit for destinations manually entered.

> **Note**
>
> Destinations in Zero Trust Access profiles are specifically used for traffic steering. For end user connectivity and access policy enforcement, use a corresponding private resource. You **must** create a private resource before you can add it to a Zero Trust Access profile. See Add a Private Resourcefor more information.



- **DNS Steering** – Click **+DNS Steering Destination** to map in a destination for your DNS trafficrule. Select the destination from the drop-down list and then click **Save**.



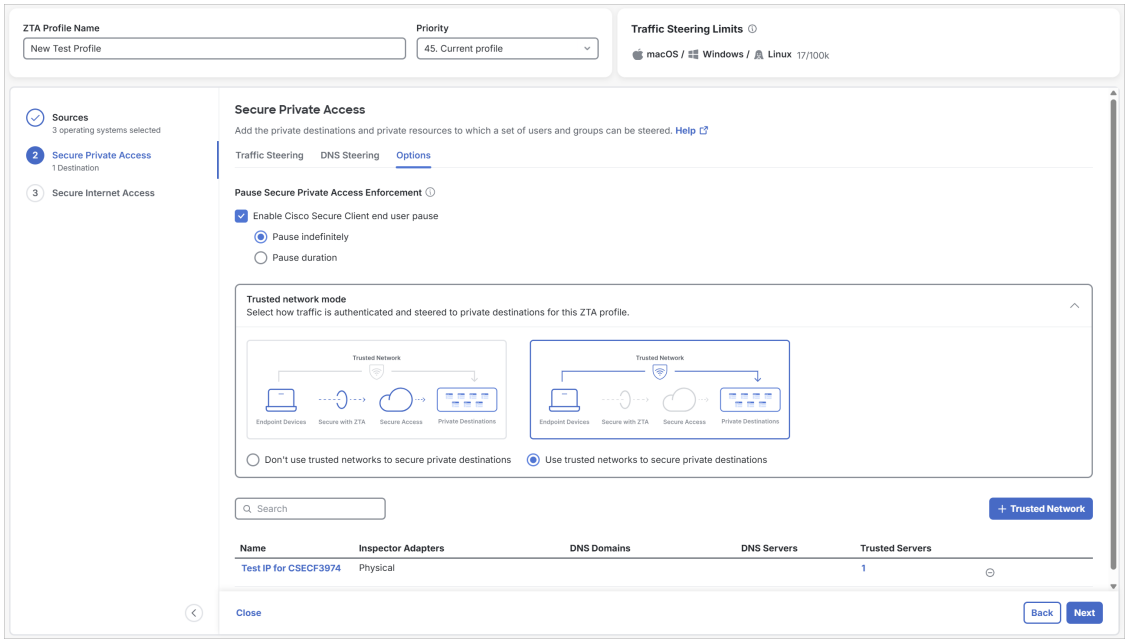
- **Options** – Configure whether the profile pauses ZTA enforcement and the network mode for traffic steering.
  - Check the **Enable Cisco Secure Client end user pause** action to pause Secure Private Access enforcement. You can check the type of enrollment you have in the Cisco Secure Client window. See Pause

ZTA with Cisco Secure Client on page 1216 for more information. If you opt to enable this feature, choose between one of the following modes:

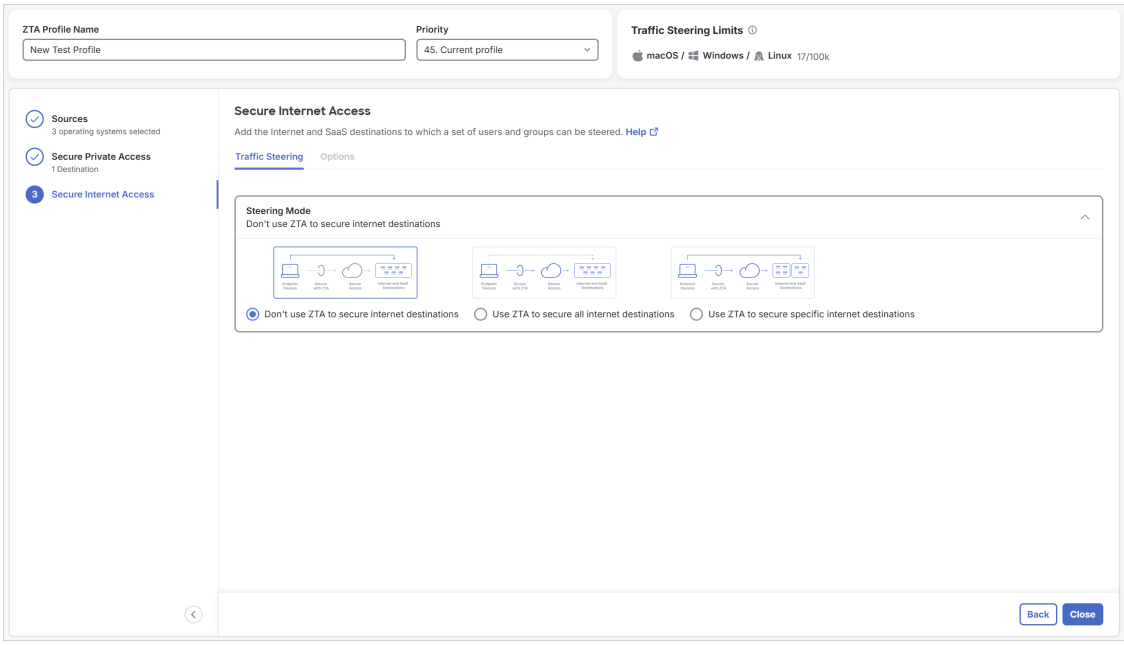
- **Pause indefinitely** - Forever pause Cisco Secure Client from enforcing private access of the ZTA profile.
- **Pause a time period** - Temporarily pause Cisco Secure Client from enforcing private access of the ZTA profile. The default value is fifteen minutes. Select the desired time period and click **OK** to save.

- **Trusted network mode** - Select either **don't use trusted networks to secure internet destinations** or **Use trusted networks to secure internet destinations**; this impacts how traffic is authenticated and steered to private destinations for this particular ZTA profile. The steering in this configuration does not affect or impact other profile configuration.

  To use trusted networks, click **+ Trusted Network**, select the required trusted networkfrom the drop-down list, and then click **Save**.



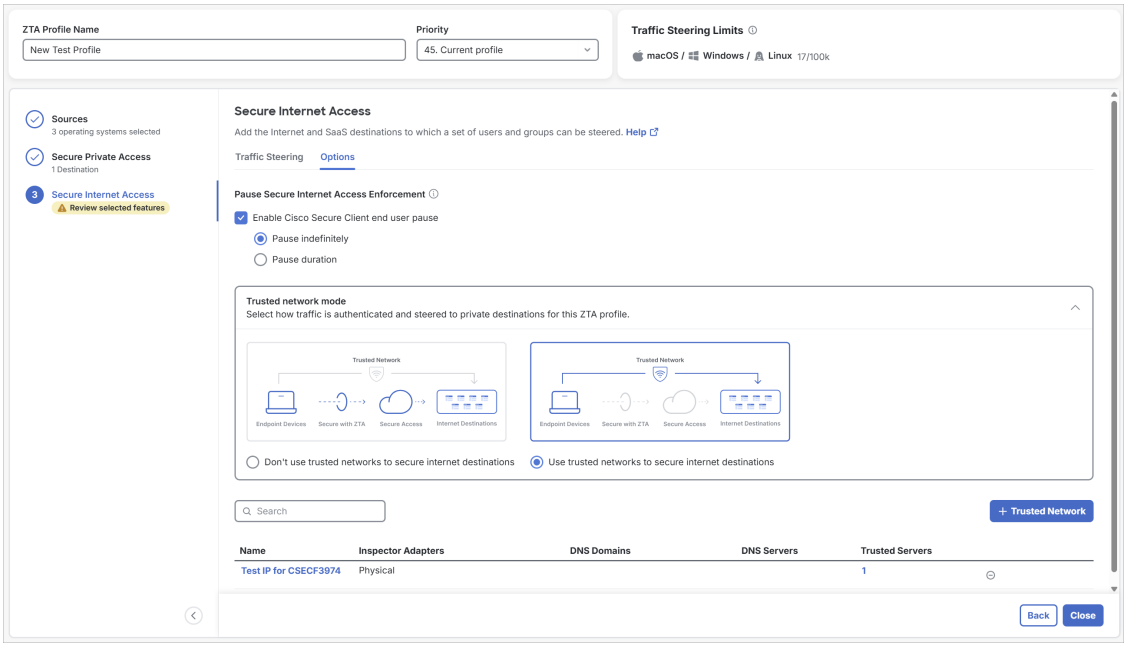
8. Click **Next**.
9. In the **Secure Internet Access** section, click through the following tabs and configure your traffic steering and pause settings for Secure Internet Access:
   - **Traffic Steering**- select one of the following traffic steering modes you want Zero Trust Access to implement
     - **Don't Use ZTA to secure internet destinations** - Zero Trust does not intercept or examine any traffic with an internet destination.
     - **Use ZTA to secure all internet destinations** - Zero Trust Access intercepts all traffic with an internet destination for examination.
     - **Use ZTA to secure specific internet destinations** - Zero Trust Access only intercepts traffic for certain internet destination, as specified with an exception.
     - **Exception** - Click **+ Exception** to include an IP address or IP address range that isexempted from the traffic steering method if you use ZTA. ○



- **Options** – Check the **Enable Cisco Secure Client end user pause** action to pause Secure Private Access enforcement. This is independent of the pause setting for Secure Internet Access. If you opt to enable this feature, choose between one of the following modes:
  - **Pause indefinitely** – Forever pause Cisco Secure Client from enforcing private access of the ZTA profile.
  - **Pause a time period** – Temporarily pause Cisco Secure Client from enforcing private access of the ZTA profile. The default value is fifteen minutes. Select the desired time period and click **OK** to save.

- **Trusted network mode** – Select either **don't use trusted networks to secure internet destinations** or **Use trusted networks to secure internet destinations**; this impacts how traffic is authenticated and steered to private destinations for this particular ZTA profile. The steering in this configuration does not affect or impact other profile configuration.

  To use trusted networks, click **+ Trusted Network**, select the required trusted networkfrom the drop-down list, and then click **Save**.



10. Click **Close**.
11. Optionally, if you want to delete an existing profile, navigate to a traffic steering rule, click the ellipsis **...** at the end of the table row, and then choose **Delete**.

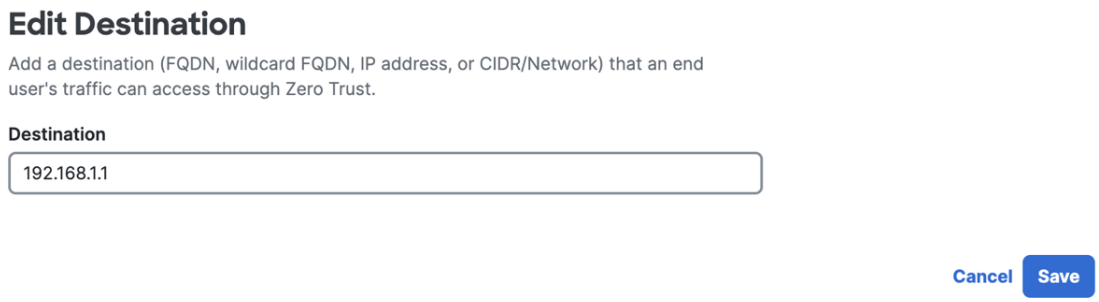
Edit a Zero Trust Traffic Rule

Provides instructions for completing the Edit a Zero Trust Traffic Rule workflow in Cisco Secure Access. You can edit a destination associated with the Zero Trust traffic rule.

You can edit a destination associated with the Zero Trust traffic rule. For more information, see Best Practices.

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. Click the **Zero Trust** tab, and then navigate to **Traffic Steering**.
3. Navigate to a traffic steering rule, click the ellipsis (**...**) at the end of the table row, and then choose **Edit**.
4. For **Edit Destination**, enter a fully-qualified domain name (FQDN), IP address, or CIDR block for the Zero Trust traffic steering rule.



5. Click **Save**.

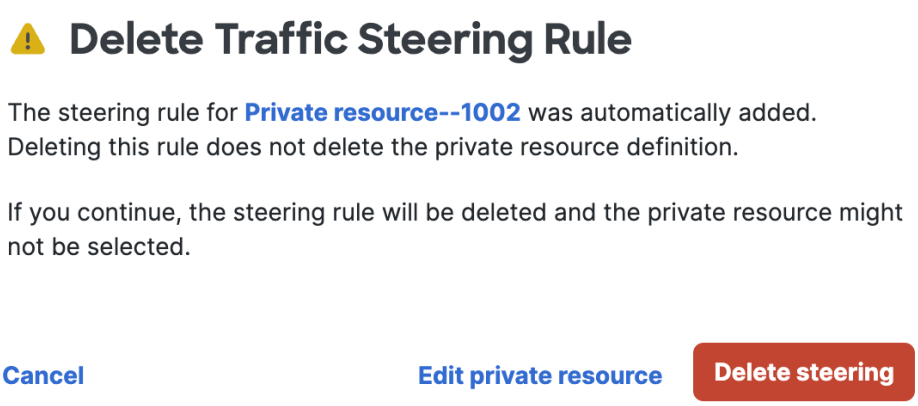
Delete a Zero Trust Traffic Rule

Provides instructions for completing the Delete a Zero Trust Traffic Rule workflow in Cisco Secure Access. You can remove a destination associated with the Zero Trust traffic rule.

You can remove a destination associated with the Zero Trust traffic rule.

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. Click on the **Zero Trust** tab, and then navigate to **Traffic Steering**.
3. Navigate to a traffic steering rule, click the ellipsis (**...**) at the end of the table row, and then choose **Delete**.



4. Click **Delete steering** to confirm the removal of the Zero Trust traffic steering rule.

Enable Client-Based Zero Trust Access to Destinations

Provides instructions for completing the Enable Client-Based Zero Trust Access to Destinations workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the following procedure to enable and allow client-based Zero Trust Access to both internet and SaaS destinations:

Procedure

1. Ensure that each destination site allows access from the egress IP addresses that your users' connections will use, as discussed in the Web Traffic and NATaaS section of Secure Access NAT as a Service.
2. Add the applicable destinations to one or more destination lists. See Manage Destination Lists and subtopics. URLs are treated as domains. Do not include addresses that are not publicly routable.
3. Install the latest version of Cisco Secure Client on user endpoint devices. Ensure that the client is enrolled in Zero Trust Access. See the applicable subtopics under Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices. Windows, macOS, iOS, and Android clients support this feature.
4. Navigate to **Connect** > **End User Connectivity** > **Zero Trust Access**. In the **Default Profile** section, click the **Edit** icon for the Default ZTA Profile. Go to the **Internet and SaaS Destinations** page of the wizard, and select one or more destination lists. Optionally, add any exceptions.
5. Define internet access rules for the destinations. You can specify the same destination lists that are specified in the ZTA profile.

What to do next

Keep the following points in mind:

- URLs in destination lists are treated as domains for traffic steering purposes.
- When you configure the traffic steering profile, you can specify destinations on the list that you do not want to be handled using Zero Trust Access. For example, if the destination list includes *.example.com, and you want to exclude ExcludedDestination.example.com, add that exclusion to the traffic steering rule.

  Enter destinations to exclude as a comma-separated list.
- Removing a destination list from a Zero Trust Access profile does NOT remove the destination list from Secure Access.
- Future deletions, changes, additions to selected destination lists will affect Zero Trust Access traffic steering to those destinations.

- User authentication interval settings configured on the rule defaults page for access rules do NOT apply to internet traffic.
- An FQDN-based steering rule can be configured to bypass Zero Trust Access proxy to a remote access VPN. CIDR block IPs and NetWitness IP ranges are supported.

Using Wildcards to Configure Traffic Steering for Private Destinations

Describes Using Wildcards to Configure Traffic Steering for Private Destinations in Cisco Secure Access. For more granular control over zero trust access to private resources and to reduce the number of individual private destinations for both ZTA profiles and DNS steering destinations, consider using wildcards to configure these destinations.

For more granular control over zero trust access to private resources and to reduce the number of individual private destinations for both ZTA profiles and DNS steering destinations, consider using wildcards to configure these destinations.

Wildcard matching does not include exact-domain matchinng; it can represent only one token and cannot represent multiple tokens. When you add a domain like google.com to an allow list, it implicitly allows all subdomains like *.google.com, but if you want to block only a specific subdomain such as news.google.com, you must add the entire FQDN.

Important

Important note about editing traffic steering entries:

When you configure a Private Resource, Secure Access automatically adds an entry for each configured resource address for client-based zero-trust access to the Traffic Steering page, in order to direct end-user traffic to the resource.

If you edit entries that were automatically added to the Zero Trust Traffic Steering page when you configured a Private Resource, the traffic steering rules for the resource are NOT updated when you make future edits to the Private Resource configuration page.

Exception

If you have deployed the zero trust client on iOS devices, see unique matching information in the "Guidelines and Limitations" section of the Set up the Zero Trust Access App for iOS Devices.

Procedure for Configuring Traffic Steering for Private Destinations Using Wildcards

Provides instructions for completing the Procedure for Configuring Traffic Steering for Private Destinations Using Wildcards workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To exclude traffic from a configured Private Resource address:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Before using this procedure, see important caveats at Traffic Steering for Zero Trust Client-Based Connections.
- The private resource address to edit must be configured as a wildcard FQDN.

Procedure

1. Navigate to **Connect** > **End User Connectivity** .
2. Click on the **Zero Trust** tab.
3. For the resource to modify, click the ellipsis (**...**) button at the end of the table row and choose **Edit**.

4. Provide subdomains to exclude from traffic steering for Zero Trust connections. For example, if your domain is **.example.com*, and you want to exclude traffic to *hr.example.com* and *boo.finance.example.com*, enter **hr** as an exclusion, then click **Add** and enter **boo.finance**.

   Note

   You can enable access to subdomains when you enter a parent FQDN. For example, you configure ccc.com. You can gain access to subdomains such as aaa.ccc.com and bbb.ccc.com.

5. Click **Save**.

Addresses That Never Use Zero Trust Access

Describes Addresses That Never Use Zero Trust Access in Cisco Secure Access. Traffic to destinations on this page will never be handled using Zero Trust Access.

Traffic to destinations on this page will never be handled using Zero Trust Access. These addresses are in addition to any system-provided exceptions and exclusions that appear in a ZTA Profile, and they cannot be modified or removed.

IPv6

::1/128 Loopback Address [RFC4291]

::/128 Unspecified Address [RFC4291]

64:ff9b::/96 IPv4-IPv6 Translat. [RFC6052]

64:ff9b:1::/48 IPv4-IPv6 Translat. [RFC8215]

100::/64 Discard-Only Address Block [RFC6666]

2001::/23 IETF Protocol Assignments [RFC2928]

2001::/32 TEREDO [RFC4380] [RFC8190]

2001:1::1/128 Port Control Protocol Anycast [RFC7723]

2001:1::2/128 Traversal Using Relays around NAT Anycast [RFC8155]

2001:1::3/128 DNS-SD Service Registration Protocol Anycast [RFC-ietf-dnssd-srp-25]

2001:2::/48 Benchmarking [RFC5180][RFC Errata 1752]

2001:3::/32 AMT [RFC7450]

2001:4:112::/48 AS112-v6 [RFC7535]

2001:10::/28 Deprecated (previously ORCHID) [RFC4843]

2001:20::/28 ORCHIDv2 [RFC7343]

2001:30::/28 Drone Remote ID Protocol Entity Tags (DETs) Prefix [RFC9374]

2001:db8::/32 Documentation [RFC3849]

2002::/16 [3] 6to4 [RFC3056]

2620:4f:8000::/48 Direct Delegation AS112 Service [RFC7534]

3fff::/20 Documentation [RFC9637]

5f00::/16 Segment Routing (SRv6) SIDs [RFC9602]

fc00::/7 Unique-Local [RFC4193] [RFC8190]

fe80::/10 Link-Local Unicast [RFC4291]

ff00::/8 Multicast Address Block

IPv4

127.0.0.0/8 Loopback Address Block

169.254.0.0/16 Link-local Address Block

224.0.0.0/4 Multicast Address Block

255.255.255.255 Broadcast Address

7.128.0.0/9 Synthetic range

Zero Trust Access to Internet Destinations

Describes Zero Trust Access to Internet Destinations in Cisco Secure Access. Some internet destinations outside your organization's network, such as YourCompany.OtherCompany.com, allow access only to traffic that originates from IP addresses that are within your organization's IP address space.

Some internet destinations outside your organization's network, such as *YourCompany.OtherCompany.com*, allow access only to traffic that originates from IP addresses that are within your organization's IP address space. Users who are in the office or using VPN will have the required IP address. Remote users who are not using VPN, including those using mobile devices, would not have access to the internet resource.

To allow these users to access the resource, use the solution described on this page to ensure that the egress IP address associated with their devices is within your organization's IP address space.

This solution also provides the ability to source traffic from local regions that do not currently have a Secure Access data center.

The solution on this page can be used only for individual SaaS applications that match the description above. It cannot be used for zero trust access to internet destinations in general, such as those defined by content category.

> **Note**
>
> Mobile platforms currently **do not** support secure internet access steering that uses "all" as a wildcard for internet destinations.

Zero Trust Access to Internet Destinations Overview

Describes Zero Trust Access to Internet Destinations Overview in Cisco Secure Access. Install the Cisco Secure Client, including the Zero Trust Access module if applicable for the device, on managed devices, including mobile devices.

- Install the Cisco Secure Client, including the Zero Trust Access module if applicable for the device, on managed devices, including mobile devices. Enroll each device in Zero Trust Access.

  For details, see Zero Trust Access links in Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices.

- Configure a resource connector group and connectors in the region near the location from which the internet destination is hosted. For details, see Manage Resource Connectors and Connector Groups.
  - Ensure that you have deployed enough connectors to handle potential capacity.

- Configure a private resource:

> **Tip**
>
> Configure a private resource with the address of an actual private resource, ensure that all other requirements on this page are met, then test. After you verify that your configuration works as expected for the internal resource, change the **Internally reachable address** in the Private Resource configuration to the internet address and test again.

  - The following settings are required:
    - Specify the specific internet destination in the **Internally reachable address** field.
    - Enable client-based zero trust access connections.
    - Do not enable decryption.
    - Associate the resource with a resource connector group.

      Network tunnels will not work for this purpose.
  - For details, see Add a Private Resource.
- Configure client-based endpoint requirements.

  For details, see Add a Client-Based Zero Trust Access Posture Profile on page 1250.
- Ensure that all requirements are met for connecting traffic to a private resource using client-based Zero Trust Access and resource connectors.

  For example, see Requirements for Zero Trust Access.
- Network authentication requirements apply to this traffic. See Network Authentication for Zero Trust Access.
- Create a private access rule (NOT an internet access rule) and choose the private resource, configured above with the internet address, as a destination. For details, see Add a Private Access Rule.

> **Note**
>
> Intrusion prevention (IPS) may not be fully effective because decryption is disabled.

- Ensure that your network (such as routes, ACLs, and NAT requirements) allows this traffic to be routed to the internet. (This step is performed outside of Cisco Secure Access.)
- Ensure that the destination site allows access from the egress IP addresses that your users' connections will use, as discussed in the Web Traffic and NATaaS section of Secure Access NAT as a Service.

Trusted Networks for Zero Trust Access Connections

Describes Trusted Networks for Zero Trust Access Connections in Cisco Secure Access. A trusted network is one that is secure, reliable, and well-protected against unauthorized access, data breaches, and other cyber threats.

A trusted network is one that is secure, reliable, and well-protected against unauthorized access, data breaches, and other cyber threats. Trusted networks are typically present within your larger corporate network, or in a trusted partner's network that has all the necessary security measures in place. Trusted Network Detection (TND) enables the recognition of a predefined trusted network. When connected to a trusted network, Secure Access can bypass ZTA enforcement, and start ZTA enforcement when the user is outside the trusted network (corporate network).

Secure Access allows you to define trusted networks using a set of criteria that Cisco Secure Client uses to detect whether an endpoint device is connected to a defined trusted network and route the user's traffic as intended. For instance, if certain destinations are configured to use Zero Trust Access, you can disable them for in-office users and utilize on-network security mechanisms. Trusted networks are used in universal Zero Trust Network Access configuration where the threat defense devices can enforce rules for the private resources associated with them, based on the assigned trusted network.

Caution: When using Secure Access to define a network as trusted, exercise extreme care in your selection. If you designate a network as trusted without thoroughly verifying that all required security and connectivity mechanisms are in place, you risk leaving user data unprotected and vulnerable to potential threats. Failure to choose a properly secured network can compromise the safety and confidentiality of sensitive information.

Add a Trusted Network

Provides instructions for completing the Add a Trusted Network workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add a trusted network for Zero Trust end-user connectivity.

Before you begin

Zero Trust Access profiles provides distinct access experiences for different users and groups. You can view, edit, and delete the profiles for private and internet access.

Wildcard matching in ZTA profiles does not include exact-domain matchinng; it can represent only one token and cannot represent multiple tokens. When you add a domain like google.com to an allow list, it implicitly allows all subdomains like *.google.com, but if you want to block only a specific subdomain such as news.google.com, you must add the entire FQDN as your DNS steering destination.

For users implementing Kerberos authentication with AD, we recommend reviewing the appropriate Microsoft documentation about configuring the correct ports and private resources to plan for for AD communication. To understand how to optimize the location of a domain controller, see this documentation.

Important

Be aware of the ZTA limitations when creating a profile. See Limitations and Range Limits for more information. You **must** be a **Full Admin** to proceed with this procedure. See Manage Accounts for more information.

Zero Trust Access profiles are an ordered list where the order of profiles determines their priority. The last profile in the list is always the Default ZTA Profile. A user's Zero Trust Access client receives settings from the first matching Zero Trust Access profile in profile order. The profile must match both the user's membership and the endpoint operating system. Default profile includes all users in the org and all client Zero Trust Access enabled private and internet resources . Use the following procedure to modify the user's access:

Procedure

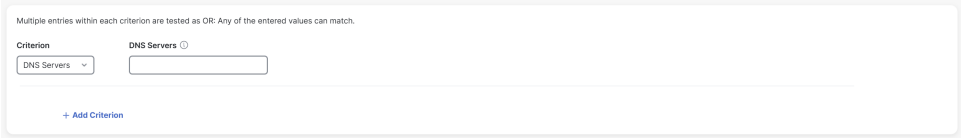
1. Navigate to **Connect** > **End User Connectivity** > **Zero Trust Access**.
2. Click **Manage Trusted Networks** and then click **+Trusted Network**.
3. For **Trusted Network Name**, enter a name for the trusted network.
4. For **Inspect**, choose **Physical adapters** or **Physical and virtual adapters**.
   - **Physical adapters**–The Trusted Network Domain (TND) inspects only physical network interfaces in an endpoint.
   - **Physical and virtual adapters**–The Trusted Network Domain (TND) inspects both physical and virtual network interfaces in an endpoint.

> **Note**
>
> The Physical and virtual adapters option is a beta feature intended for limited testing and not for production environments.

5. Navigate to **Criterion** and then choose your criterion.
   a) Choose **DNS Servers**.

      If you choose this option, enter all the DNS server addresses (comma separated) for the trusted network in the adjacent **DNS Servers** field. Cisco Secure Client detects a trusted network only if it matches any of the specified DNS servers.

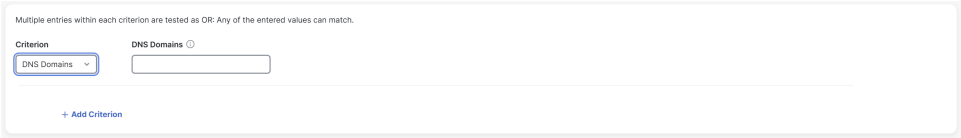
      Add up to a maximum of **100** DNS servers.



   b) Choose **DNS Domains** and then enter the list of comma-separated DNS domain suffixes for the trusted network.

      Cisco Secure Client detects a trusted network only if it matches any of the specified DNS domain suffixes.

      You can add up to **100** DNS domains.

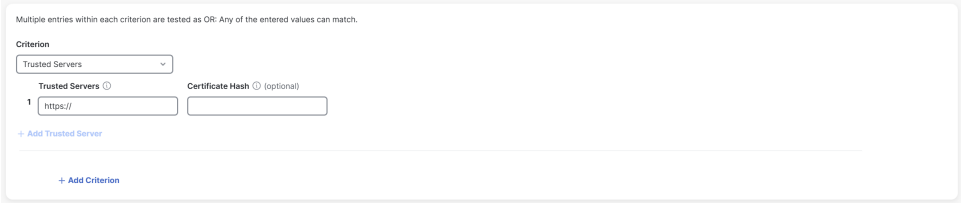


   c) Choose **Trusted Servers** and then for **Trusted Servers** enter a trusted server address. (Optional) For **Certificate Hash** field, enter the hash of the public key of this certificate.

      A DNS server specified must translate the domain name of this server to its corresponding IP address and provide a TLS certificate.

      You can add up to **10** Trusted Servers. Only one of the trusted servers is required to pass validation.

> **Note**
>
> The Certificate Hash option is not applicable for iOS devices.



6. (Optional) Click **+Add Criterion** to add more criteria.

> **Note**
>
> You can add a criteria only once.

7. Click **Save**.

Manage Threat Defense Devices for Universal Zero Trust Network Access

Describes Manage Threat Defense Devices for Universal Zero Trust Network Access in Cisco Secure Access. A Cisco Secure Firewall Threat Defense device can act as an on-premises proxy to Secure Access cloud for private resource access traffic.

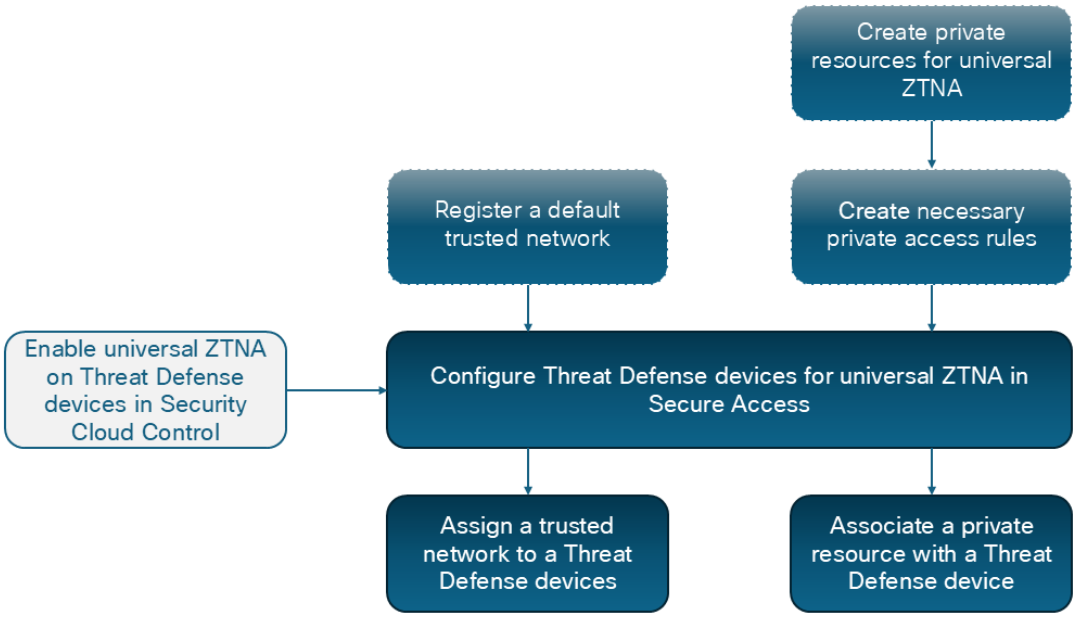
A Cisco Secure Firewall Threat Defense device can act as an on-premises proxy to Secure Access cloud for private resource access traffic. To utilize universal Zero Trust Network Access (ZTNA), Threat Defense devices are configured in Secure Access as on-premises proxies. This enables you to manage the connections that allow user traffic to reach private resources in your network efficiently without compromising on security. This improves end-user experience and ensures consistent security controls for users, independent of where they are connected from.

Threat Defense devices that are enabled for universal ZTNA in Security Cloud Control, become available in Secure Access for further configuration. To know more about the configuration of Threat Defense devices for universal ZTNA, refer to Universal Zero Trust Network Access Configuration Guide.

Once the Threat Defense devices are available in Secure Access, you can perform the following tasks:

- View Threat Defense devices configured for Universal Zero Trust Network Access
- Associate Private Resources with Threat Defense devices
- Assign a Trusted Network to Threat Defense devices

The following workflow displays the tasks to be performed in Secure Access to configure universal ZTNA.



View Threat Defense devices configured for Universal Zero Trust Network Access

Describes View Threat Defense devices configured for Universal Zero Trust Network Access in Cisco Secure Access. Once the Threat Defense devices are available in Secure Access, you can view the configuration attributes of these devices.

Once the Threat Defense devices are available in Secure Access, you can view the configuration attributes of these devices. You can also edit the attributes of a Threat Defense device and view information about the private resources, trusted network, and policies associated with each Threat Defense device.

Secure Access lists all the available Threat Defense devices along with their details and displays the status of synchronization for universal ZTNA configuration, associated resources, and enforced rules in **Connect > Network Connections > FTDs**.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. To view the Threat Defense devices configured for universal ZTNA, you must have at least read-only access in Secure Access.

To view the details of a Threat Defense device (configured for universal ZTNA) in Secure Access, perform the following steps:

Before you begin

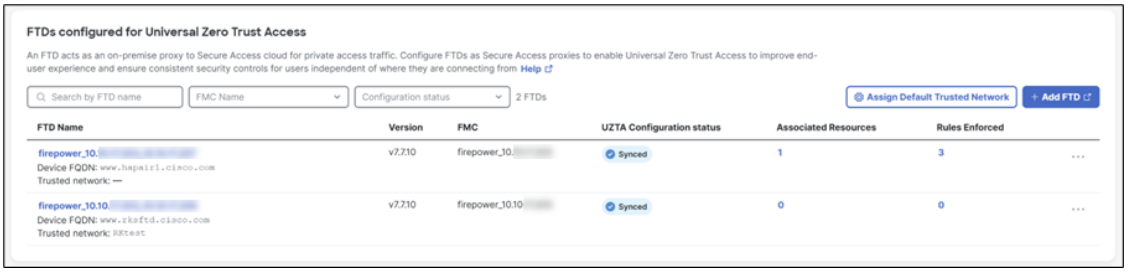
To view the Threat Defense devices configured for universal ZTNA, you must have at least read-only access in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect > Network Connections > FTDs**.

   The list displays the following details:

   - **FTD Name** – Displays the Threat Defense device name along with the device FQDN and the associated trusted network.
   - **Version** – Displays the Firewall Management Center version.
   - **FMC** – Displays the Firewall Management Center name.
   - **UTNA Configuration status** – Displays the status of the universal ZTNA configuration synchronization with the Firewall Management Center. The possible statuses are:
     - **Synced** – The configuration is synchronized with the Firewall Management Center.
     - **Syncing** – The configuration is synchronizing with the Firewall Management Center.
     - **Out of sync** – The configuration synchronization is not initiated with the Firewall Management Center. This can happen when auto deployment is not enabled.
     - **Failed to sync** – The configuration synchronization with the Firewall Management Center has failed. For more information, see Troubleshooting Universal ZTNA guide.
   - **Associated Resources** – Displays the number of resources associated with the Threat Defense device.
   - **Rules Enforced** – Displays the number of rules enforced by the Threat Defense device.

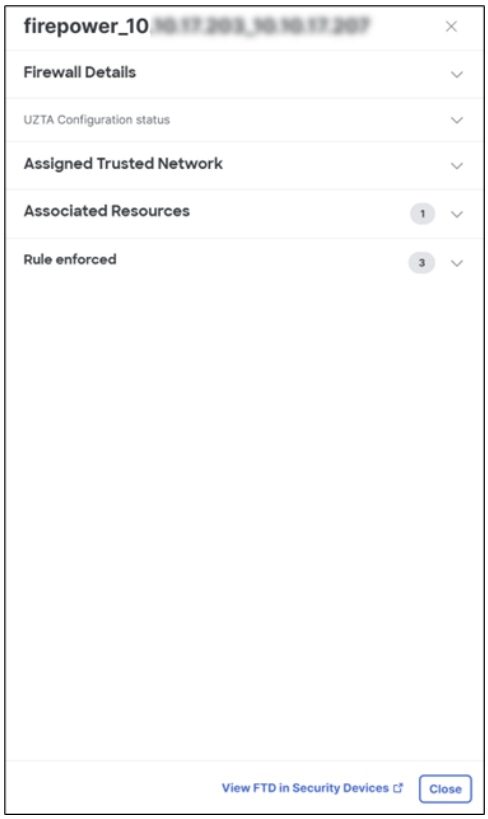


2. Click the corresponding **FTD Name.** .

   Alternatively, click the ellipsis (...) adjacent to the corresponding **FTD Name**, and choose **View FTD Details**.

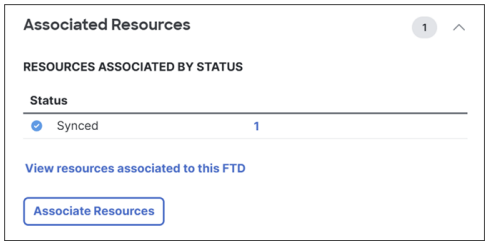
3. Review the Firewall Details, UZTNA Configuration Status, Assigned Trusted Network, Associated Resources, and Rule Enforced sections for the selected Threat Defense device.

> **Note**
>
> - The **Firewall Details** section displays the auto deployment state.
> - The **UZTA configuration status** section displays the reason if the status is **Failed to sync** or **Out of sync**.



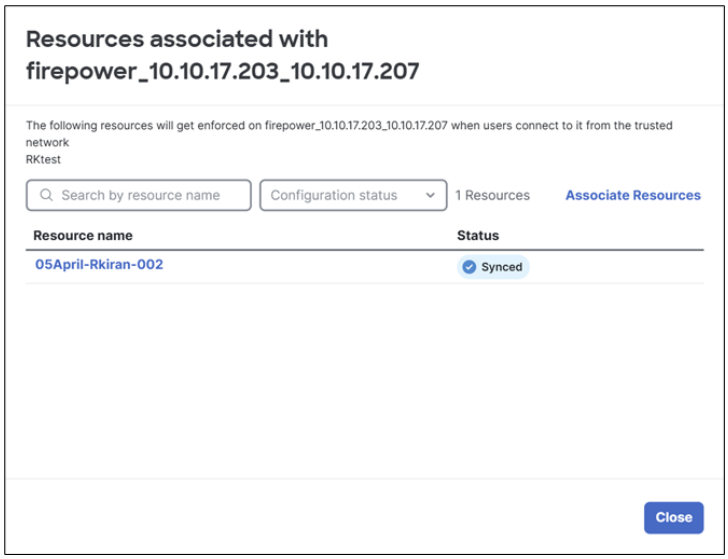
4. In the **Associated Resources** section, click **View resources associated to this FTD** to view the list of associated private resources.

   Alternatively, click the associated resource count.



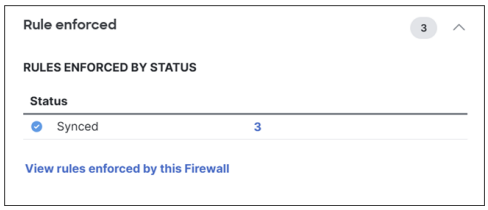
5. Review the associated resources.

   (Optional) Click **Associate Resources** to associate additional private resources with the Threat Defense device. For more information, see Associate Private Resources with Threat Defense devices.

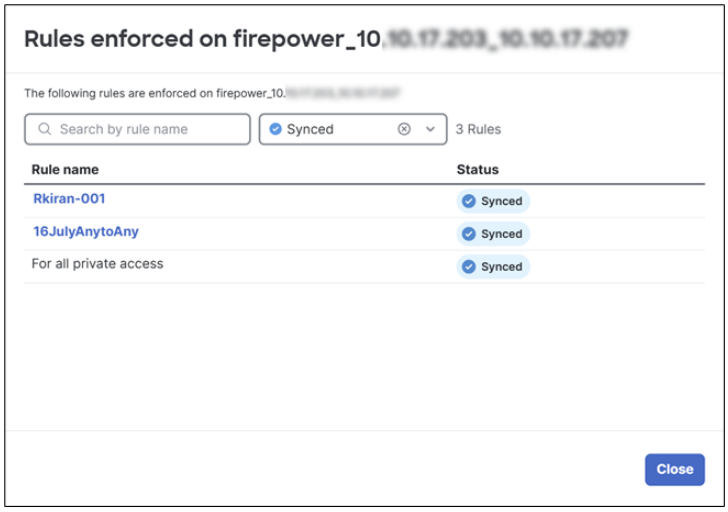


6. In the **Rule enforced** section, click **View rules enforced by this Firewall** to view the list of enforced rules.

   Alternatively, click the enforced rule count.



7. Review the enforced rules.



Associate Private Resources with Threat Defense Devices

Describes Associate Private Resources with Threat Defense Devices in Cisco Secure Access. To enforce the rules for a private resource using a firewall, you must associate private resources with a Threat Defense device.

To enforce the rules for a private resource using a firewall, you must associate private resources with a Threat Defense device. This ensures that the user traffic to the private resource is routed through the firewall instead of the Secure Access cloud when the user is connected to a trusted network.

Associate Private Resources with Firewall Threat Defense

The final step in configuring universal ZTNA is to associate the private resources with the Firewall Threat Defense devices.

Before you begin

You must have created the private resources on Secure Access.

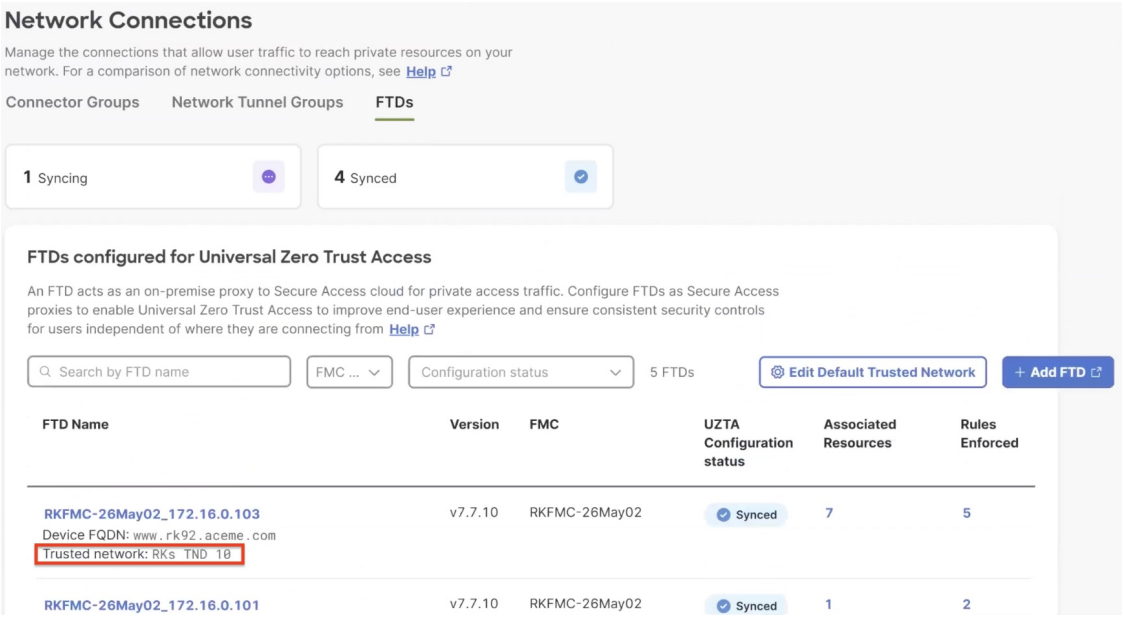
Procedure

1. In Security Cloud Control, click **Products** > **Secure Access**.

   Secure Access product menu displays in the left navigation bar.

2. Click **Connect** > **Network Connections**.
3. Click the **FTDs** tab.

   The available Secure Firewall Threat Defense devices that are configured for universal zero trust network access are displayed.



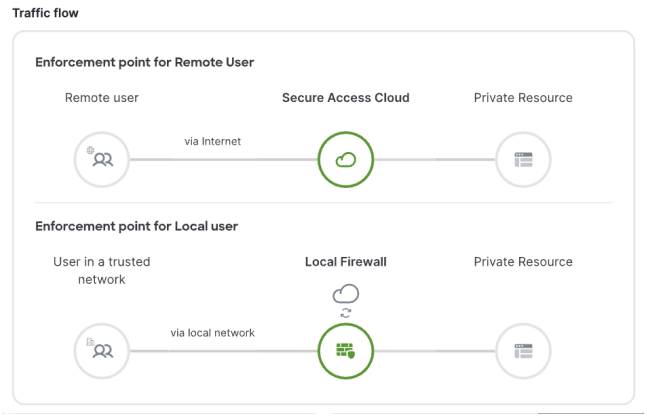
Ensure that the device is associated with a trusted network to enforce policies on traffic originating from the trusted network before proceeding to the next step.

After a Threat Defense device is onboarded, it is automatically associated with a default trusted network if one exists. Otherwise, you must create a trusted network and associate it with the Threat Defense device.

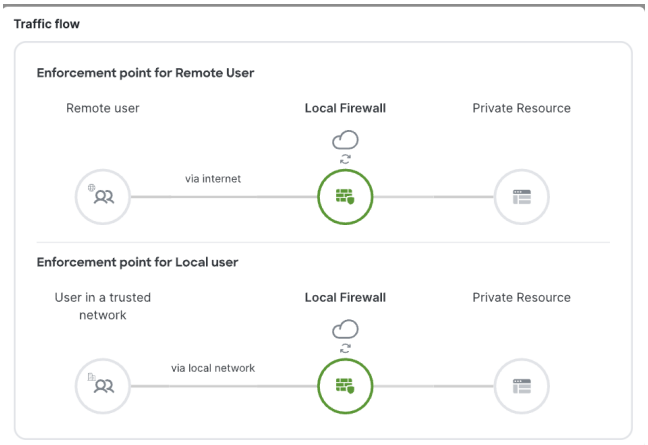
4. Click the name of a Threat Defense device to configure.
5. In the right pane, click **Associate Resources**.

> **Note**
>
> - Only those resources that are enabled for zero trust access may associate with a Threat Defense device.
> - A Threat Defense device must reach the associated private resources.
> - Resources associated with a Threat Defense device are shared with other devices with the same FQDN.

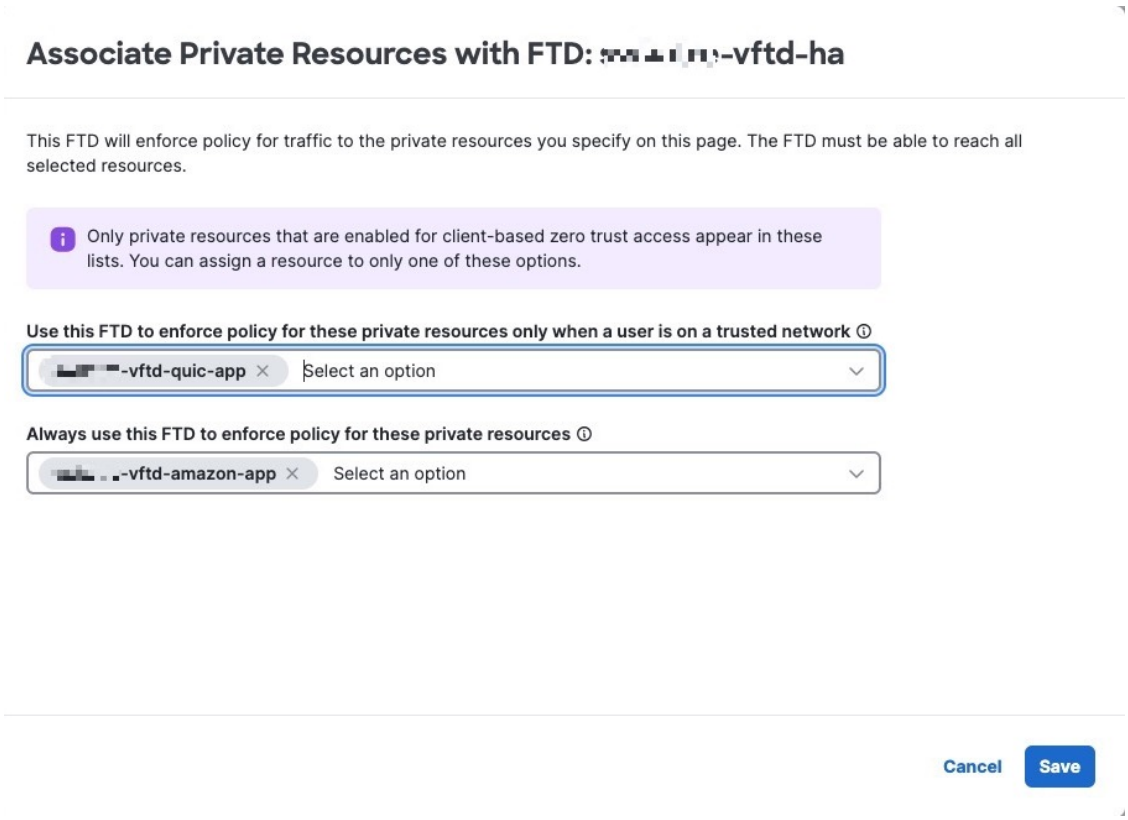
6. In the **Associate Private Resources** dialog box, make the following selections to specify the access policy enforcement and traffic flow for a user:
   - **Use Threat Defense device to enforce policy only for on-premises users**: From the **Use this FTD to enforce policy** drop-down list, select the private resources, which a user should be able to access only from an on-premises location.



- **Use Threat Defense device to enforce policy for both on-premises and remote users**: From the **Always use this FTD to enforce policy** drop-down list, select the private resources for which the selected Threat Defense device always enforces policy, regardless of whether the user is located on-premises or is remote.



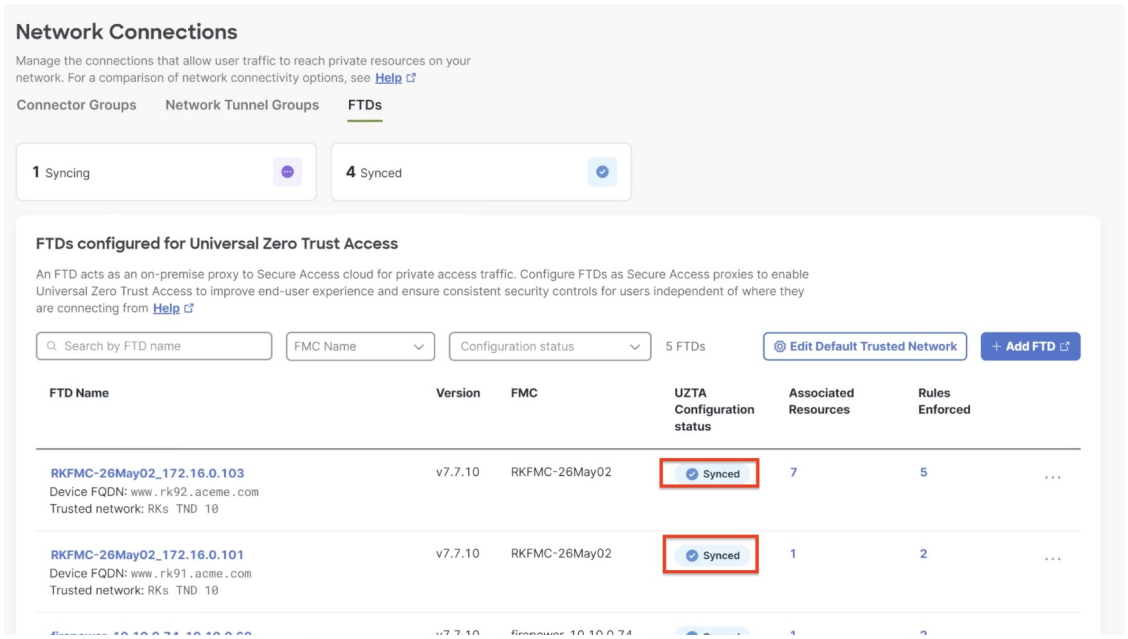
The following figure shows an example of using a Threat Defense device to enforce access rules for the **vftd-quic-app** for on-premises users and **vftd-amazon-app** for all users, whether on-premises or remote.



7. Click **Save**.

   The configurations are applied to the device, and the **UZTA Configuration status** column for the device displays **Synced**.

   The following figure shows an example.



   Configuration status can also be:

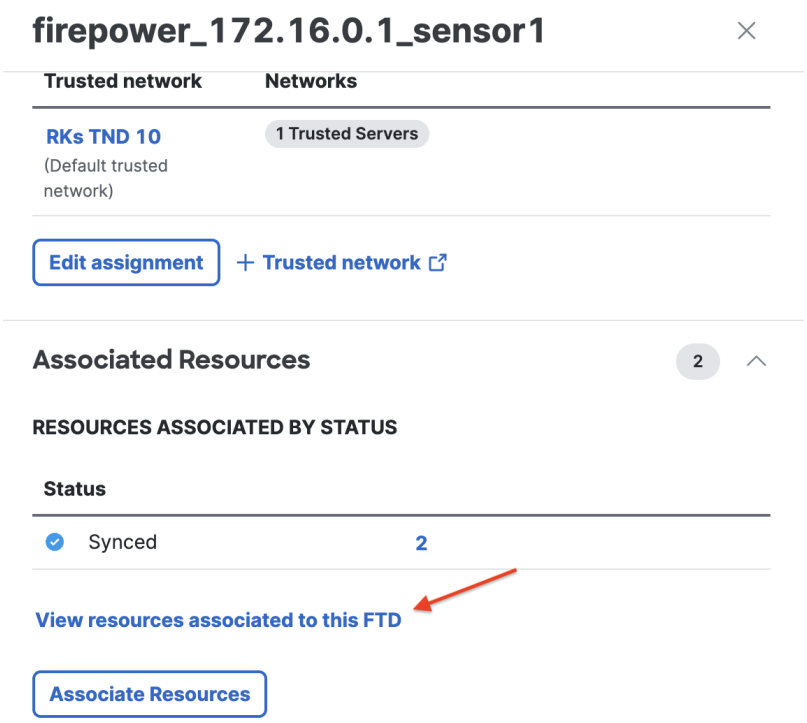
   - Syncing–updates to the Threat Defense device are ongoing.
   - Out of sync–modifications to Secure Access configurations are pending update to the Threat Defense device.

- Failed to sync–configurations were not updated on the Threat Defense device.

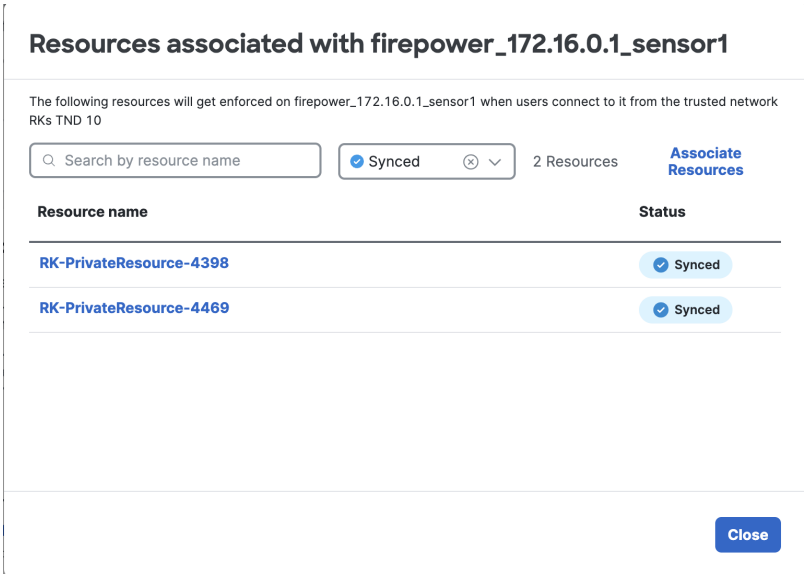
To view a detailed and granular status for each resource and rule associated with a Threat Defense device, perform the actions outlined:

a) Click the numeral in the **Associated Resources** column.

In the slide-in pane, under the **Associated Resources** section, click **View resources associated with this FTD**.

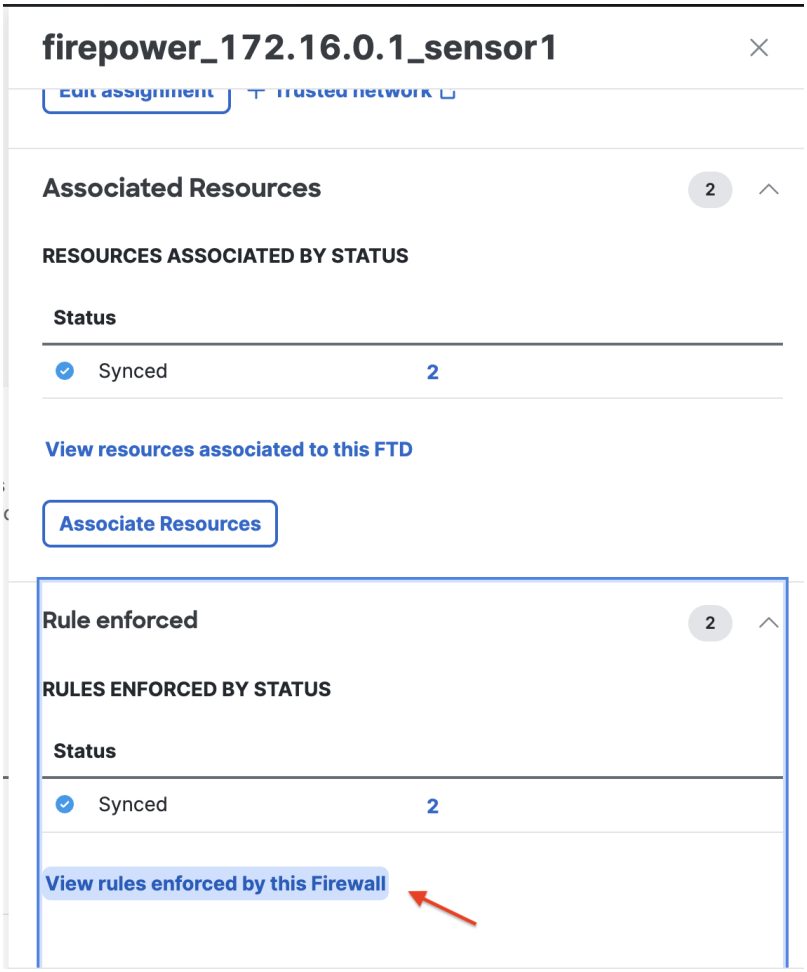


The configuration status of each resource is displayed.

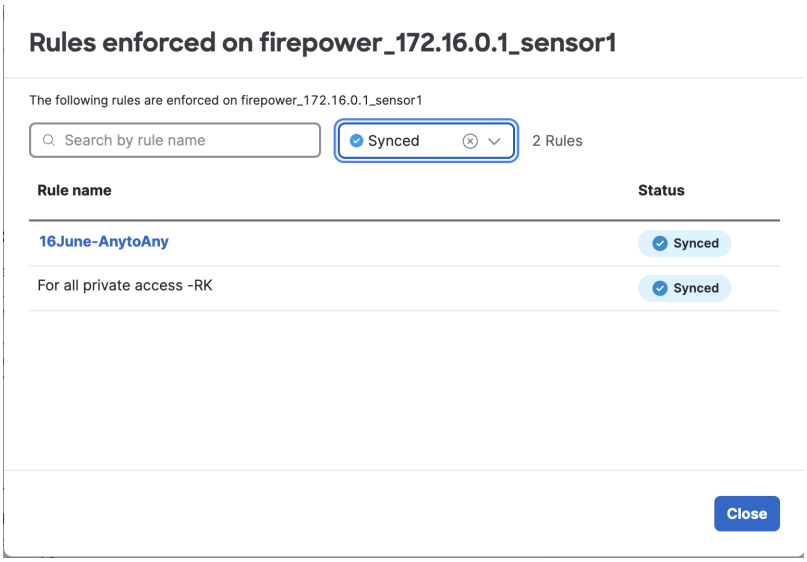


b) Similarly, to check the configuration status of each rule that is enforced by the Threat Defense device, click the numeral in the **Rules Enforced** column.

In the slide-in pane, under the **Rules Enforced** section, click **View rules enforced by this Firewall**.



The configuration status of each rule that is enforced is displayed.



Universal ZTNA is now set up for your clients to securely access the private resources in your network.

Assign a Trusted Network to Threat Defense devices

Describes Assign a Trusted Network to Threat Defense devices in Cisco Secure Access. Universal ZTNA allows Threat Defense devices to enforce rules for private resources when the user is connected to a trusted network.

Universal ZTNA allows Threat Defense devices to enforce rules for private resources when the user is connected to a trusted network. In Secure Access, you can define trusted networks to use for universal ZTNA. You can also define a network as a default trusted network. When Threat Defense devices are onboarded, Secure Access assigns the default trusted network to the Threat Defense devices automatically. You can modify this and assign a different trusted network to a Threat Defense device.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. You must have a full admin role in Secure Access.

To assign a trusted network to a Threat Defense device, perform the following steps:

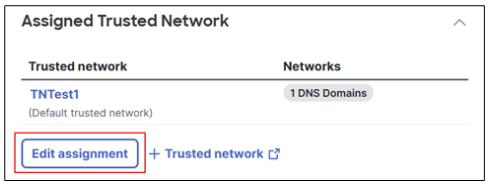
Before you begin

- You must have a full admin role in Secure Access. For more information, see Manage Accounts.
- Trusted networks must be defined for universal ZTNA. For more information, see Trusted Networks for Zero Trust Access Connections.

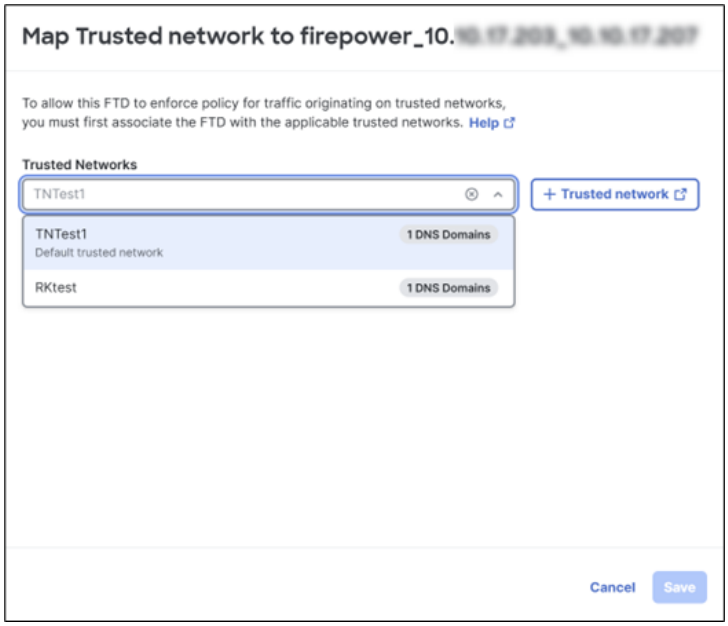
Procedure

1. Navigate to **Connect > Network Connections > FTDs**.
2. Click the corresponding **FTD Name**.

   Alternatively, click the ellipsis (...) adjacent to the corresponding **FTD Name**, and choose **View FTD Details**, or click the associated resources count.
3. In the **Assigned Trusted Network** section, click **Edit assignment**.

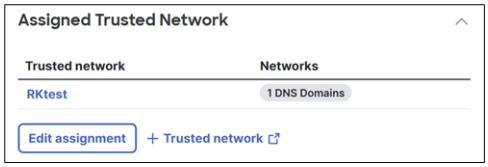


4. From the **Trusted Networks** drop-down list, select the corresponding trusted network.



5. Click **Save**.

   The trusted network is displayed in the Assigned Trusted Network section.



Manage User Trust Profile Zero Trust Access

This topic describes how to configure and manage User Trust Profiles in Cisco Secure Access to control user access and security conditions for Zero Trust Access (ZTA) to private resources.

This section explains how to configure and manage user access profiles in Cisco Secure Access to control end-user device and behavioral requirements when connecting to private resources using Client-Based Zero Trust Access (ZTA).

- **User Trust Profile**–Set this as the default profile to apply access controls based on the trust level assigned to users, according to their authentication and security conditions. These profiles can be linked to resources to automatically apply appropriate access rules. For detailed configuration steps, see Enable User Trust Profile on page 1243.
- **Bypass Untrusted User**–Temporarily bypass the Untrusted trust level for a user in Cisco Secure Access. For more information, see Bypass Untrusted User.

Enable User Trust Profile

This topic describes how to enable User Trust Profiles in Cisco Secure Access, select a default profile to control access based on trust levels, and use the Bypass Trust Level option to unblock users if necessary.

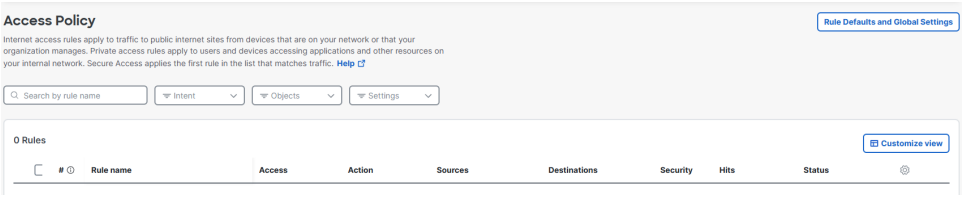
User trust profiles determine the ability to control access based on the trust levels specified on the User, Group, and Endpoint Devices page. It verifies trust levels before granting access, as users marked as Untrusted are blocked. Use the Bypass Trust Level option in User details to unblock.

Before you begin

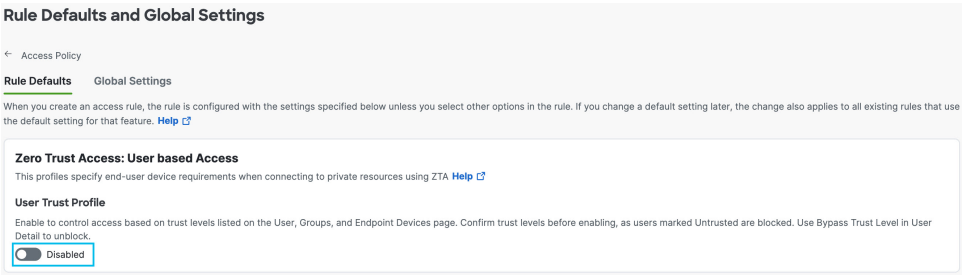
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policy** > **Rule Default and Global Settings**.

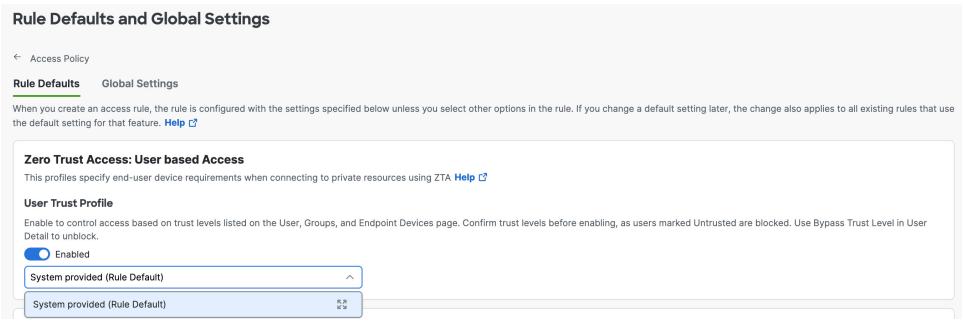


2. To enable the **User Trust Profile**, click the **Disabled** toggle button. This will enable you to control access based on trust levels defined on the User, Groups, and Endpoint Devices page.

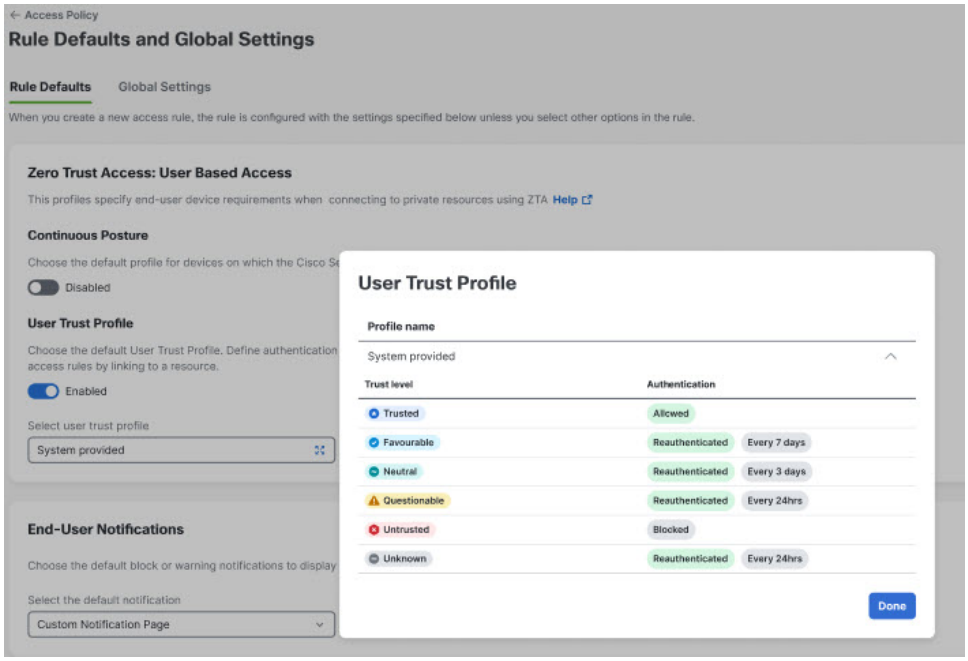


3. From the drop-down list, choose the default user trust profile.
4. Click the  icon next to the **System provided (Rule Default)** in the drop-down list.

> **Note**
>
> Admins must be careful when enabling the **User Trust Profile** feature, as users marked as Untrusted will be blocked. Use the **Bypass Trust Level** in User Detail to unblock them. For more information, see Bypass Untrusted User on page 1245.



The **User Trust Profiles** window displays, the available trust levels and their corresponding authentication settings–**Allowed, Reauthentication** (for example, every 7 days or 24 hours), or **Blocked**–for each trust level.



5. Click **Done** to save your changes.

Bypass Untrusted User

This topic describes how to temporarily bypass the Untrusted trust level for a user in Cisco Secure Access, including the steps to grant access, set the bypass duration, and ensure proper investigation before proceeding.

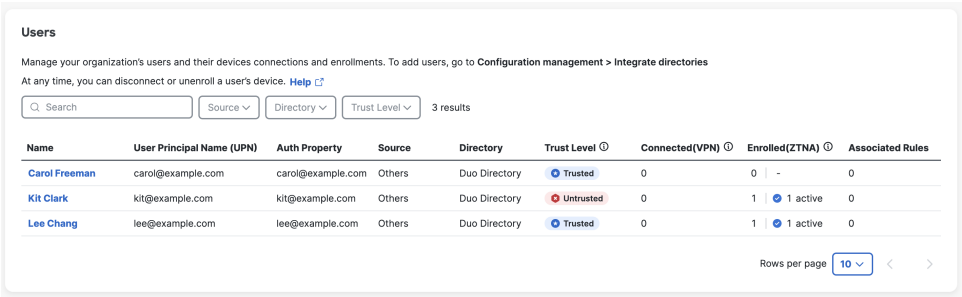
This topic describes how to temporarily bypass the **Untrusted** trust level for a user in Secure Access. It outlines the steps required to grant access to users who have been flagged as **Untrusted** which includes setting the bypass duration.

Before you begin

- Access to an account with the Full Admin role in Secure Access is required. For more information, see Manage Accounts.
- The user must thoroughly investigate the untrusted user's activity and confirm that there is no associated risk before proceeding with a bypass.

Procedure

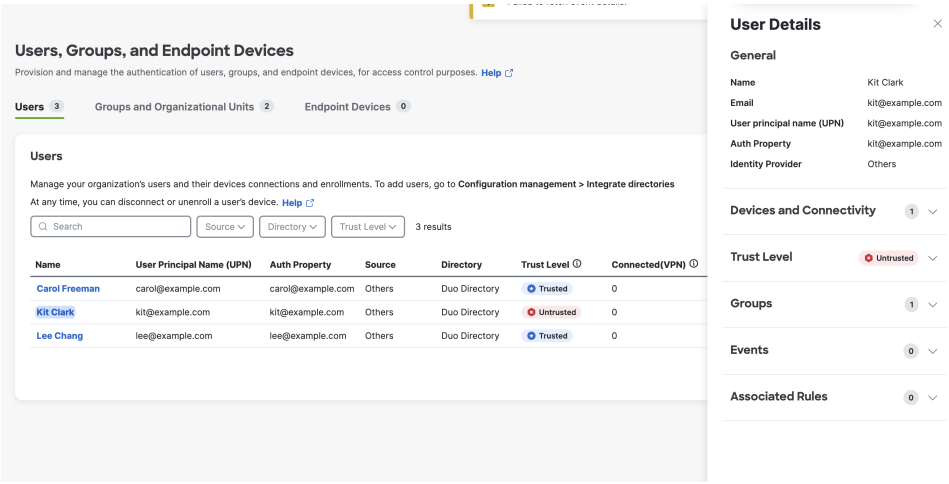
1. From Secure Access, navigate to **Connect > Users, Groups, and Endpoint Devices**, and click **Users**.



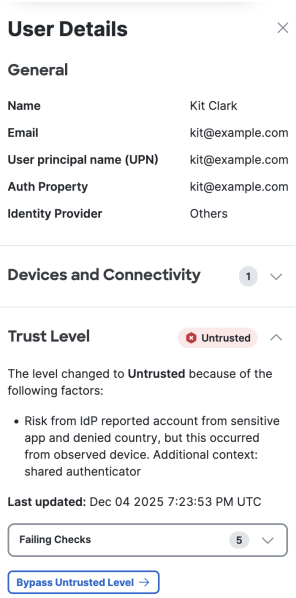
2. Click a user's name to view the corresponding details.

The following attributes are displayed:

- **Name**–The name of the user.
- **Email**–The email address of the user.
- **User Principal Name**–The Unique Principal Name of the user.
- **Auth Property**–The authentication property used by Secure Access for this user.
- **Identity Provider**–The identity provider (IdP) that manages the user account.
- **Trust Level** – Indicates if the user is exhibiting behavior that is high risk, malicious, or undesirable.



This section shows the user's current trust level, a description of that trust level, and failed checks, if any.

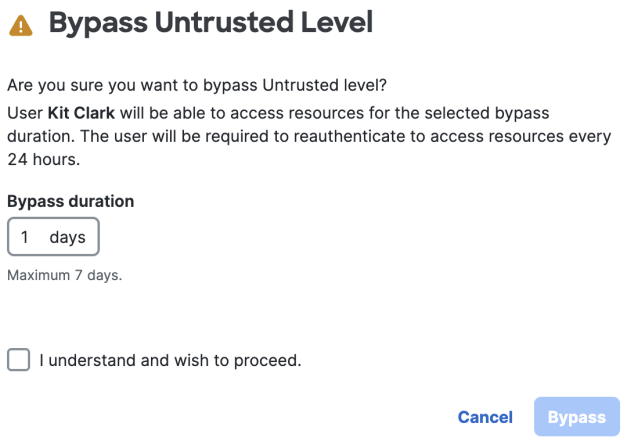


For details on each trust level value (**Trusted**, **Favorable**, **Neutral**, **Questionable**, **Untrusted**, **Unknown**), refer to View Users Provisioned in Secure Access. For more information, see Integrate Cisco Identity Intelligence with Secure Access.

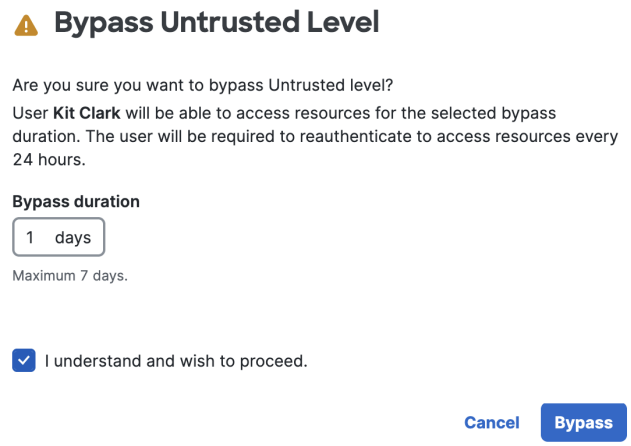
3. To bypass the Untrusted level, click **Bypass Untrusted Level**.

   A **Bypass Untrusted Level** dialog box is displayed with the message, "`Are you sure you want to bypass the untrusted level?`"

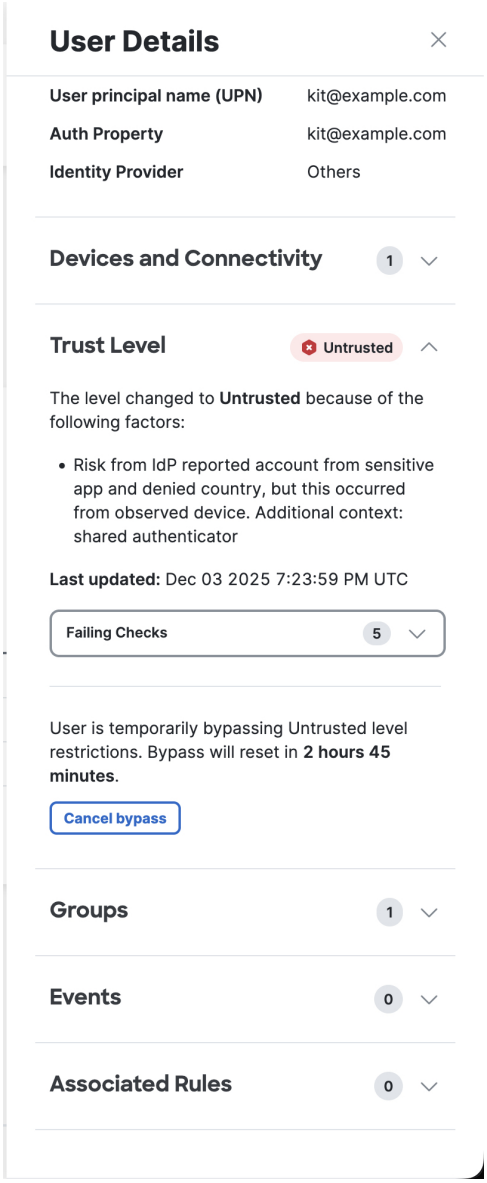
> **Note**
>
> You must ensure that you have thoroughly investigated the user's activity and confirmed that there is no associated risk before proceeding with a bypass.



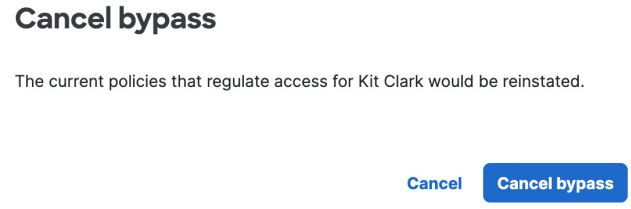
4. Enter the **Bypass duration**–from 1 day to a maximum of 7 days.
5. Check the **I understand and wish to proceed** checkbox and click **Bypass.**



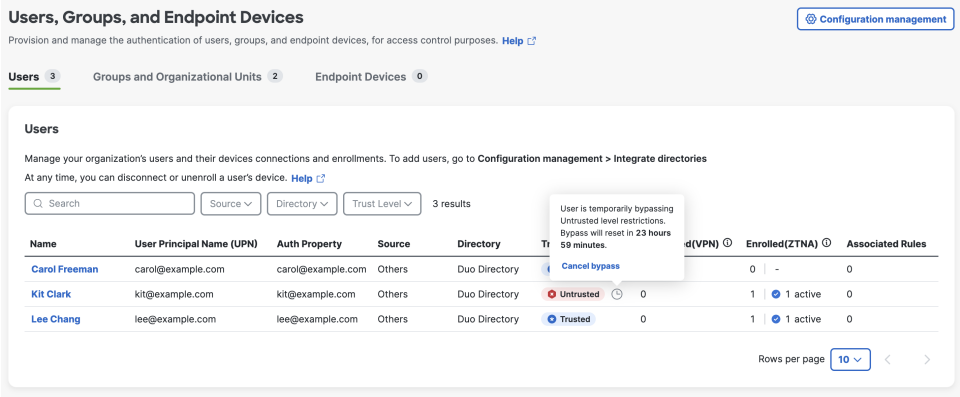
6. On the **User Details** page, in the untrusted level section, a message is displayed, `"User is temporarily bypassing Untrusted level restrictions. The bypass will reset based on the duration you choose."`To cancel the bypass, click **Cancel bypass**.



If you click the **Cancel bypass** button, a dialog box seeking your confirmation for canceling the bypass appears.



Alternatively, on the **Users, Groups, and Endpoint Devices** page, under **Users**, hover over the icon to view the message: `"User is temporarily bypassing Untrusted level restrictions. The bypass will reset based on the 1 to 7 days chosen by the admin and the amount of time that has passed since the bypass was selected."` To cancel the bypass, click **Cancel bypass**.



Manage Zero Trust Access Posture Profiles

Describes Manage Zero Trust Access Posture Profiles in Cisco Secure Access. These profiles specify end-user device requirements when connecting to private and internet resources using Zero Trust Access.

These profiles specify end-user device requirements when connecting to private and internet resources using Zero Trust Access.

There are two types of profiles to choose from:

- **Client-based** - Choose this as the default profile for devices on which the Cisco Secure Client is installed. Client-based profiles can also be used for internet access. See Add a Client-Based Zero Trust Access Posture Profile
- **Browser-based** - Choose this as the default profile for devices on which the Cisco Secure Client **is not** installed. See Add a Browser-Based Zero Trust Access Posture Profile

> **Note**
>
> Enterprise browsers do not currently support proactive analysis functionality.

Client-based access permits more posture requirements than clientless access, so you should tailor profiles to the type of access.

ZTA Posture Timeouts

Timeouts are built into ZTA posture profiles and are expected in a healthy environment. Note that these are *not* applicable for mobile ZTA

Posture Refresh rate - 5 minutes.

A posture refresh rate is the status of the posture fetched by the client-based access policy. It is cached in a cookie and the cookie itself is what expires at five minutes.

Stale Posture Status - 15 minutes.

This is max amount of time before a posture is considered stale and outdated. The posture status is fetched from Duo cloud is timestamped from the end device. If that timestamp is 15 minutes or greater when it is fetched, then the posture is considered stale and is rejected.

Zero Trust Access Posture Attributes

The following

- Supported operating systems
- Firewall
- Endpoint security agents
- System password
- Disk encryption
- Browser

Add a Client-Based Zero Trust Access Posture Profile

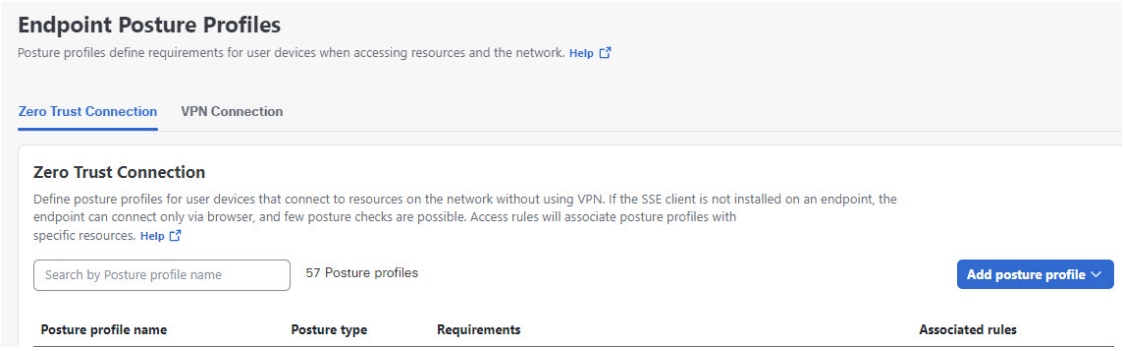
Provides instructions for completing the Add a Client-Based Zero Trust Access Posture Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure a client-based Zero Trust Access posture profile to define posture requirements for endpoint devices that connect to private resources. Cisco Secure Client must be installed on the endpoint device, and Secure Access checks the requirements when the device connects to the network.

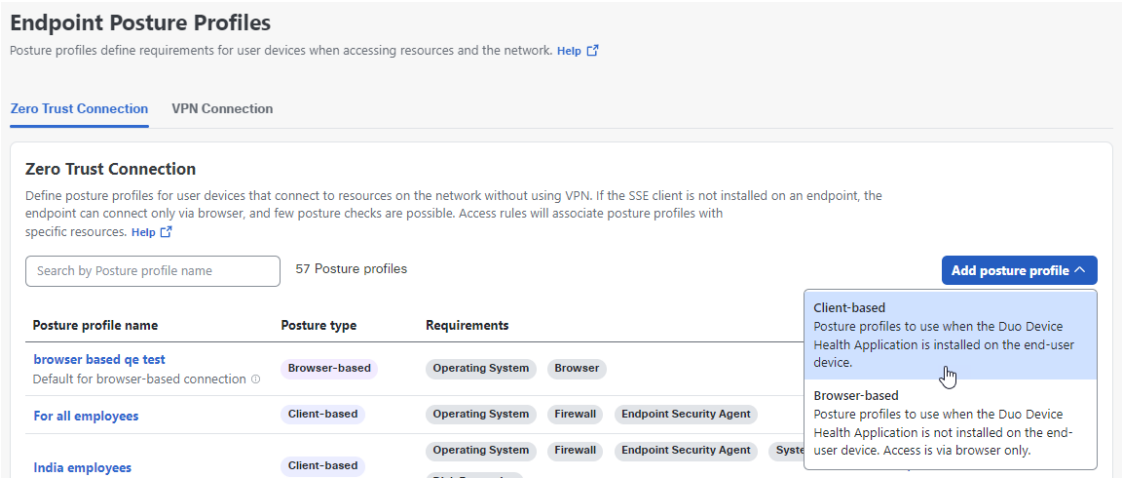
> **Note**
>
> Each requirement is optional, and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

Procedure

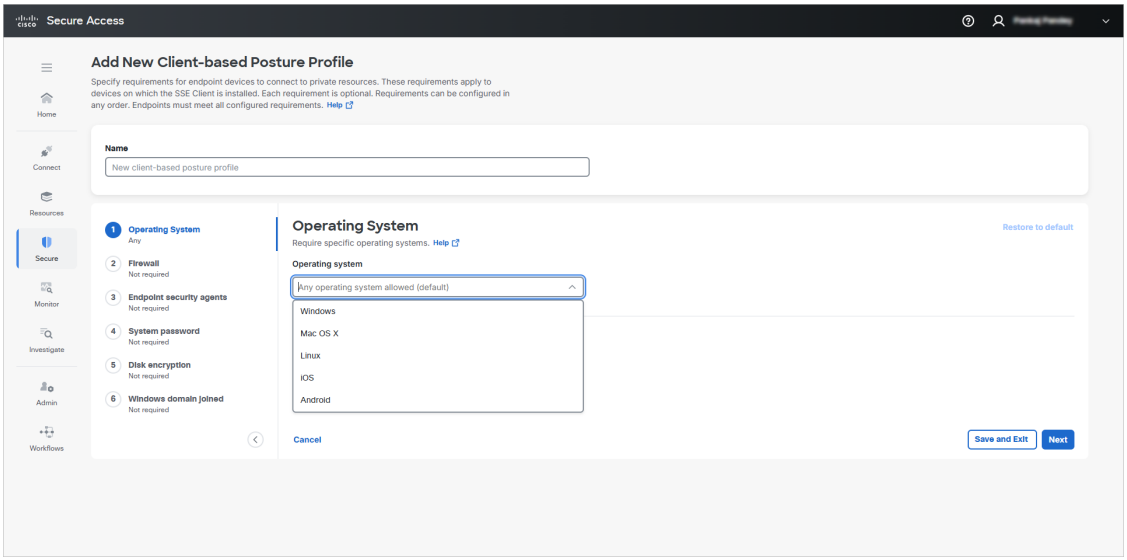
1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



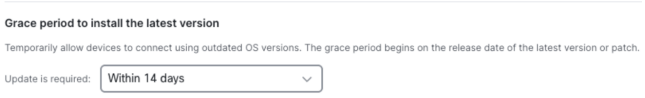
2. For **Zero Trust Connection**, click **Add Posture Profile** and choose **Client-based**.



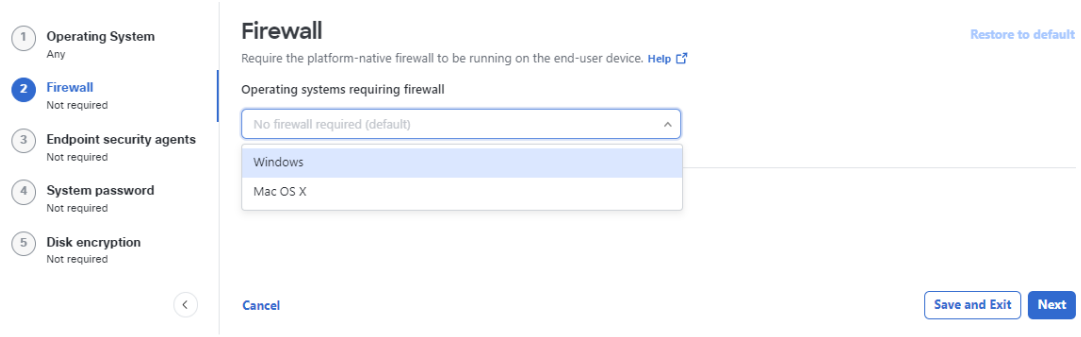
3. Give your posture profile a unique **Name**.
4. In the **Operating System** window, choose the operating systems for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Supported Operating Systems for more information.



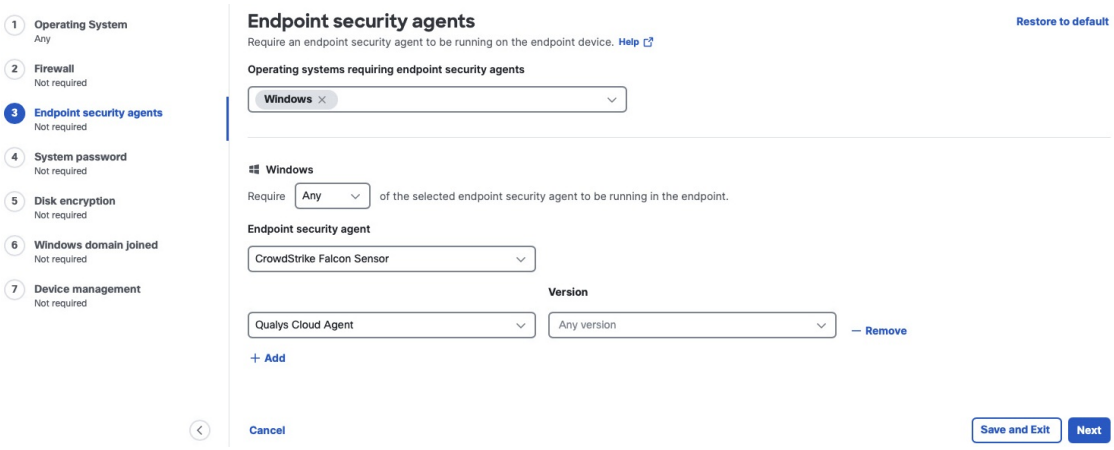
5. In the **Operating System** window, select the **Grace Period** for your device OS version. This value determines how long the operating system version is allowed to be out of date before the device itself is no longer supported. As an admin you can specify grace periods to provide users time to update their devices' OS to comply with latest updates and OS expiry. These grace periods indicate how long after expiry the OS may still be accepted as meeting posture requirements.



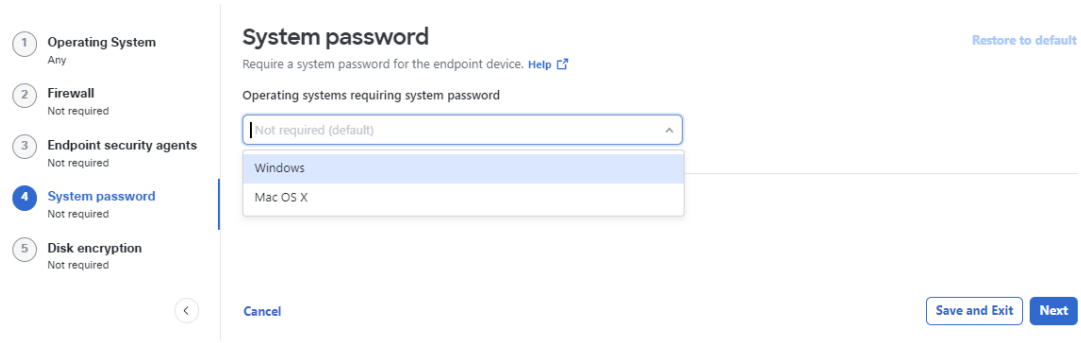
6. For the **Firewall** option, choose the firewall for your profile. Click **Save and Exit** or **Next** to select endpoint security agents. See Firewall Requirements.



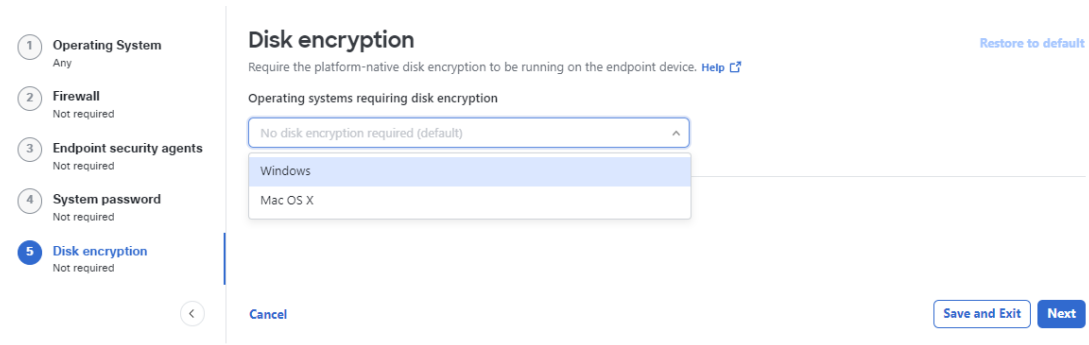
7. For the **Endpoint security agents** option, choose an endpoint security agent from the drop-down menu for your preferred profile. Configure what the endpoint agent action requires for action with either **Any** or **All**; when applicable, use the additional drop-down menus to select the type and version of the agent. Click **Save and Exit** or **Next** to continue. See Endpoint Security Agents.



8. For the **System password** option, choose whether to enforce a system password for the endpoint. Click **Save and Exit** or **Next** to select disk encryption. See Endpoint Security Agents.

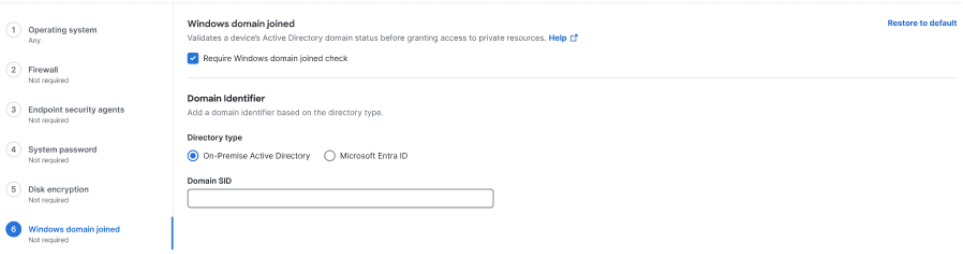


9. For the **Disk encryption** option, choose the disk encryption package(s) for your profile. Click **Save and Exit** or **Next** to enforce whether the device should join a Windows domain. See Disk Encryption.



10. For the **Windows domain joined** option, check the box to enforce verification that the device has joined a domain. Click **Save and Exit** or **Next** to return to the OS requirements. See Windows Domain Join for more information. Ensure you select the device type you have, either an on-premises Active Directory or Microsoft Entra domain and enter the appropriate information for Domain Security Identifiers (SID) or Tenant IDs respectively.

> **Note**
>
> To locate the SID value, we recommend opening Powershell and executing the following command:
>
> ```
> get-ad-domain | select name, domainsid
> (Get-ADDomain).DomainSID.Value
> ```
>
> Note that the last six digits of this return is the **relative identifier** and is not supported as part of the SID value. SID values should be in this format: `S-1-5-21-1292428093-839522115-1801674531`.



11. Click **Next**. Alternatively, click **Save and Exit** to leave the profile temporarily incomplete.

What to do next

We strongly recommend assigning this posture profile to the Access policy. You can either create a new Internet Access rule or Private Access rule, or edit an existing rule.

Add a Browser-based Zero Trust Access Posture Profile

Use this procedure to configure a browser-based Zero Trust Access posture profile for endpoint devices that is not configured with Cisco Secure Client, define posture requirements, and integrate Microsoft Entra ID to control secure access to private resources.

Configure a browser-based Zero Trust Access posture profile to define posture requirements for endpoint devices that connect to private resources. The Cisco Secure Client is not installed on these endpoint devices. Secure Access checks the requirements when a device connects to the network.

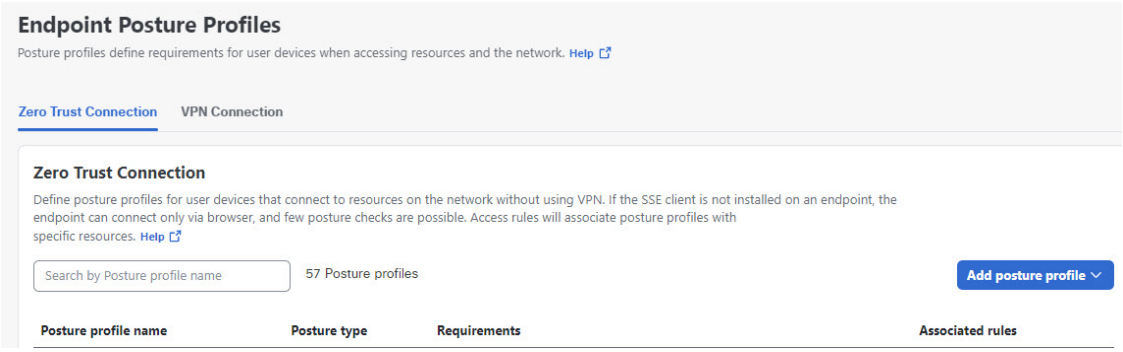
> **Note**
>
> Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all conditions of any requirement that is configured.

Before you begin

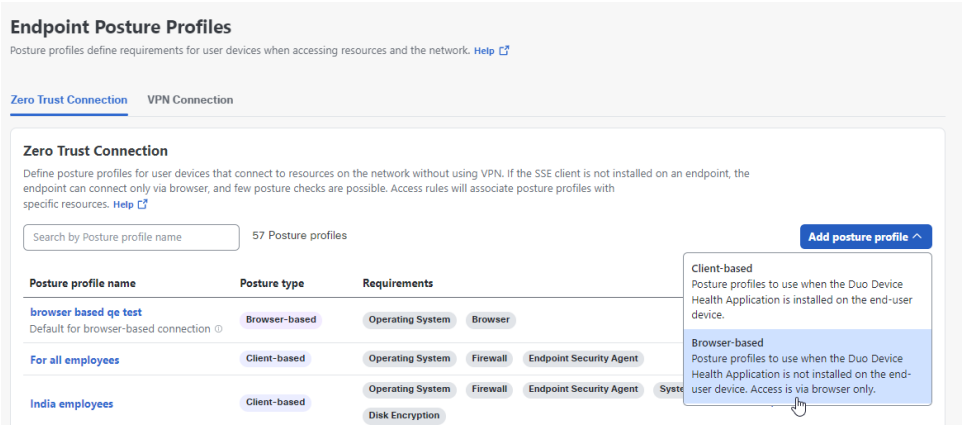
- You must have the full Admin user role. For more information, see Manage Accounts.

Procedure

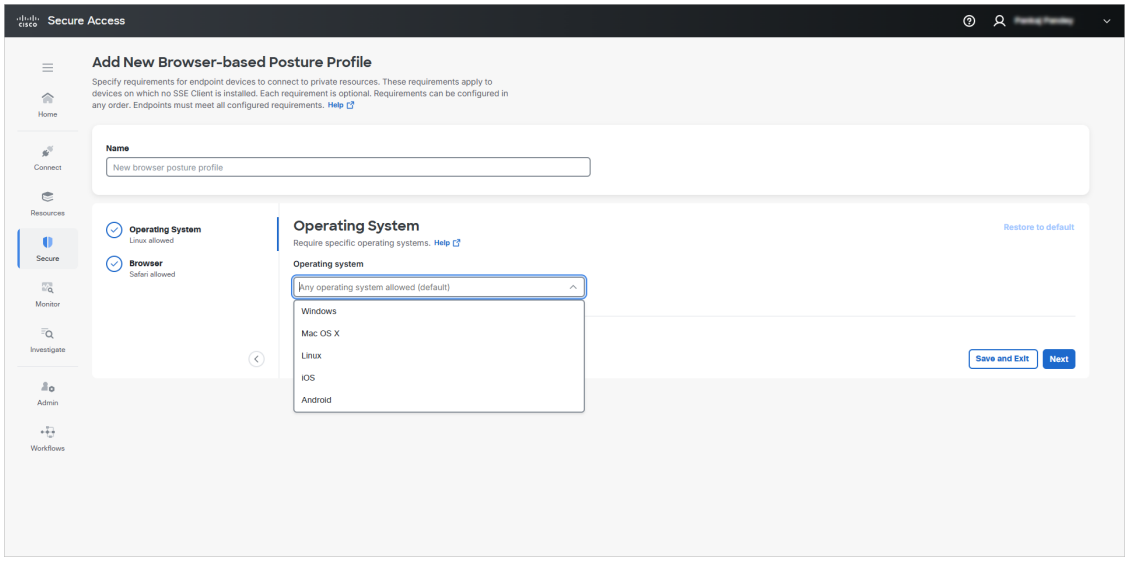
1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



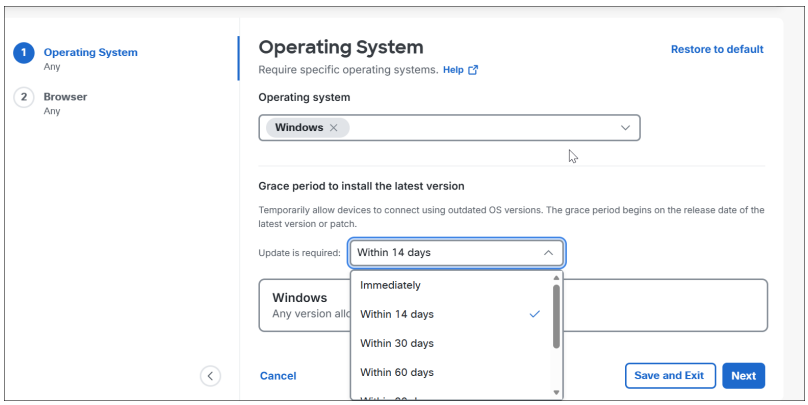
2. For **Zero Trust Connection**, click **Add posture profile**, and choose **Browser-based**.



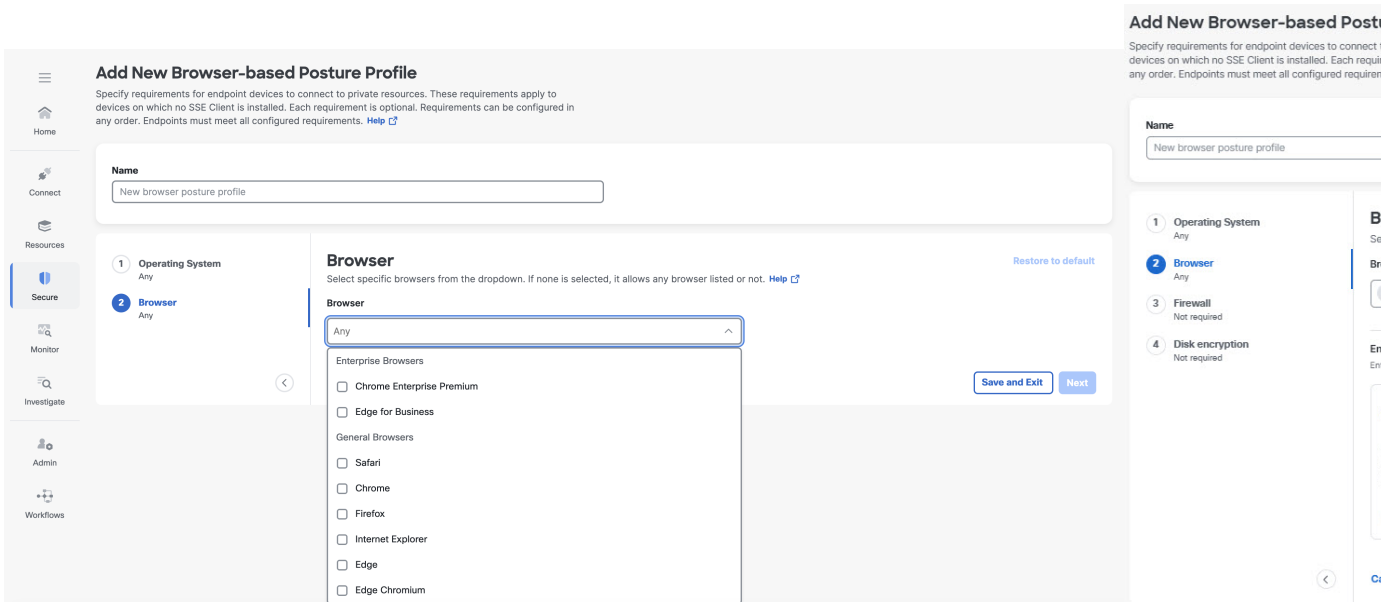
3. Give your posture profile descriptive **Name**.
4. Select the required operating systems from the drop-down list.



5. Under **Grace period to install the latest version**, from the **Update is required** drop down list, select the desired grace period based on your organization policy. You can choose from available day options, such as within 14 days. Click**Save and exit** or **Next** to select supported browsers.



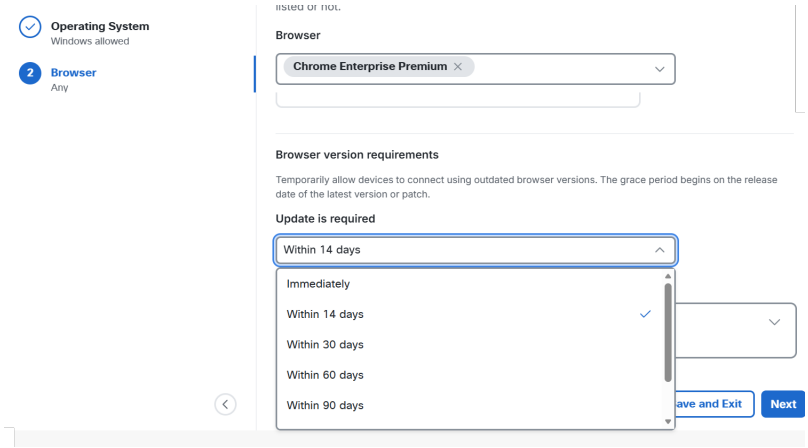
6. Add the required browsers from the drop-down list. Click **Save and Exit** or **Next** to select supported posture requirements.



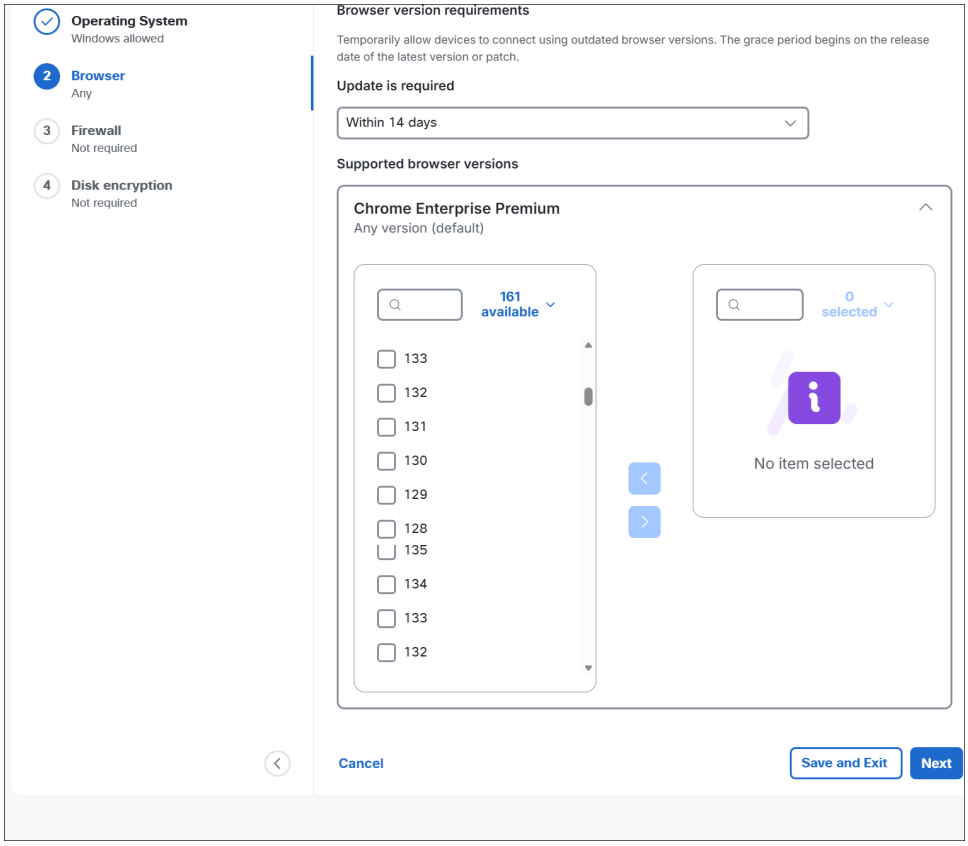
> **Note**
>
> The browser type you select must have already been integrated with Secure Access. If you have not integrated any third-party service, then you cannot continue with this procedure. For more information see Manage Third-Party Integrations on page 2623.

7. Under **Browser version requirements,** from the **Update is required** drop down list, select the desired period based on your organization policy.
   - You can choose from the available day options, such as within 14 days.

> **Note**
>
> The Update required feature is applicable only when the "latest" clause is selected. When you choose the "latest" clause, if a user's browser is not on the latest version, access will be denied. This ensures that only browsers with the most current version are allowed to connect, enhancing security by enforcing up-to-date browser versions.

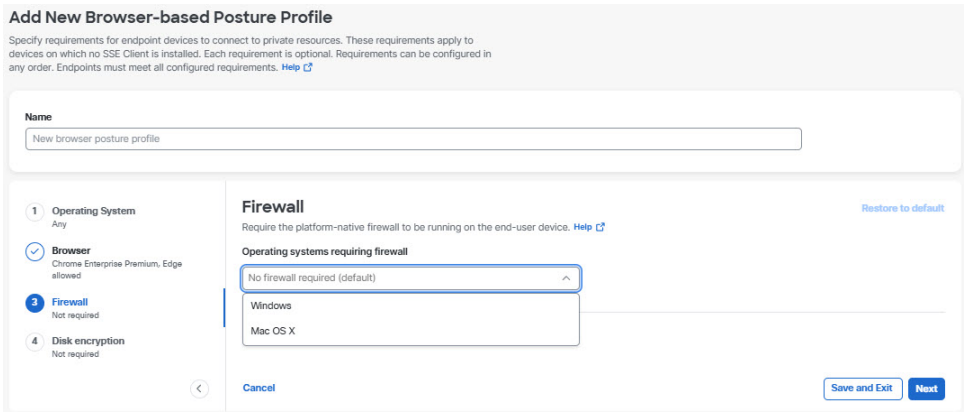


8. Under **Supported browser version**, select the check box for the browser versions you want to allow from the left pane. Click the right arrow button to move the selected versions to the right pane. Click **Save and exit** or **Next** to proceed to supported posture requirements.
   - You can choose from any of the available version options (such as the latest version, current version, and previous versions).

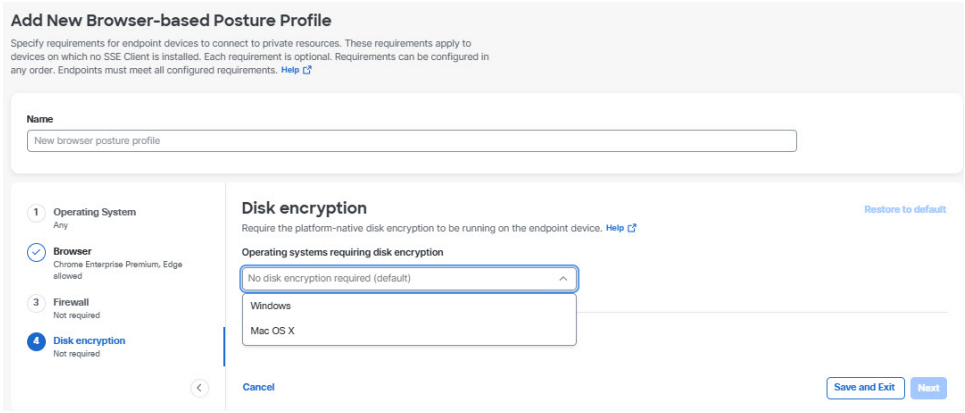


9. Add the posture requirements for the browser you selected:

a) (Optional) **Firewall**: Specify the required platform-native firewall to run on the end-user device.



b) **Disk encryption**: Specify the required platform-native disk encryption to run on the end-user device.



10. Click **Save and Exit** to complete the posture profile. Optionally, click **Next** to modify the selected operating systems.

What to do next

We strongly recommend assigning this posture profile to the Access policy. You can create a new Internet Access rule or Private Access rule, or edit an existing rule.

View a Browser-based Zero Trust Access Posture Profile

View the browser-based zero trust access posture profile for browser used in Secure Access.

View a browser-based Zero Trust Access posture profile to define posture requirements for endpoint devices that connect to private resources.

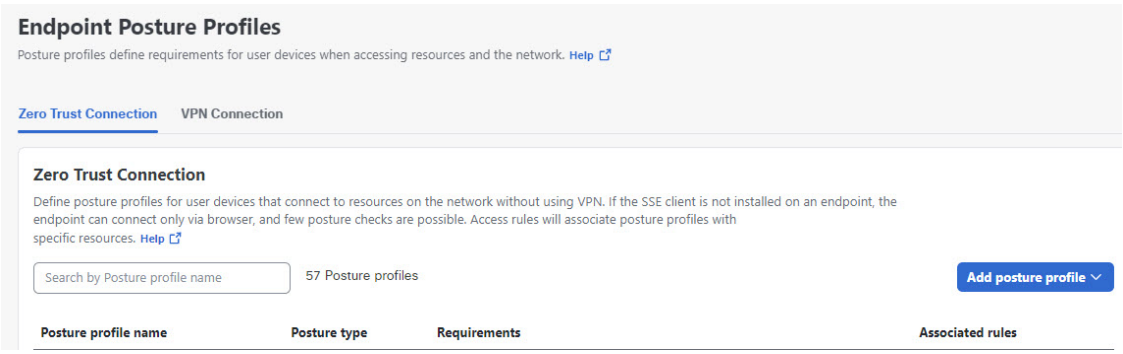
> **Note**
>
> Each requirement is optional; and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

Before you begin

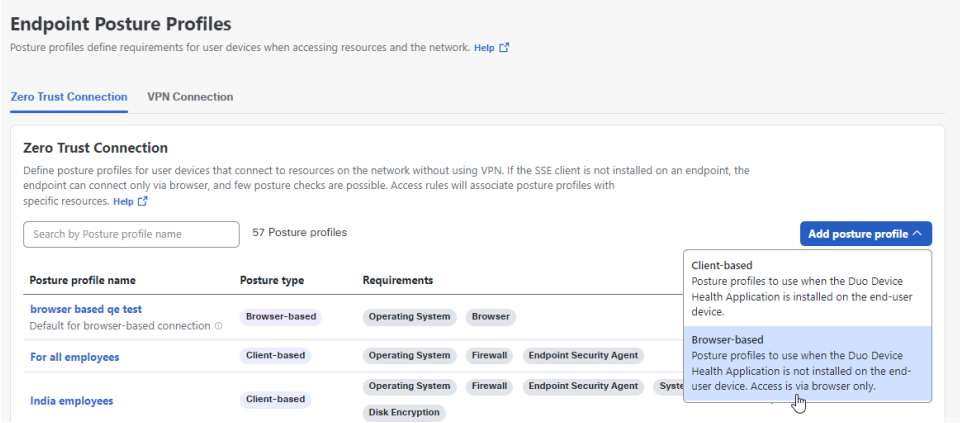
- You must have the full Admin user role. For more information, see Manage Accounts.

Procedure

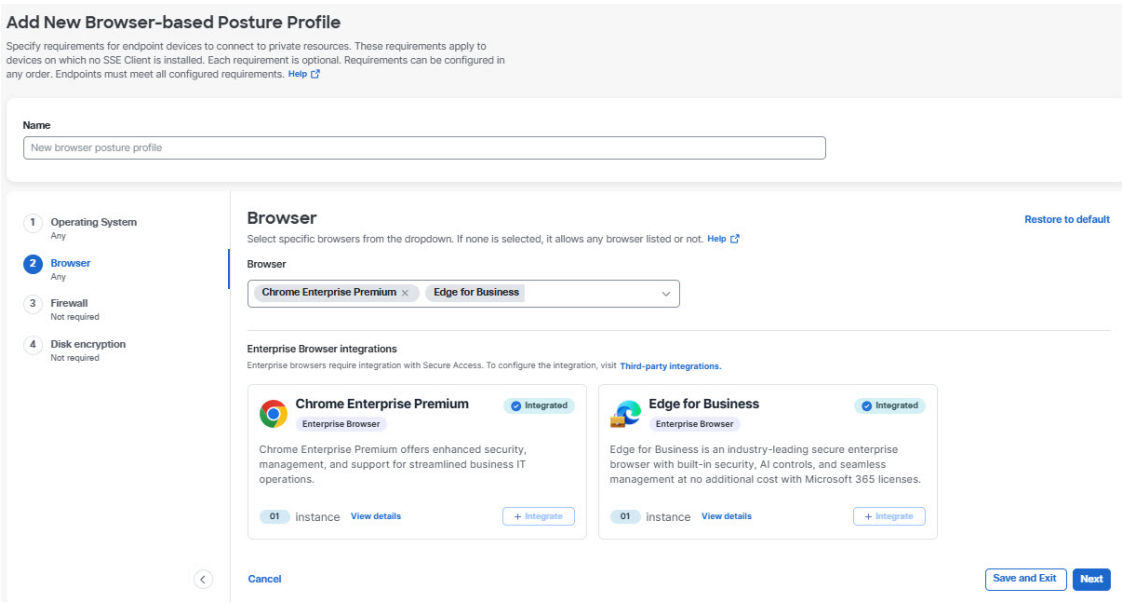
1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



2. For **Zero Trust Connection**, click **Add posture profile** and choose **Browser-based**.



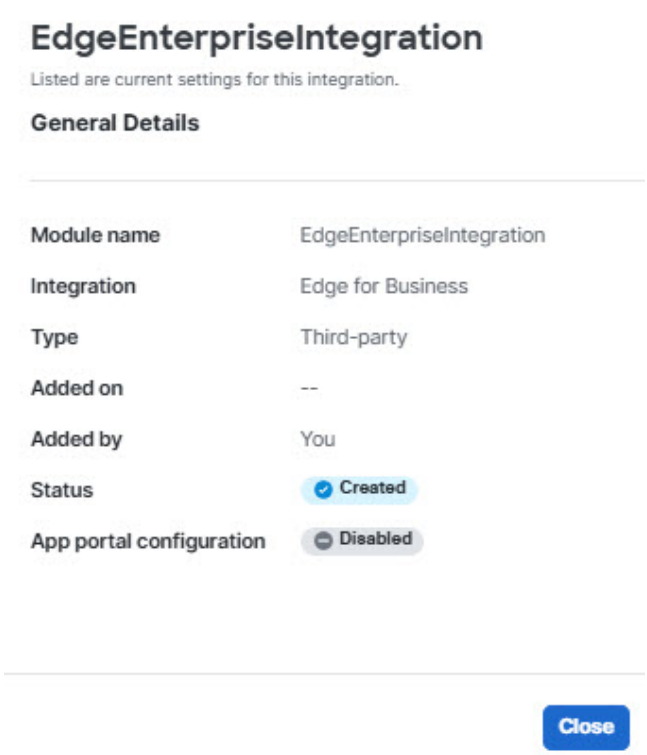
3. On the **Browser** tab, navigate to supported browsers.



4. Click **View details**.

   Navigate to the supported browsers table and click on the name of a posture profile integration to view the details about the integration.

   - **Module name**–The name of the posture profile integration for browser used.
   - **Integration**–The type of the posture profile.
   - **Type**–The type of the Secure Access integration.
   - **Added on**–The date and time when the organization added the posture profile integration.
   - **Added by**–The organization ID and user account that added the posture profile integration.
   - **Status**–The status of the posture profile integration, either **Active** or **Inactive**.
   - **App portal configuration**–The status of the app portal configuration, either **Enabled** or **Disabled**.


EdgeEnterpriseIntegration
Listed are current settings for this integration.
General Details
Module name
EdgeEnterpriseIntegration
Integration
Edge for Business
Type
Third-party
Added on
--
Added by
You
Status
Created
App portal configuration
Disabled
Close

38 Endpoint Security

Topics:

- Manage Endpoint Security

Provides an overview of Endpoint Security in Cisco Secure Access, including Manage Endpoint Security. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Endpoint Security

Describes Manage Endpoint Security in Cisco Secure Access. Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications.

Secure Access is a converged cloud security solution that enables fast, reliable, and secure private network connections to your applications. End users are assured of a secure, transparent user experience, anywhere they work – office, home, or on the road. User devices can read, write, and update private resources by setting up virtual private networks (VPNs) or zero trust network access (ZTNA) connections to Secure Access through IPsec network tunnels.

About Endpoint Posture

Posture is a service in Secure Access that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control user access to protected areas of a network. See View a Endpoint Posture on page 1267.

About Posture Profiles

Posture profiles define requirements for end-user devices when accessing the network and private resources. There are two types of profiles, depending on your connection type:

- **VPN** - Define posture requirements for end-user devices connecting to the network using VPN. The VPN client must be installed on the end-user device. Requirements are checked when the device connects to the network. See Manage VPN Connection Posture Profiles.
- **Zero Trust Access** - Define posture profiles for user devices that connect to resources on the network without using VPN. See Manage Zero Trust Access Posture Profiles.

Endpoint Posture Assessment

Describes Endpoint Posture Assessment in Cisco Secure Access. Endpoint posture assessment involves orchestrating and performing data collection and evaluating the posture of a given endpoint.

Endpoint posture assessment involves orchestrating and performing data collection and evaluating the posture of a given endpoint.

Typically, endpoint posture information is gathered and then published to appropriate data repositories to make collected information available for further analysis supporting organizational security processes.

Endpoint posture assessment typically includes:

- Collecting the attributes of a given endpoint;
- Making the attributes available for evaluation and action; and
- Verifying that the endpoint's posture is in compliance with enterprise standards and policy.

Endpoint Attributes

Describes Endpoint Attributes in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Secure Access can evaluate certain attributes and conditions on end-user devices. This guide describes the endpoint attributes evaluated by Secure Access.

Supported Operating Systems

Describes Supported Operating Systems in Cisco Secure Access. This option checks for the existence of any required operating systems that are needed on the endpoint device.

This option checks for the existence of any required operating systems that are needed on the endpoint device.

The operating system hosts and manages your data, applications, and connected devices. Inadequate protections for the operating system could also affect the performance of all of these components and ultimately affect productivity of your users and the organization.

The following sections describe the supported operating systems and package dependencies for Secure Access posture profiles.

Zero Trust Connections

- Windows
- Mac OS X
- Linux
- iOS
- Android (version 14 or later)
- Chrome Enterprise Premium
- Edge for Business

> **Note**
>
> Edge for Business Posture enforcement checks are only applicable for clients connecting from clients running Windows OS due to restrictions by the MS Edge for Business Connector.

VPN Connections

- Windows
- Mac OS X
- Linux

Inadequate protections for the operating system could also affect the performance of all of these components and ultimately affect productivity of your users and the organization.

Firewall Conditions

Describes Firewall Conditions in Cisco Secure Access. This option checks for the existence of a firewall on the endpoint device.

This option checks for the existence of a firewall on the endpoint device.

- Windows
  - Require the platform-native firewall to be running on the endpoint device.
- Mac OS X
  - Require the platform-native firewall to be running on the endpoint device.

Endpoint Security Agents

Describes Endpoint Security Agents in Cisco Secure Access. This option checks for the existence of an endpoint security agent required to be running on the endpoint device.

This option checks for the existence of an endpoint security agent required to be running on the endpoint device. The Endpoint Security Agent is a modern solution that delivers comprehensive, multilayered protection to safeguard your

device against diverse threats. Its unified architecture allows you to deploy multiple solutions through a single agent for streamlined management and enhanced security.

System Password Enforcement

Describes System Password Enforcement in Cisco Secure Access. This option checks whether a system password is required on the endpoint device.

This option checks whether a system password is required on the endpoint device.

Disk Encryption

Describes Disk Encryption in Cisco Secure Access. This option checks for the existence of disk encryption running on the endpoint device.

This option checks for the existence of disk encryption running on the endpoint device.

Disk encryption ensures that files are always stored on disk in an encrypted form. The files become available to the operating system and applications in readable form while the system is running and unlocked by a trusted user. An unauthorized user inspecting the contents of the disk directly finds garbled random-looking data instead of the actual files.

With user data encryption enabled, the **/home** directory in the file system is encrypted and user data is available when the system is running. The user **/home** partition is mounted on a separate disk partition and block level encryption is enabled for that disk.

> **Note**
>
> By default, the disk encryption check only detects for the presence of the disk encryption software but does not require that particular disk drives are encrypted. On a Windows platform, it is possible to require that the default **C:** drive is encrypted. For more information, see Welcome to Cisco Secure Access.

Supported Browsers

Describes Supported Browsers in Cisco Secure Access. This option checks for the existence of a required web browser on the endpoint device.

This option checks for the existence of a required web browser on the endpoint device.

Windows Registry Conditions

Describes Windows Registry Conditions in Cisco Secure Access. This option checks for the existence of a registry key or the value of the registry key on the endpoint device.

This option checks for the existence of a registry key or the value of the registry key on the endpoint device. The posture check for this partcular field only requires the path to the directory containing the registry and should not include the registry name.

Windows Domain Join

Describes Windows Domain Join in Cisco Secure Access. This option enforces a check to verify if the device has joined a Windows domain.

This option enforces a check to verify if the device has joined a Windows domain. You have the option to also specific a specific SID to ensure a device is joined to a specific Domain.

At this time Secure Access supports both Azure AD and Microsoft Entra. Events generated from successful or failed domain joins and snapshots of detailed posture checks are avilable in the Activity Search Report. By using the Azure AD

you can reduce the risk of devices joined to unapproved domains. Add and managed your domains within your posture profile; see step 9 of Add a Client-Based Zero Trust Access Posture Profile on page 1250.

File Conditions

Describes File Conditions in Cisco Secure Access. This option checks for the existence of a file, the date of a file, and the versions of a file on the endpoint device.

This option checks for the existence of a file, the date of a file, and the versions of a file on the endpoint device.

> **Note**
>
> File conditions are checked against case-sensitive checksum protocols.

Process Conditions

Describes Process Conditions in Cisco Secure Access. This option checks if an application or process is running or not running on the endpoint device.

This option checks if an application or process is running or not running on the endpoint device.

> **Note**
>
> You must include the full name of a process along with its extension to ensure the proper functionality of the Process Conditions option. For example, instead of 'Firefox,' use 'Firefox.exe.'

Certificate Conditions

Describes Certificate Conditions in Cisco Secure Access. Secure Access supports certificate and Security Assertion Markup Language (SAML) authentication for remote access VPN connection profiles.

Secure Access supports certificate and Security Assertion Markup Language (SAML) authentication for remote access VPN connection profiles. This option checks if any required server certificates are present and valid on the endpoint device.

Prerequisites

- You must enable the certificates for authentication when end-users connect on a VPN. For more information, see Add VPN Profiles.

About Certificate Conditions

> **Note**
>
> Secure Access also supports certificate and RADIUS authentication for remote access VPN connection profiles.

A user on VPN is authenticated with both a client certificate and SAML server. The client certificates are installed on every users' device and are validated by CA certificate(s) to verify identity. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers. When a user logs into a SAML-enabled application, the service provider requests authorization from the appropriate IdP. The identity provider authenticates the user's

credentials and returns the authorization to the service provider. Once authorized, the user can use the application. In the case of certificate and SAML authentication, certificates are authenticated before SAML authentication.

When selected, you can configure up to two certificates to authenticate each endpoint. For each certificate, configure the following attributes:

- **Subject** – The subject field identifies the entity that owns or is associated with the public key embedded in the certificate. It often corresponds to the hostname or domain name the VPN server uses.

  Note

  The subject field is important because it ensures that VPN clients can verify the identity of the server they are connecting to by checking the certificate's subject against the expected hostname. The Common Name (CN) within the subject field is often used to identify the primary hostname of the server.

- **Issuer** – The issuer field is the entity (trusted authority) that issues the digital certificates used for authentication and secure communication within a VPN. These certificates verify the identity of the VPN server and clients, ensuring secure access to the network.
- **Subject alternate name** – The subject alternative name field allows a single certificate to cover multiple hostnames or IP addresses, ensuring secure connections when a VPN client connects to a server with different names or addresses.

You select the **Type** to check when validating the endpoint certificate. You can manually enter a **Value**, or you can select **SAML attribute name** from the **Type** drop-down to use the values provided by the SAML identity provider (IdP) that is integrated with Secure Access.

View a Endpoint Posture

Learn how to view Endpoint Posture profile requirements, and review browser-based integration criteria and rules in Zero Trust Connection.

To view the Endpoint Posture profile requirements defined for end-user devices when accessing the network and private resources.

Note

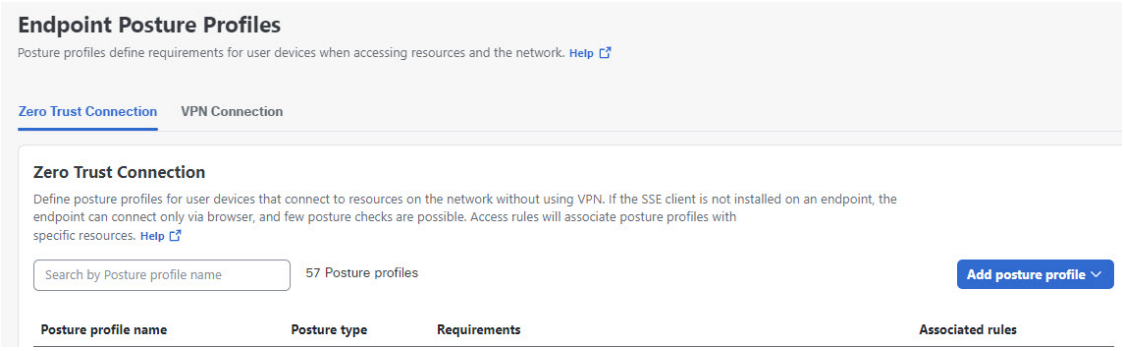
Each requirement is optional; and requirements can be configured in any order. However, endpoints must meet all conditions of any configured requirement.

Before you begin

- You must have the full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Profiles** > **Endpoint Posture Profiles**.



2. For **Zero Trust Connection**, click **Posture Profile Name** to view the browser based integration details.
   - **Applied Criteria**– The applied criteria for the browser based integration.
   - **Applied Rules**–The applied rules for the browser based integration.



3. Click **Edit**.

Part IV

Security Protection and Enforcement

Topics:

- Virtual Appliances
- File Inspection and Analysis
- File Type Controls
- Notification Pages
- Data Loss Prevention
- Secure Browser Extension
- Data Classifications
- Built-in Data Identifiers
- AI Guardrails Data Classifications
- Secure ICAP
- Requirements for Salesforce Tenants
- SaaS API Data Loss Prevention
- Cloud Malware Protection
- Remote Browser Isolation
- Internet Security
- PAC Files
- Certificates
- Secure Access Investigate

Configuring security features, enforcement, and advanced protection capabilities.

39 Virtual Appliances

Topics:

- Get Started with Virtual Appliances
- Manage VAs in Secure Access
- Deploy Virtual Appliances
- Deploy VAs in Hyper-V for Windows 2012 or Higher
- Deploy VAs in VMware
- Deploy VAs in Microsoft Azure
- Deploy VAs in Amazon Web Services
- Deploy VAs in Google Cloud Platform
- Deploy VAs in KVM
- Deploy VAs in Nutanix
- Deploy VAs in Alibaba Cloud
- Configure Virtual Appliances
- Local DNS Forwarding
- Test Virtual Appliance Deployments
- SNMP Monitoring for Virtual Appliances
- Troubleshoot Virtual Appliances

Provides an overview of Virtual Appliances in Cisco Secure Access, including Get Started with Virtual Appliances, Manage VAs in Secure Access, and Deploy Virtual Appliances. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with Virtual Appliances

Describes Get Started with Virtual Appliances in Cisco Secure Access. Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines.

Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines. Virtual Appliances function as conditional DNS forwarders on your network. VAs record the internal IP address information of DNS requests for usage in reports, security enforcement, and category filtering. VAs encrypt and authenticate DNS data for enhanced security.

Supported Deployments

Describes Supported Deployments in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can deploy Secure Access VAs with these hypervisors and cloud environments:

- VMWare ESX/ESXi
- Windows Hyper-V
- KVM
- Microsoft Azure
- Google Cloud Platform
- Amazon Web Services
- Nutanix
- Alibaba Cloud

For more information, see Deploy Virtual Appliances.

How Secure Access Virtual Appliances Work

Describes How Secure Access Virtual Appliances Work. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Virtual Appliances act as conditional DNS forwarders in your network. VAs intelligently forward public DNS queries to the Cisco Secure Access global network and local DNS queries to your existing local DNS servers and forwarders. Every public DNS query sent to Secure Access is encrypted, authenticated, and includes the client's internal IP address.

VAs do not cache DNS records. Caching occurs on the Secure Access DNS resolvers. When a VA responds with records to an endpoint's DNS query, any Time-to-Live (TTL) values in the response are equal to the TTLs as set by the authoritative DNS nameserver minus any time a record set has been in the Secure Access resolver cache.

Virtual Appliances and Granular Identity Information

Describes Virtual Appliances and Granular Identity Information in Cisco Secure Access. If you already forward DNS requests to Secure Access, all the DNS traffic visible in your Secure Access reports come from Registered Networks.

If you already forward DNS requests to Secure Access, all the DNS traffic visible in your Secure Access reports come from Registered Networks. The VAs provide internal IP visibility, allowing you to track down malicious or inappropriate traffic within your network to a specific IP address.

Without Virtual Appliances

Describes Without Virtual Appliances in Cisco Secure Access. You can not research security and DNS traffic for an individual computer or IP address.

You can not research security and DNS traffic for an individual computer or IP address.

app.yesware.com	Allowed		Office NAT 1	67.215.	N/A
app.yesware.com	Allowed		Office NAT 1	67.215.	N/A

With Virtual Appliances

Describes With Virtual Appliances in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Virtual Appliances record the internal IP address of every DNS request. You can associate DNS traffic to a specific internal IP address.

search.cpan.org	Allowed	Software/Technology	Vancouver	67.215.	10.10.10.183
.cisco.com	Allowed	Software/Technology,...	forwarder04....	67.215.	10.111.0.208
data.flurry.com	Allowed	Software/Technology	Townsend	67.215.	10.112.0.62
ads.flurry.com	Allowed	Software/Technology,...	Townsend	67.215.	10.112.0.62

Active Directory Integration

Describes Active Directory Integration in Cisco Secure Access. You can enable the integration of Active Directory (AD) with Secure Access VAs.

You can enable the integration of Active Directory (AD) with Secure Access VAs. AD provides user, group, or computer identity information in both reports and access rules. For more information, see the AD Integration with Virtual Appliances.

Configure Granular Rules

Describes Configure Granular Rules in Cisco Secure Access. Set various access rules in your policy for example, bring your own device (BYOD) corporate networks, guest Wi-Fi, server-only networks, by specifying the internal IP or IP range.

Set various access rules in your policy for example, bring your own device (BYOD) corporate networks, guest Wi-Fi, server-only networks, by specifying the internal IP or IP range. Granular rules make it easy to filter unwanted content and malicious traffic on a per-network basis.

Prerequisites for Virtual Appliances

Describes Prerequisites for Virtual Appliances in Cisco Secure Access. The Cisco Secure Access Virtual Appliance is a lightweight virtual machine that acts as a non-caching, conditional DNS forwarder.

The Cisco Secure Access Virtual Appliance is a lightweight virtual machine that acts as a non-caching, conditional DNS forwarder. Before you deploy the Secure Access Virtual Appliances in your environments, we recommend that you review the requirements and prerequisites.

> **Note**
>
> Secure Access Virtual Appliance images are configured with Ubuntu v22.04.

Endpoint Software

Describes Endpoint Software in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- You are not required to install client-side software for Virtual Appliance deployments.
- You do not have to reconfigure image operating systems.

Virtual Appliance Requirements and Prerequisites

Describes Virtual Appliance Requirements and Prerequisites in Cisco Secure Access. Ensure your Virtual Appliance (VA) complies with Secure Access requirements annd prerequisites prior to onboarding them.

Ensure your Virtual Appliance (VA) complies with Secure Access requirements and prerequisites prior to onboarding them. Confirm they match the following general requirements for optimal support and functionality:

- For information about license and package requirements, see Determine Your Current Package.
- At a minimum, to process millions of DNS queries per day, allocate these resources for each VA:
  - Two virtual CPU cores
  - 2GB RAM
  - 7GB of disk space
- Deploy two Virtual Appliances in a Site. VAs must be deployed in pairs to ensure redundancy at the DNS level and to allow for updates without downtime.
- Download a fresh image from Secure Access for each deployment. You need to download a fresh image from Umbrella for each deployment, and when there is a new version.
- **Correct Date/Time**–Ensure your hypervisor host has the correct date and time. The incorrect date or time can cause update or sync issues with the VAs. The VA syncs time independently and is always set to UTC by default.
- Each VA can process millions of DNS requests in a single day. If your network could exceed this number, see Virtual Appliance Sizing Guide.
- VAs deployed on platforms such as Amazon Web Services and Google Cloud Platform require a minimum of 1GB RAM per CPU core.

Microsoft Hyper-V Requirements

Your Microsoft Hyper-V appliance must have one of the following Windows Server operating systems:

- Windows Server 2012, SP1, or R2 (Standard or Data center), 2016 or 2019 with Hyper-V role
- Hyper-V Server 2012, 2012 R2, 2016 or 2019

> **Note**
>
> Deploying the virtual appliance through System Center Virtual Machine Manager (SCVMM) has not been qualified and is not officially supported.

Cloud Platform Requirements

Secure Access supports the following cloud platform environments:

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

KVM Requirements

Secure Access supports the following KVM Linux versions:

- KVM on Ubuntu Linux (supported LTS versions)
- KVM on Red Hat Linux (supported versions)

Nutanix Requirements

Confirm your Nutanix platform has the following running:

- Supported version of Nutanix Acropolis Hypervisor (AHV)

Networking Requirements

Describes Networking Requirements in Cisco Secure Access. Once VAs are deployed, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders.

Once VAs are deployed, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders. This is usually accomplished through the network's DHCP configuration. For more information, see Local DNS Forwarding.

Allow Connections to Secure Access Domains and Services

Describes Allow Connections to Secure Access Domains and Services. You must allow connections to certain domains and URLs for the Virtual Appliances to communicate with the Secure Access cloud services and local DNS servers.

You must allow connections to certain domains and URLs for the Virtual Appliances to communicate with the Secure Access cloud services and local DNS servers. These requirements apply to each platform where the VA is deployed.

- For DNS traffic to Secure Access, see Secure Access DNS Resolvers.
  - Standard and encrypted DNS queries to the Secure Access DNS resolvers.
    - Port 443 is used as failover if your firewall does not allow DNSCrypt on port 53.
    - Port 5353 is used as failover if DNSCrypt is not allowed on port 53 and port 443.
- For DNS traffic on internal domains, allow connections on the Virtual Appliance to local DNS servers on UDP and TCP port 53.
- For more information, see Secure Access DNS and Web – Client Certificate Revocation Services.
- For more information, see Secure Access DNS and Web – Client Configuration Services.
- For more information, see Secure Access Cisco Secure Client and External DNS Resolution.

Network Time Protocol Servers

Describes Network Time Protocol Servers in Cisco Secure Access. Allow connections from your Virtual Appliances to NTP servers on UDP port 123.

Allow connections from your Virtual Appliances to NTP servers on UDP port 123.

- **ntp.ubuntu.com**
  - 185.125.190.57 /32
  - 185.125.190.56/32
  - 91.189.91.157/32
  - 185.125.190.58/32

> **Note**
>
> If you have configured custom NTP servers on the VA, use the custom NTP server IPs instead.

Intrusion Protection Systems (IPS) and Deep Packet Inspection (DPI)

Describes Intrusion Protection Systems (IPS) and Deep Packet Inspection (DPI) in Cisco Secure Access. If you have deployed an IPS or DPI, ensure that traffic on port 53 TCP/UDP to and from the VAs is excluded from packet inspection.

If you have deployed an IPS or DPI, ensure that traffic on port **53 TCP/UDP** to and from the VAs is excluded from packet inspection. The Secure Access DNS encryption methods might be flagged and dropped. If the VAs can not successfully send and receive encrypted DNS packets, Secure Access displays a warning.

Network Address Translation (NAT)

Describes Network Address Translation (NAT) in Cisco Secure Access. If a routing device running a separate NAT is placed between the endpoints and VAs in your organization, than Secure Access displays the NAT device's IP address for the endpoint's IP address.

If a routing device running a separate NAT is placed between the endpoints and VAs in your organization, than Secure Access displays the NAT device's IP address for the endpoint's IP address. The endpoints must reach the VAs without being subjected to a separate NAT. If you are unable to remove a routing device with a separate NAT, you may have to run a separate set of VAs within that NAT. If you have any questions regarding this matter, contact Support.

Encrypting Traffic with DNSCrypt

Describes Encrypting Traffic with DNSCrypt in Cisco Secure Access. Virtual Appliances support DNSCrypt between the virtual machine and the Secure Access public DNS resolvers.

Virtual Appliances support DNSCrypt between the virtual machine and the Secure Access public DNS resolvers. This means that any information contained in the EDNS packets forwarded from the VA are encrypted by DNSCrypt and cannot be intercepted. For optimum protection, this feature is enabled by default.

Unencrypted traffic is considered a problem that should be resolved. When encryption can not be established between your VA and the Secure Access DNS servers, Secure Access displays a warning. Encryption is established with a probe sent on port 53 (UDP/TCP) to the following addresses:

- IPv4: 18.252.251.72 and 18.254.118.193
- IPv6: 2600:1f15:ef3:1800::aaaa and 2600:1f15:ef3:1801::bbbb

If you have a firewall or IPS/IDS doing deep packet inspection and expecting to see only DNS traffic, the probe may fail.

If the probe fails, it is retried on 443 (UDP/TCP) and then on 5353 (UDP). Thus, the encrypted packets may not match the expected traffic on that port. Review your firewall configuration if that is the case and open a case with Support if you believe that you are allowing this traffic.

Virtual Appliance Deployment Guidelines

Describes Virtual Appliance Deployment Guidelines in Cisco Secure Access. Cisco Secure Access supports various deployments and configurations of Secure Access Virtual Appliances (VAs).

Cisco Secure Access supports various deployments and configurations of Secure Access Virtual Appliances (VAs).

> **Note**
>
> You must configure the Internal Domains for your organization. The endpoints must use the Secure Access Virtual Appliances as the primary DNS server.

Deploy Virtual Appliances in Pairs

Describes Deploy Virtual Appliances in Pairs in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

VAs must always be deployed in pairs. Running two or more VAs offers high availability in case of system updates. This ensures that there is no interruption in Internet service during an update, and allows you to configure updates for scheduled maintenance windows or off-hours.

- **No downtime associated with upgrades**

  When an upgrade takes place, individual virtual appliances will restart, causing up to 20 minutes of downtime. During this time, any DNS queries routed to the virtual appliance will time out and you will lose internet connectivity. Running two VAs ensures that there is no interruption in Internet service.

- **Ability to schedule updates**

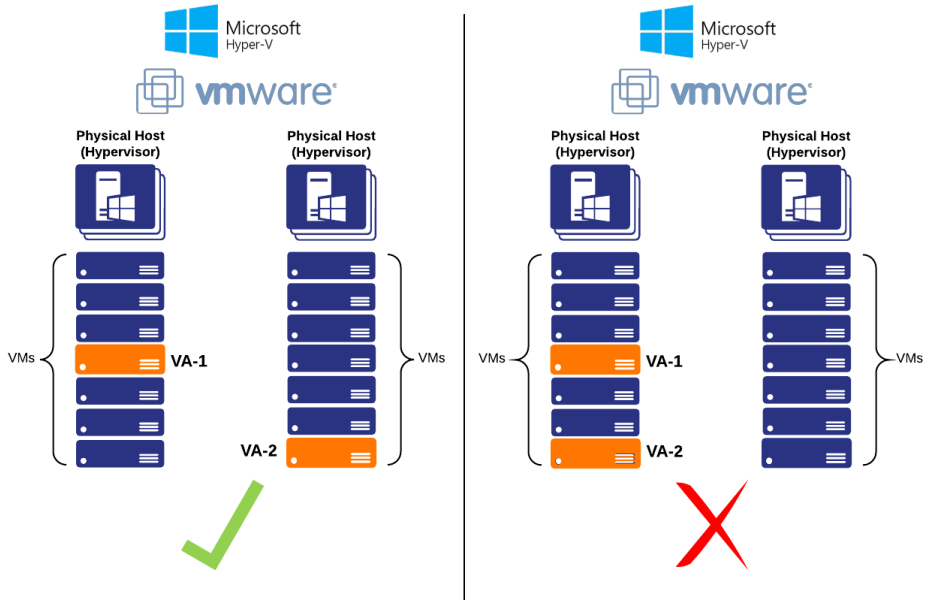
  Running two VAs allows for scheduling updates. You can schedule updates for off-hours or during scheduled maintenance windows.

- **High availability**

  If issues arise in one of your VAs, or if you would like to rebuild or move a VA to another host, you can take action without interruptions.

To set up a second virtual appliance, repeat the procedure for setting up the first one. For more information, see Deploy Virtual Appliances.

Whenever possible, deploy VAs on separate physical hypervisor hosts. If a hypervisor hosting a VA becomes unavailable, the second VA will continue serving DNS requests without interruption.



Multiple DNS Egresses

Describes Multiple DNS Egresses in Cisco Secure Access. In most cases where multiple offices or points of presence exist, each office sends and receives its DNS traffic.

In most cases where multiple offices or points of presence exist, each office sends and receives its DNS traffic. An office independently sends DNS queries directly to Secure Access. In this case, each office requires its own pair of VAs. When using Secure Access, DNS queries always route to the closest Secure Access data center.

Single DNS Egress

Describes Single DNS Egress in Cisco Secure Access. In some cases, especially if the networks are geographically close to one another, a single egress may handle all DNS traffic originating from multiple networks.

In some cases, especially if the networks are geographically close to one another, a single egress may handle all DNS traffic originating from multiple networks. This topology is typically used to route traffic through security appliances, Active Directory Domain Controllers, or other network and security devices at a central location to avoid deploying and managing them at every location. This is usually accomplished with a Site-2-Site VPN or an MPLS circuit.

In this case, only the office which sends and receives public DNS queries requires VAs.

Double NAT

Describes Double NAT in Cisco Secure Access. Endpoints and Virtual Appliances that are not behind the same Network Address Translation (NAT) address result in the VAs seeing the IP address of the NAT device instead of the endpoint's IP address.

Endpoints and Virtual Appliances that are not behind the same Network Address Translation (NAT) address result in the VAs seeing the IP address of the NAT device instead of the endpoint's IP address.

With Secure Access Virtual Appliance deployments, we do not recommend a double NAT environment. A double NAT environment can limit both the ability to create granular rules and endpoint-level reporting in Secure Access. However, you can still create a separate rule for the NAT IP address, which would be useful for Guest Wi-FI situations, where knowing the endpoint IP address may not necessarily be helpful, but having a separate rule for that group of endpoints is important.

Virtual Appliance Sizing Guide

Describes Virtual Appliance Sizing Guide in Cisco Secure Access. The following information is a guide to help you deploy the Cisco Secure Access Virtual Appliances (VAs) in your organization's environment.

The following information is a guide to help you deploy the Cisco Secure Access Virtual Appliances (VAs) in your organization's environment. The key factors are ensuring that the hardware prerequisites are met, and understanding the network latencies between hops and the overall number of Secure Access Sites and users for each VA.

Prerequisites and Network Requirements

- For more information, see Prerequisites for Virtual Appliances.

High-Traffic Sites and Virtual Appliances

Describes High-Traffic Sites and Virtual Appliances in Cisco Secure Access. For sizing guidance, increasing the number of CPU cores on a VA will improve its performance, but the amount of RAM allocated to the machine must scale along with the number of CPU cores present.

For sizing guidance, increasing the number of CPU cores on a VA will improve its performance, but the amount of RAM allocated to the machine must scale along with the number of CPU cores present.

Secure Access requires that you allocate at least 1 GB of RAM for each CPU core on the VA. For example, a VA deployed with two CPU cores should have a minimum of 2GB of RAM allocated to it.

VA Specifications	Maximum Queries per Second at Maximum 80% CPU Utilization
1 CPU, 1GB RAM	1300
2 CPU, 2 GB RAM	3500
4 CPU, 4 GB RAM	8000
8 CPU, 8 GB RAM	16000
16 CPU, 16 GB RAM	28000

AD Connector Sizing Guidelines

Describes AD Connector Sizing Guidelines in Cisco Secure Access. For Active Directory integration with Virtual Appliances, we recommend that you size the AD Connector deployment for the number of VAs and domain controllers configured to communicate with this connector.

For Active Directory integration with Virtual Appliances, we recommend that you size the AD Connector deployment for the number of VAs and domain controllers configured to communicate with this connector.

Number of Virtual Appliances	Number of Domain Controllers	Minimum Connector Specifications
1-2	1-5	2 CPU, 1 GB RAM
4-15	6-20	4 CPU, 8 GB RAM
16-20	21-64	4 CPU, 16 GB RAM
>20	>64	8 CPU, 32 GB RAM

Each domain controller is assumed to process a maximum of 400 AD events a second. If any of your domain controllers are processing more events, make sure to increment the number of domain controllers accordingly. For example, if you have a domain controller that processes around 1000 AD events a second at peak load, count that as three domain controllers in the sizing table above.

If a connector is run on a system with lower CPU and memory specifications, the connector will continue to function. Some optimizations, such as parallel synchronization of login events to virtual appliances, will not be turned on.

Deployment Considerations

Describes Deployment Considerations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The number and location of VAs deployed in your environment depends on:

- Overall latency:
  - Latency between VA and the Secure Access Anycast DNS resolvers
  - Latency between users and the VAs
- Number of Sites
- Number of users served by the VAs

Overall Latency

Describes Overall Latency in Cisco Secure Access. In general, clients on the network have the best web browsing experience when the total time to retrieve web resources is under 300ms.

In general, clients on the network have the best web browsing experience when the total time to retrieve web resources is under 300ms. This total time to obtain web resources (such as documents, images, and stylesheets) includes both the time to retrieve a DNS response and the time needed to establish a connection with the server indicated in the DNS response. Secure Access aims to minimize the distance that a DNS packet must travel from a client device to our DNS resolvers. However, we do not control the responsiveness of those web servers or how traffic from various locations on the Internet is routed.

TOTAL TIME = *Time to retrieve DNS response + Time to retrieve a web resource*

There are two factors to consider when optimizing DNS response time: the distance between the VA and the Secure Access Anycast DNS resolvers, and the distance between the client and the VA.

The VA, when deployed, will forward all externally-bound DNS requests to the Secure Access DNS resolvers, 18.252.251.72 and 18.254.118.193 or 2600:1f15:ef3:1800::aaaa and 2600:1f15:ef3:1801::bbbb. Therefore, when determining the latency between the VA and the closest Secure Access data center, we recommend an average DNS response time under 150ms for the best user experience.

When determining where to deploy VAs in your environment, you will want to take into account the distance between the clients that will utilize the VAs and the VAs themselves. For optimal performance, an average ping time between a client and the VM host on which the VA lives should not exceed 50ms.

Number of Secure Access Sites

Describes Number of Secure Access Sites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

Secure Access Sites allow you to divide up your Secure Access deployments. Each Secure Access Site is an isolated deployment in which the components will only communicate with other components in the same Secure Access Site. This is primarily useful in environments containing locations with high-latency connections or in environments with locations whose internal IP space overlaps.

Secure Access requires that you deploy at least two Virtual Appliances for a Site. This ensures high availability of the Virtual Appliances and the option to receive updates without downtime.

Number of Users for a VA

Describes Number of Users for a VA in Cisco Secure Access. A typical VA deployed with minimum hardware requirements has a tested throughput of at least 2000 queries per second.

A typical VA deployed with minimum hardware requirements has a tested throughput of at least 2000 queries per second.

Taking into account these metrics, a single VA can handle DNS requests from at least 57,000 concurrent users. Secure Access defines a single user as a client that generates an average of 1000 DNS requests in a typical eight-hour workday. Therefore, Secure Access defines concurrent users as the number of users or devices sending DNS requests to a VA at the same time.

If the VA specifications are increased to two virtual CPUs and 1GB RAM, a single VA will be able to handle DNS requests from at least 115,000 concurrent users. The number of users on the network likely will NOT be the limiting factor when determining the number of VAs to deploy.

Manage VAs in Secure Access

Describes Manage VAs in Secure Access. Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines that function as conditional DNS forwarders on your network.

Cisco Secure Access Virtual Appliances (VAs) are lightweight virtual machines that function as conditional DNS forwarders on your network. Secure Access VAs support DNS-layer security only.

In Secure Access, you can manage the configuration and deployment of the VAs for your organization.

First, download the images for the VAs and configure authentication for the VAs. Then deploy the VAs in your environment.

- Configure the authentication for secure communications between Secure Access and your VAs. For more information, see Configure Authentication for Virtual Appliances.
- Download the software images to deploy the Secure Access VAs in your environment. For more information, see Deploy Virtual Appliances.

Manage the Secure Access Site.

- Manage the Site associated with the VA. For more information, see Manage Site for Virtual Appliance.

Manage the settings and updates for the VAs.

- Manage the settings for the DNS forwarders. For more information, see Manage DNS Forwarders.
- Configure automatic updates on the VAs in the organization or make a manual update to a VA. For more information, see Configure Updates to Virtual Appliances.

Configure Authentication for Virtual Appliances

Describes Configure Authentication for Virtual Appliances in Cisco Secure Access. Cisco Secure Access communicates with the Secure Access Virtual Appliances (VAs) that are deployed in your organization.

Cisco Secure Access communicates with the Secure Access Virtual Appliances (VAs) that are deployed in your organization. Secure Access makes software syncs and health checks to your VAs and requires that API requests from the VAs use authentication.

To manage the authentication of the communications from the VAs to Secure Access, we recommend that you configure API key credentials for your VA deployments.

Your API key credentials apply to all AD Connectors and Virtual Appliances deployed in your environment.

> **Note**
>
> The API key authentication is available for Secure Access Virtual Appliance version 3.7.0 and newer and the Cisco AD Connector version 1.14.4 or newer.

For more information about configuring authentication for AD Connectors and Virtual Appliances, see Configure Authentication for AD Connectors and VAs.

How to Set Up Your API Credentials

Provides instructions for completing the How to Set Up Your API Credentials workflow in Cisco Secure Access. First, create the Secure Access Key Admin API key and secret.

Procedure

1. First, create the Secure Access Key Admin API key and secret.
2. Then, use your Secure Access Key Admin API key credentials to generate your Secure Access client API key and secret.

What to do next

Your Secure Access client API key credentials are stored in the Virtual Appliances deployed in the organization.

Important

Secure Access client API key credentials are valid for 90 days.

Virtual Appliances use your Secure Access client API key credentials to generate an OAuth 2.0 access token. The access token is included in every API request from the Virtual Appliance to Secure Access.

Authentication for VAs is available in Secure Access Virtual Appliance version 3.7.0 and newer.

Procedure for Configuring Authentication for Virtual Appliances

Describes Procedure for Configuring Authentication for Virtual Appliances in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Secure Access Virtual Appliance version 3.7.0 and newer.

Create a Secure Access Key Admin API key and secret. Use the Secure Access Key Admin API credentials to generate your Secure Access client API key credentials.

The Secure Access client API key and secret are stored in the VAs that you deploy in your environments. The generated API credentials (key and secret) apply to all VAs in the organization.

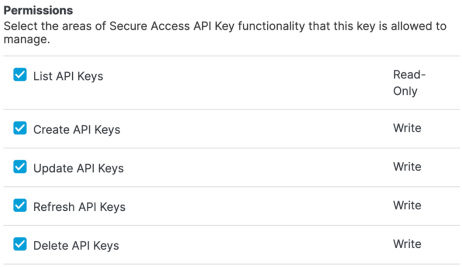
- Step 1 – Create the Key Admin API Key Credentials
- Step 2 – Add the Key Admin API Key Credentials

Step 1 – Create the Key Admin API Key Credentials

Provides instructions for completing the Step 1 – Create the Key Admin API Key Credentials workflow in Cisco Secure Access. Create a Secure Access Key Admin API key.

Procedure

Create a Secure Access Key Admin API key. For more information, see Add Key Admin API Keys. Select each type of permission for the key.



Note

Save your Key Admin API key and secret and use these credentials to configure the authentication for the VAs in the organization.

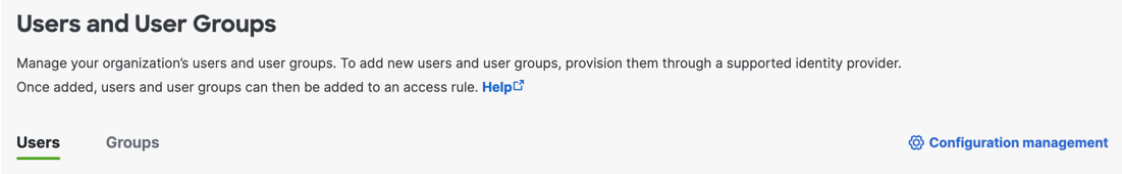
Step 2 – Add the Key Admin API Key Credentials

Provides instructions for completing the Step 2 – Add the Key Admin API Key Credentials workflow in Cisco Secure Access. Add the Secure Access Key Admin API key and secret to the VA configuration in Users and Groups.

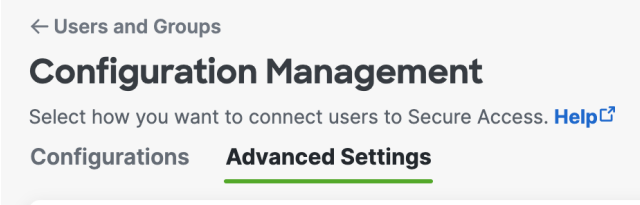
Add the Secure Access Key Admin API key and secret to the VA configuration in **Users and Groups**. Then, generate a Secure Access client API key and secret.

Procedure

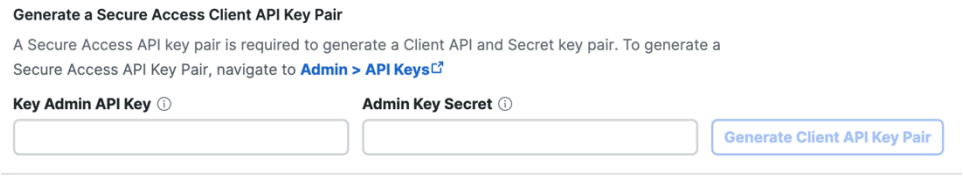
1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.



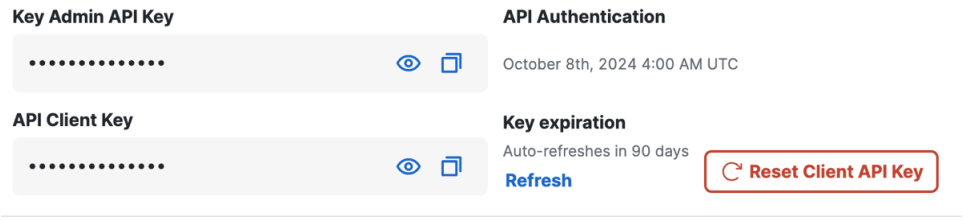
2. Click **Advanced Settings**.



3. For **Key Admin API Key**, add the Key Admin API key, and for **Key Admin Key Secret**, add the Key Admin API key secret. For information about creating the Key Admin API key, see Step 1 – Create the Key Admin API Key Credentials.



4. After you add the Key Admin API key and secret, click **Generate Client API Key Pair**.
5. Save the Secure Access client API key and secret. Secure Access updates the client API key and secret automatically every 90 days.



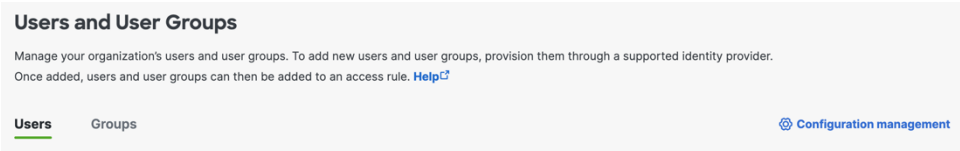
Refresh Client API Key and Secret

Provides instructions for completing the Refresh Client API Key and Secret workflow in Cisco Secure Access. Refresh your Secure Access client API key and secret.

Refresh your Secure Access client API key and secret.

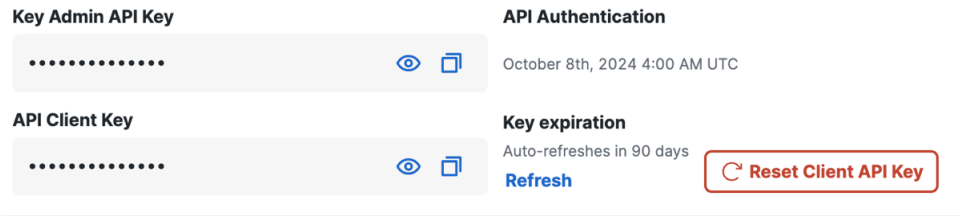
Procedure

1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.

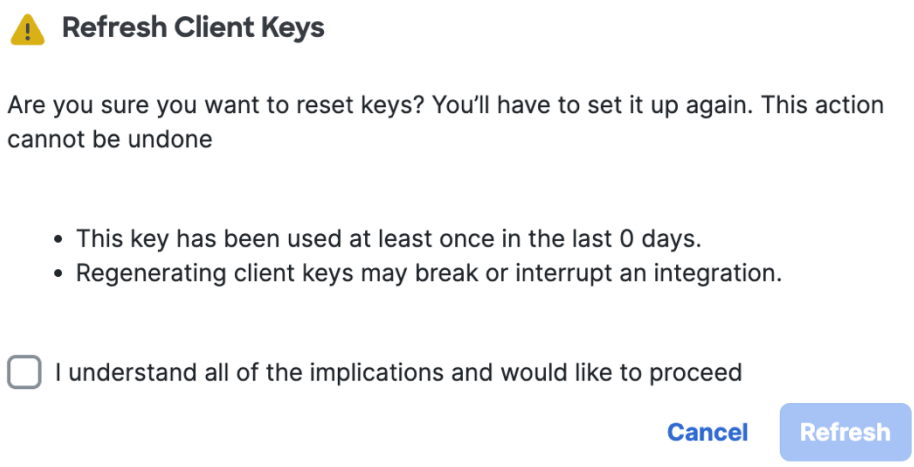


2. Click **Advanced Settings**.
3. Click **Refresh**.

   Secure Access refreshes the client API key and secret.



4. For **Refresh Client Keys**, check the box to confirm the deletion of the client API key and secret.



5. Click **Refresh**.

Reset Client API Key

Provides instructions for completing the Reset Client API Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

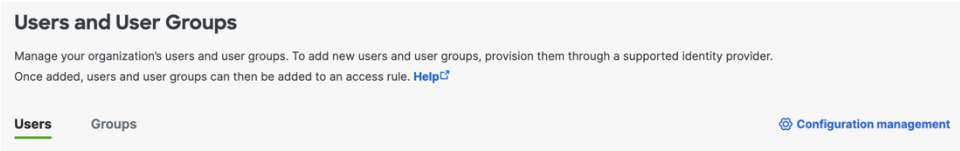
Delete your Secure Access Key Admin API key and Secure Access client API key.

Important

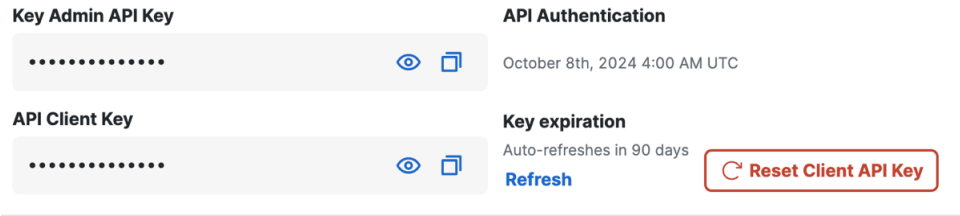
After you delete the Key Admin API key and client API key, existing VA deployments may continue to use the stored Secure Access client API key and secret for up to 90 days.

Procedure

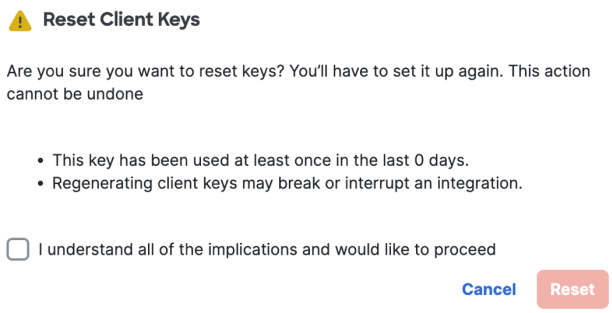
1. Navigate to **Connect** > **Users and User Groups** > **Configuration Management**.



2. Click **Advanced Settings**.
3. Click **Reset Client API Key**.



4. For **Reset Client API Keys**, check the box to confirm the deletion of both the Key Admin API key and client API key for the VAs in the organization.



5. Click **Reset**.

Manage DNS Forwarders

Describes Manage DNS Forwarders in Cisco Secure Access. Once deployed in your environment, you can view your Cisco Secure Access Virtual Appliances (VAs) in Cisco Secure Access.

Once deployed in your environment, you can view your Cisco Secure Access Virtual Appliances (VAs) in Cisco Secure Access. Navigate to **DNS Forwarders** in Secure Access and manage the settings for the VAs. On each VA, you can manage the Secure Access Site for the VA, reset the VA's password, and upgrade and delete a VA.

Procedure for Managing DNS Forwarders

Describes Procedure for Managing DNS Forwarders in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

View the properties of each deployed Virtual Appliance, sync configuration settings to the deployed VAs, and manage the Virtual Appliances.

- View the DNS Forwarders
- Sync the Configuration Settings to Deployed VAs
- Edit a Site
- Upgrade a Virtual Appliance

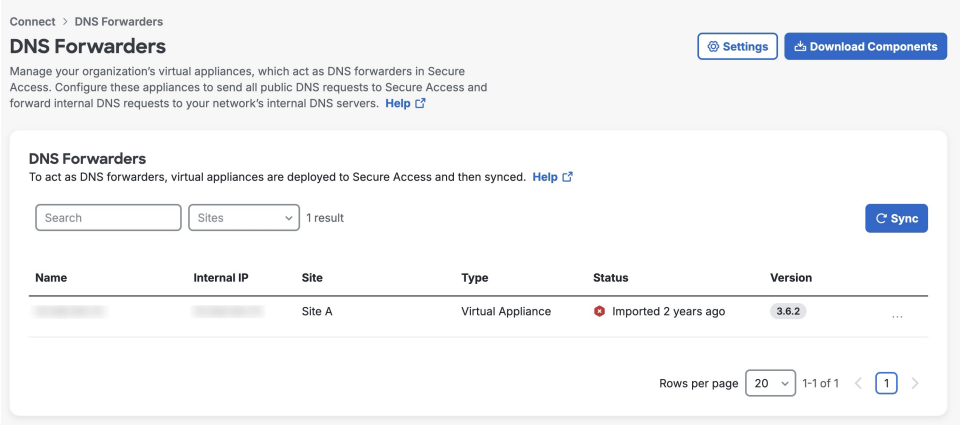
- Reset Password for Virtual Appliance
- Delete a Virtual Appliance

View the DNS Forwarders

Provides instructions for completing the View the DNS Forwarders workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. On **DNS Forwarders**, view the deployed Virtual Appliances. The VAs have several properties:
   - **Name**–The descriptive name of the VA.
   - **Internal IP**–The internal IP address of the VA.
   - **Site**–The name of the Site associated with the VA.
   - **Type**–The type of the DNS Forwarder, for example: Virtual Appliance.
   - **Status**–The status of the VA.
   - **Version**–The version of the deployed software image on the VA.



Sync the Configuration Settings to Deployed VAs

Provides instructions for completing the Sync the Configuration Settings to Deployed VAs workflow in Cisco Secure Access. Secure Access refreshes the latest configuration settings for the deployed Virtual Appliances.

Secure Access refreshes the latest configuration settings for the deployed Virtual Appliances.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. On **DNS Forwarders**, click **Sync**.

Edit a Site

Describes Edit a Site in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- For more information, see Manage Site for Virtual Appliance.

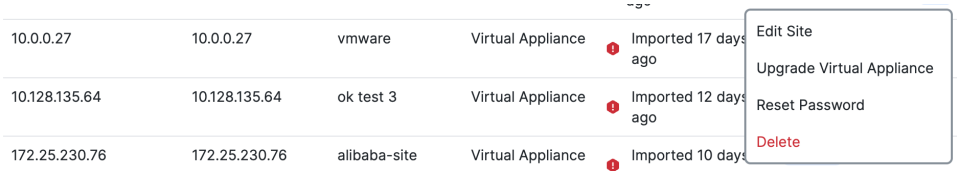
Upgrade a Virtual Appliance

Provides instructions for completing the Upgrade a Virtual Appliance workflow in Cisco Secure Access. The update of a VA results in the loss of DNS service for the duration of the update.

The update of a VA results in the loss of DNS service for the duration of the update. We highly recommend that you perform updates during non-business hours, or preferably, deploy a second VA for this site to automate the process of updates without introducing VA downtime.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Navigate to a Virtual Appliance and click the ellipsis (**...**), and then click **Upgrade Virtual Appliance**.



3. For **Upgrade Virtual Appliance**, click **Upgrade**.

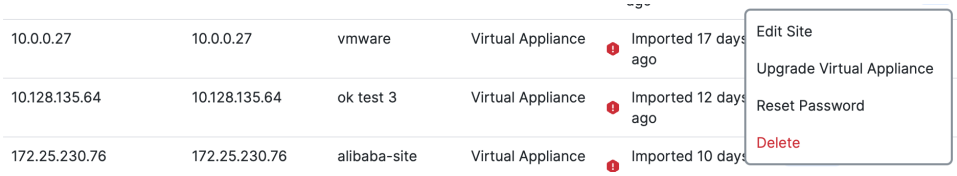
Reset Password

Provides instructions for completing the Reset Password workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

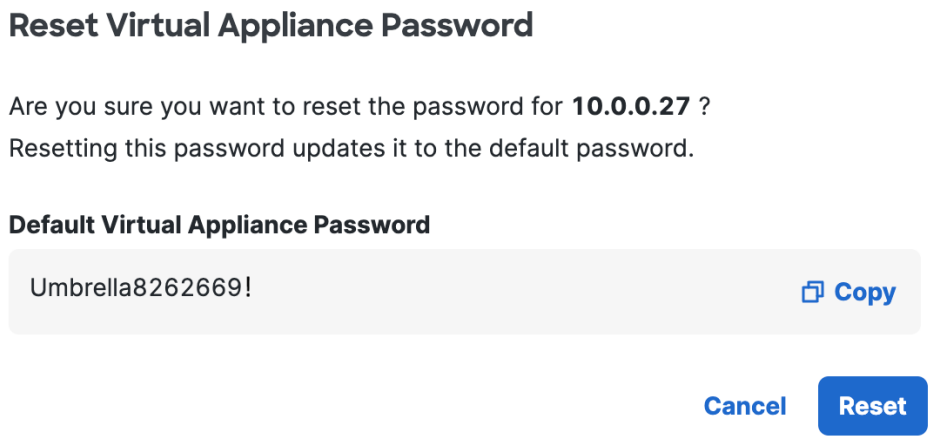
Reset a Virtual Appliance's password. The Virtual Appliance username is **vmadmin**.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance and click the ellipsis (**...**), and then select **Reset Password**.



3. For **Reset Virtual Appliance Password**, click. **Reset**, to generate a new password for the Virtual Appliance.



Note

It can take up to 15 minutes for the password to reset and sync with the deployed VAs.

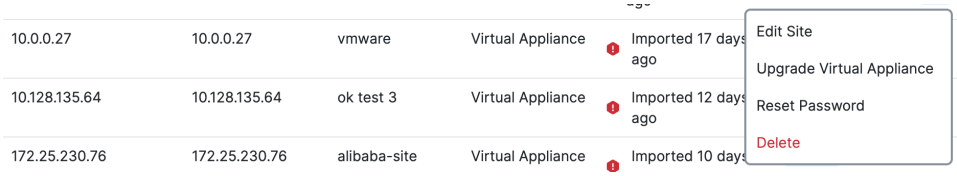
Delete a Virtual Appliance

Provides instructions for completing the Delete a Virtual Appliance workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

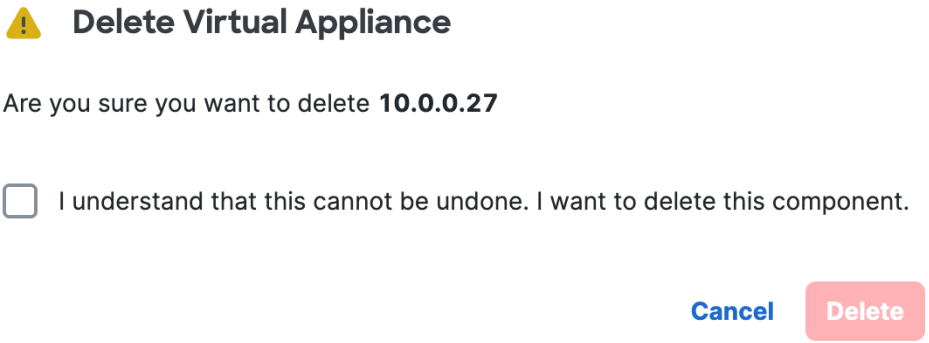
Remove the Virtual Appliance from the organization.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance and click the ellipsis (**...**), and then select **Delete**.



3. Check the box to confirm the deletion of the VA, and then click **Delete**.



Manage Site for Virtual Appliance

Describes Manage Site for Virtual Appliance in Cisco Secure Access. A Cisco Secure Access Virtual Appliance (VA) is associated with a Secure Access Site.

A Cisco Secure Access Virtual Appliance (VA) is associated with a Secure Access Site. You can add a new Site, select and rename a Site, or delete the Site for the VA. If you do not select a Site for the VA, Secure Access uses the default Site.

For information about managing Sites and Internal Networks, see Manage Sites and Manage Internal Networks.

Procedure for Managing Site for Virtual Appliance

Describes Procedure for Managing Site for Virtual Appliance in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Add a new site, select a site, rename a site, or delete a site for the VA.

- Add a Site
- Select a Site
- Rename a Site
- Delete a Site

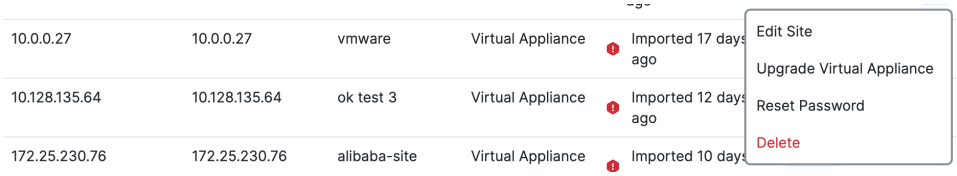
Add a Site

Provides instructions for completing the Add a Site workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add a Site for the VA.

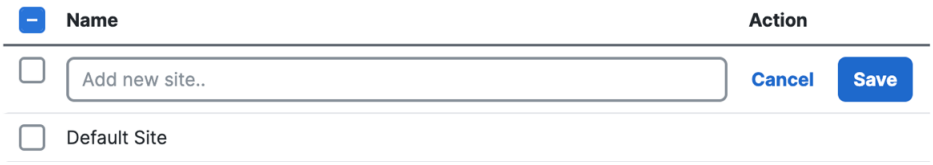
Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Click **+Add**, enter a descriptive name for the Site, and then click **Save**.

   After you add a Site, associate the Site with an Internal Network. For more information, see Manage Internal Networks.



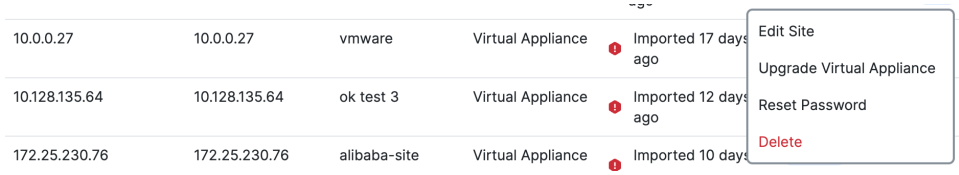
Select a Site

Provides instructions for completing the Select a Site workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

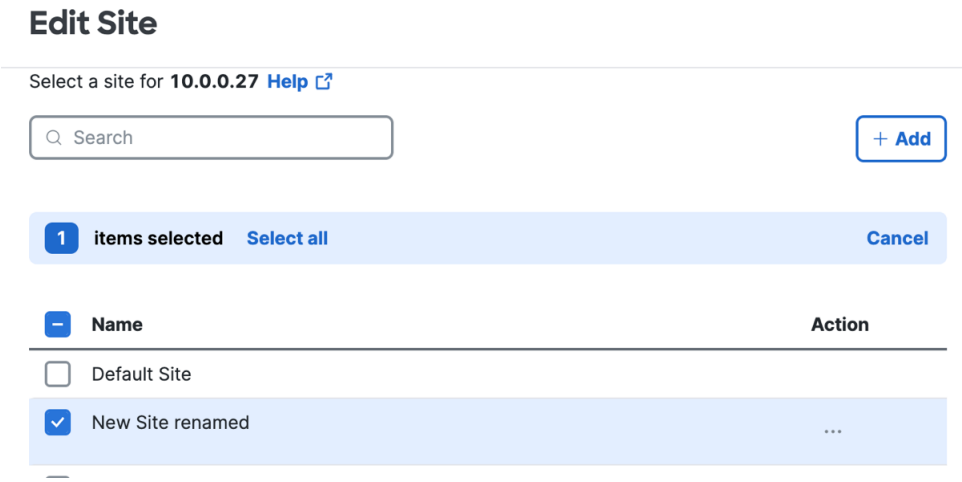
Select a Site for the VA.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Locate and select a Site for the VA, and then click **Save**.



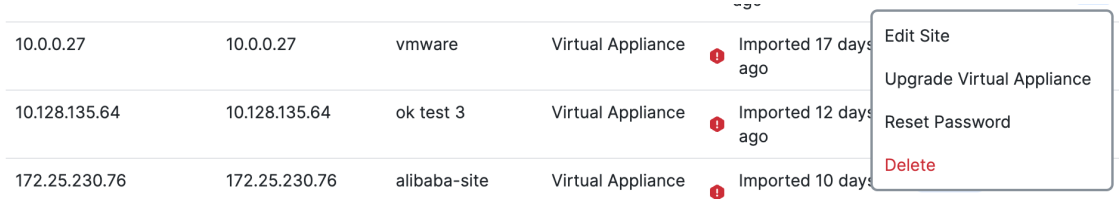
Rename a Site

Provides instructions for completing the Rename a Site workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

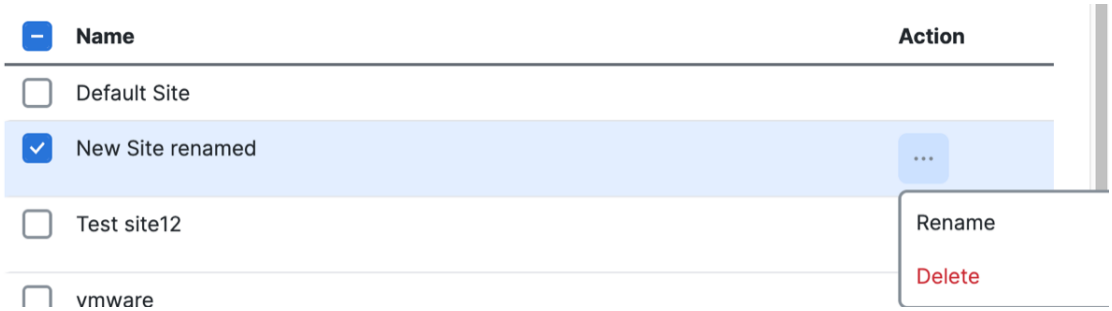
Edit the name of a Site.

Procedure

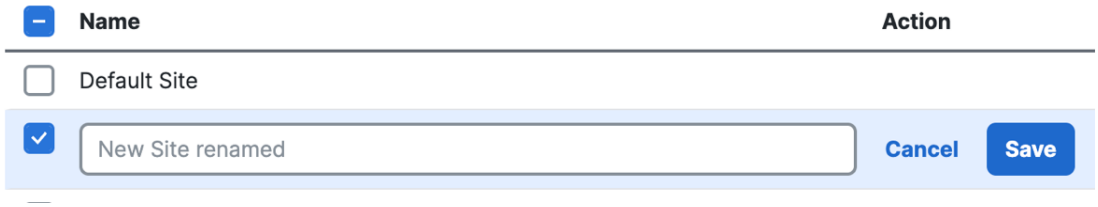
1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**



3. Locate the name of a Site, and then for **Action** click the ellipsis (**...**).



4. Click **Rename**, enter a descriptive name in the text area, and then click **Save**.



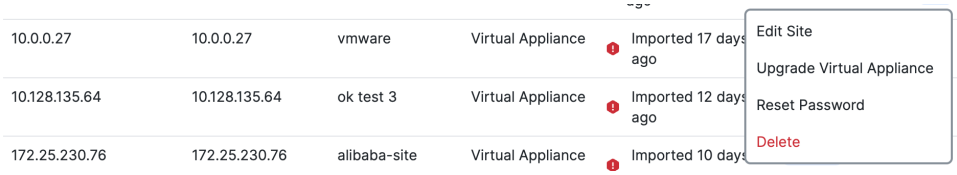
Delete a Site

Provides instructions for completing the Delete a Site workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

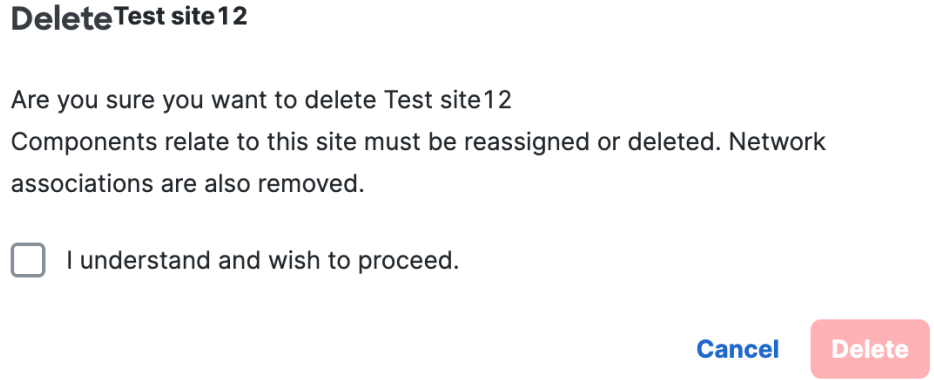
Delete a Site.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Locate a Virtual Appliance, click the ellipsis (**...**), and then select **Edit Site**.



3. Locate the name of a Site, and then for **Action** click the ellipsis (**...**).
4. Click **Delete**, check **I understand and wish to proceed**, and then click **Delete** to remove the Site.



Configure Updates for Virtual Appliances

Describes Configure Updates for Virtual Appliances in Cisco Secure Access. Cisco Secure Access Virtual Appliances (VAs) can receive automatic software updates.

Cisco Secure Access Virtual Appliances (VAs) can receive automatic software updates. New software versions for the Virtual Appliances become available and are usually applied without any intervention required.

How Secure Access Updates Your Virtual Appliance

Provides instructions for completing the How Secure Access Updates Your Virtual Appliance workflow in Cisco Secure Access. You can configure updates for the VAs in your organization.

You can configure updates for the VAs in your organization. Secure Access makes API requests from each VA and pushes out software updates. If you wish to update a specific VA first, do this manually. For more information, see Manually Configure Update of a Virtual Appliance.

Logic is built-in to our API to prevent two VAs at a single site from updating at once or updating when one of the VAs is in an error state. The following checks are performed:

Procedure

1. The API checks if there is only a single VA for the site. If there is only one VA, the API does not offer a command to auto-update.
2. If there is a secondary VA for the site but it is in an error state, then the first VA will not auto-update.
3. The API checks to see if a second VA for that site is already updating and if it is in a mid-update state it will not auto-update during that window of time. If we have ordered a VA to update and have not heard back that it has completed, this qualifies as a mid-update state.
4. If all the prerequisite checks have been met, the VA is updated.

Procedure for Configuring Updates for Virtual Appliances

Describes Procedure for Configuring Updates for Virtual Appliances in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For more information, see Networking Requirements.
- Configure Automatic Updates of Virtual Appliances
- Manually Configure Update of a Virtual Appliance
- Postpone Updates to Virtual Appliances

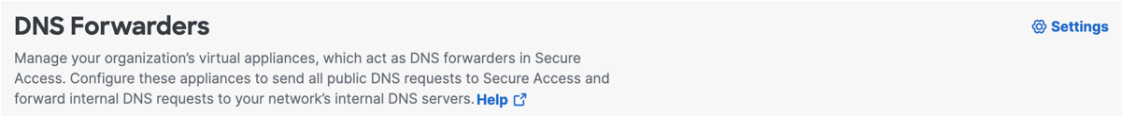
Configure Automatic Updates of Virtual Appliances

Provides instructions for completing the Configure Automatic Updates of Virtual Appliances workflow in Cisco Secure Access. Set up automatic updates to your deployed Virtual Appliances.

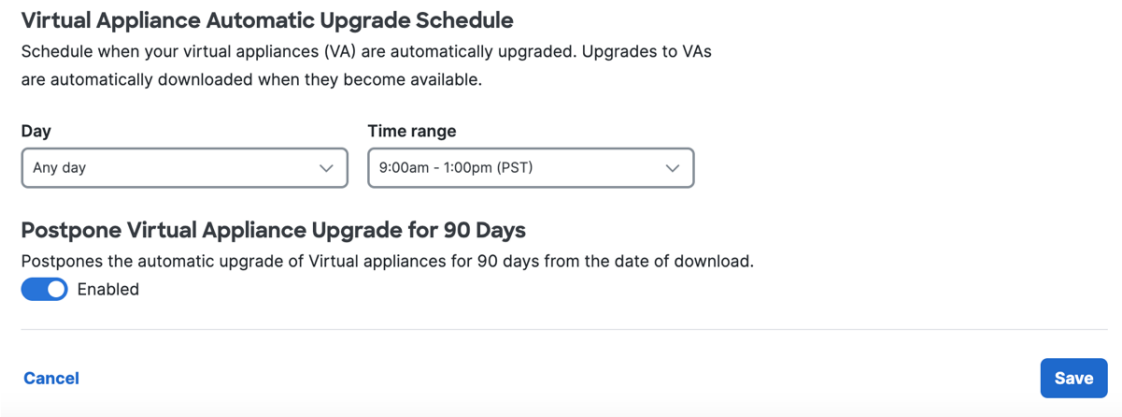
Set up automatic updates to your deployed Virtual Appliances.

Procedure

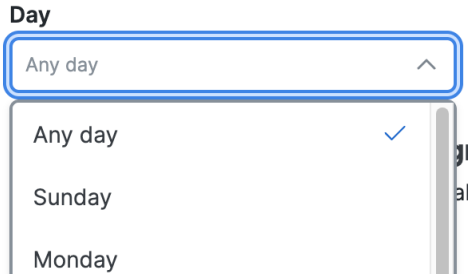
1. Navigate to **Connect** > **DNS Forwarders** > **Settings**.



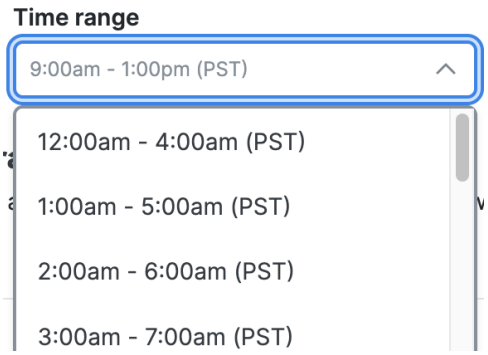
2. For **Virtual Appliance Automatic Upgrade Schedule**, choose the **Day** and **Time range** for the automatic software updates.



   a. For **Day**, select **Any day** or a day of the week.



   b. For **Time range**, select one of the available times.



3. Click **Save**.

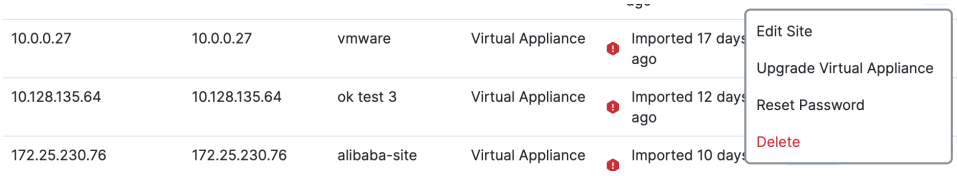
Manually Configure Update of a Virtual Appliance

Provides instructions for completing the Manually Configure Update of a Virtual Appliance workflow in Cisco Secure Access. The update of a VA results in the loss of DNS service for the duration of the update.

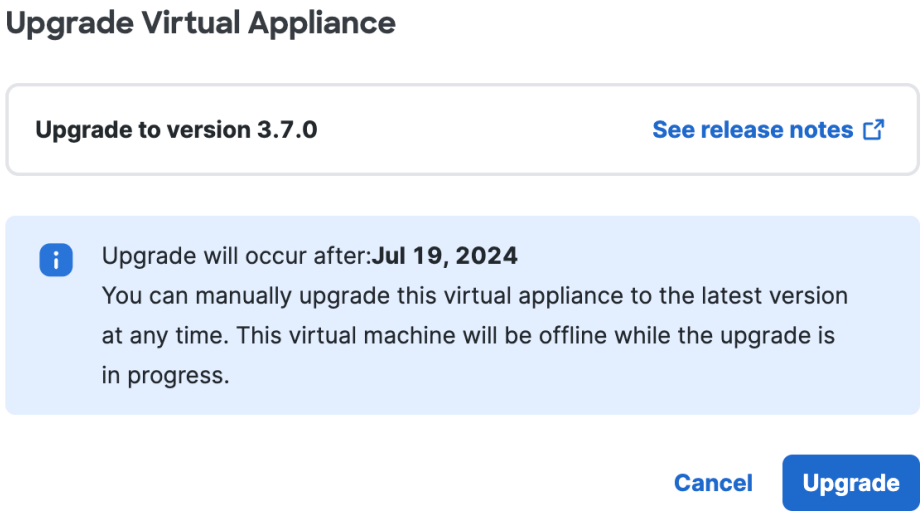
The update of a VA results in the loss of DNS service for the duration of the update. We highly recommend that you perform updates during non-business hours, or preferably, deploy a second VA for this site to automate the process of updates without introducing VA downtime.

Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Navigate to a Virtual Appliance and click the ellipsis (**...**), and then click **Upgrade Virtual Appliance**.



3. For **Upgrade Virtual Appliance**, click **Upgrade**.



Postpone Updates to Virtual Appliances

Provides instructions for completing the Postpone Updates to Virtual Appliances workflow in Cisco Secure Access. You can postpone the upgrade of the software on the Secure Access Virtual Appliances in your environment.

You can postpone the upgrade of the software on the Secure Access Virtual Appliances in your environment. Configure the delay of the upgrade for 90 days since the latest software update was made available.

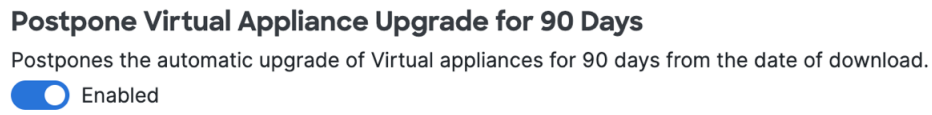
After 90 days, Secure Access upgrades the software on your Virtual Appliances according to the schedule that you configured.

> **Note**
>
> The software update delay applies to major releases only, and not for patch releases.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** > **Settings**.

2. For **Postpone Virtual Appliance Automatic Upgrade for 90 Days**, select **Enabled**.



Configure Failover to Third-Party Resolvers

Describes Configure Failover to Third-Party Resolvers in Cisco Secure Access. Configuring failover in Cisco Secure Access Virtual Appliance (VA) version 3.8.4 and later, allows administrators to specify public IPv4 DNS resolver IP addresses as fallback options.

Configuring failover in Cisco Secure Access Virtual Appliance (VA) version 3.8.4 and later, allows administrators to specify public IPv4 DNS resolver IP addresses as fallback options. When this feature is enabled, the VA routes DNS queries according to a defined order during failover: initially to the configured Cisco resolvers, then to the Cisco global resolver, and, if those are unreachable, to the administrator-specified third-party public IPv4 resolvers.

This capability allows organizations to:

- Maintain uninterrupted DNS resolution for users and applications during Cisco resolver outages.
- Customize DNS failover behavior by selecting up to five public IPv4 DNS resolvers that best meet organizational requirements.

Configuration and management of this feature are performed through the Secure Access dashboard. Only IPv4 addresses are supported for custom fallback resolvers. The failover sequence and health monitoring are handled automatically by the VA, ensuring seamless DNS service continuity and simplified administration.

Recovery and Switchback

The Virtual Appliance periodically checks the connectivity status of the configured Cisco resolvers. When connectivity is restored, the VA automatically switches DNS queries back to the Cisco resolvers. The recovery process typically takes two to three minutes and requires no manual intervention.

Key Considerations

- **IPv4 Support Only:** Only IPv4 addresses are supported for custom public DNS resolvers.
- **Configuration Requirement:** Failover functions only when the VA is configured with at least one Cisco IPv4 resolver.
- **Failover Latency:** The transition from a Cisco resolver to a third-party resolver takes approximately three minutes. DNS resolution will be temporarily unavailable during this period.
- **Failover Sequence:** The VA resolves DNS queries in the following order:
  1. Configured Cisco resolver
  2. Cisco global IPv4 resolver
  3. First available custom IP address (third-party resolver)

Enable Third-Party Resolver Failover

Provides instructions for completing the Enable Third-Party Resolver Failover workflow in Cisco Secure Access. Ensure you are running VA version 3.8.4 or later.

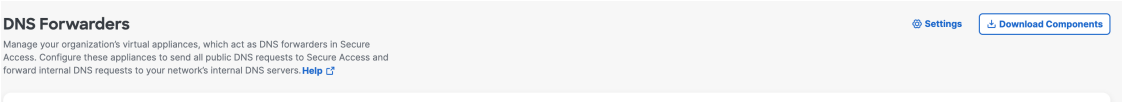
Enabling third-party resolver failover allows administrators to specify public IPv4 DNS resolver addresses as fallback options in the Secure Access dashboard. When enabled, the VA automatically routes DNS queries to these configured resolvers if Cisco DNS services become unavailable, helping to maintain continuous DNS resolution for connected clients.

Before you begin

- Ensure you are running VA version 3.8.4 or later.
- At least one Cisco IPv4 resolver must be configured.
- Administrator privileges are required to modify DNS Forwarder settings.

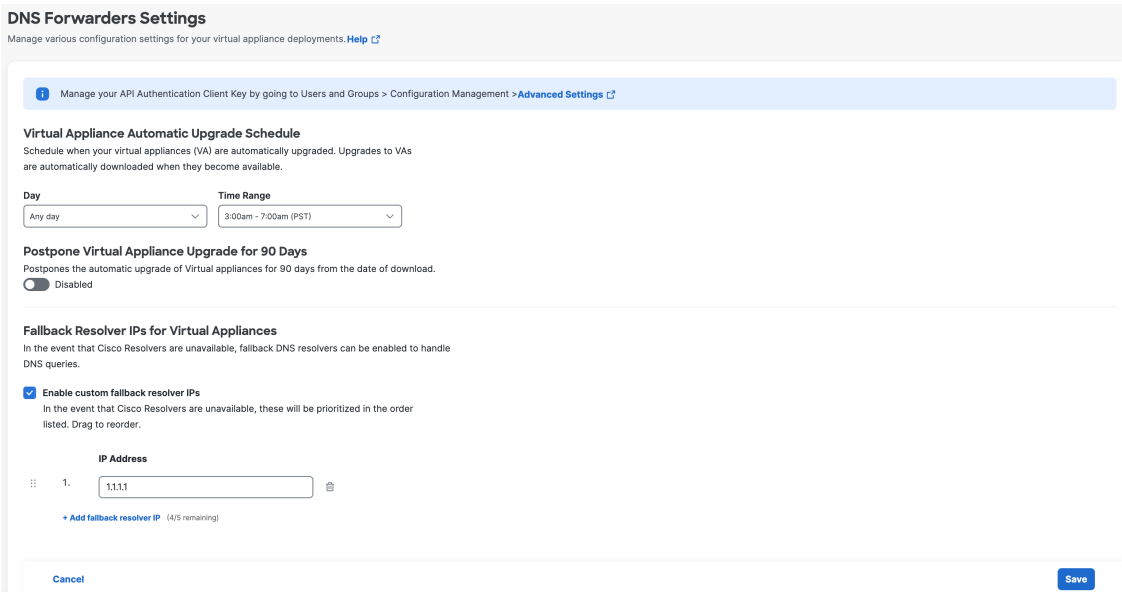
Procedure

1. Navigate to **Connect** > **DNS Forwarders**.
2. Click **Settings**.



   The **DNS Forwarders Settings** page is displayed.

3. In the **Fallback Resolver IPs for Virtual Appliances** area, check the **Enable Custom fallback resolver IPs** checkbox.



4. Enter the IPv4 address of the non-Cisco public fallback DNS resolver in the field.

   Click **Add fallback resolver IP** to add additional IPV4 addresses. You can add up to five custom public IPv4 resolver addresses as fallback options.

> **Note**
>
> Only IPv4 addresses are supported for custom fallback DNS resolvers.

5. Click **Save**.

Verify the Current Resolver on the Virtual Appliance

Describes Verify the Current Resolver on the Virtual Appliance in Cisco Secure Access. To determine which resolver is currently handling DNS queries: Access the VA through the VMware console or SSH.

To determine which resolver is currently handling DNS queries:

1. Access the VA through the VMware console or SSH.
2. Run the **config va status** command. Alternately, run the **config va show** command.
3. Review the **Current Resolver** section in the command output to identify the active nameserver.

   You identify whether the Cisco Umbrella DNS resolver or a third-party fallback resolver is currently active.

Sample command output for Umbrella DNS resolver

The following screenshots show the output of the **config va status** and **config va show** commands, demonstrating how the Virtual Appliance displays the active resolver when an Umbrella DNS resolver is being used.

```
10.128.135.75 ~ $ config va status
thisdnsv4 : This DNS Server : DNS ok (green)
        UDP lookup of myip.opendns.com @ 127.0.0.1,53 ok : 127.0.0.1
        TCP connection to 127.0.0.1,53 ok : 127.0.0.1
localdns : Local DNS Servers : Unconfigured (yellow)
dns : Umbrella DNS Servers : All DNS ok (green)
        UDP lookup of 208.67.220.220 @ 208.67.220.220,443 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver2.opendns.com.
        TCP connection to 208.67.220.220,443 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver2.opendns.com.
        UDP lookup of 208.67.222.222 @ 208.67.222.222,443 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver1.opendns.com.
        TCP connection to 208.67.222.222,443 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver1.opendns.com.
dnscrypt : DNScrypt Encryption : All DNScrypt ok (green)
        Resolver 208.67.220.220 DNSCrypt : Enabled at port 443
        Resolver 208.67.222.222 DNSCrypt : Enabled at port 443
        Authorities port : 443, Enabled : 1
ad : AD Connector : Unknown (white)
cloud : Umbrella Cloud : SSL ok (green)
        Subject Name: C=US; ST=California; L=San Jose; O=CISCO SYSTEMS, INC.; CN=api.opendns.com
        Issuer name: C=US; O=DigiCert Inc; CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
updates : Updates : SSL GET ok (green)
        SSL Get from https://disthost.umbrella.com:443/enterprise/upgrade/va/internal/MANIFEST : 13355 bytes
ssh : Support Tunnel : Disabled (white)
current_resolver : Umbrella DNS Server : All DNS ok (green)
        UDP lookup of 208.67.220.220 @ 208.67.220.220,53 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver2.opendns.com.
        TCP connection to 208.67.220.220,53 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver2.opendns.com.
        UDP lookup of 208.67.222.222 @ 208.67.222.222,53 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver1.opendns.com.
        TCP connection to 208.67.222.222,53 ok : dns.sse.cisco.com., dns.opendns.com., dns.umbrella.com., resolver1.opendns.com.
10.128.135.75 ~ $
```

```
10.128.135.75 ~ $ config va show
            Virtual Appliance Configuration

                Name:  10.128.135.75

                Local DNS -
                    ip address :
                    DNSSEC     : disabled

                Internal Domains Count: 4

                Resolvers: 208.67.220.220 208.67.222.222

                SSH access : enabled

                HTTPS status : disabled

                SSL Certificate Start Time : NA

                SSL Certificate Expiry Time : NA

                Issuer : NA

                Common Names : NA

                Subject Alternative Name : NA

                Per-IP based Rate Limiting  : Disabled

                Primary Adapter   : ens160
                    MAC Adress    : 00:50:56:96:3e:5d
                    IP Address    : 10.128.135.75
                    Netmask       : 255.255.255.0
                    Gateway       : 10.128.135.1
                    IPv6 Address  :
                    IPv6 Gateway  : fe80::2fc:baff:fe63:bb37

                Current Resolver  : 208.67.220.220 208.67.222.222

10.128.135.75 ~ $
```

Sample command output for third-party resolver

The following screenshots show the output of the **config va status** and **config va show** commands, demonstrating how the Virtual Appliance displays the active resolver when a third-party fallback DNS resolver is in use.

```
10.128.135.75 ~ $ config va status
thisdnsv4 : This DNS Server : DNS ok (green)
        UDP lookup of myip.opendns.com @ 127.0.0.1,53 ok : 127.0.0.1
        TCP connection to 127.0.0.1,53 ok : 127.0.0.1
localdns : Local DNS Servers : Unconfigured (yellow)
dns : Umbrella DNS Servers : All DNS fail (red)
        UDP lookup of 208.67.220.220 @ 208.67.220.220,53 fails : Error : ;; communications error to 208.67.220.220#53: timed out
        TCP connection to 208.67.220.220,53 fails : Error : ;; Connection to 208.67.220.220#53(208.67.220.220) for 220.220.67.208.in-addr.arpa. failed: timed out.
        UDP lookup of 208.67.222.222 @ 208.67.222.222,53 fails : Error : ;; communications error to 208.67.222.222#53: timed out
        TCP connection to 208.67.222.222,53 fails : Error : ;; Connection to 208.67.222.222#53(208.67.222.222) for 222.222.67.208.in-addr.arpa. failed: timed out.
dnscrypt : DNScrypt Encryption : All DNScrypt fail (red)
        Resolver 208.67.220.220 DNSCrypt : Disabled
        Resolver 208.67.222.222 DNSCrypt : Disabled
        Authorities port : 53, Enabled : 0
ad : AD Connector : Unknown (white)
cloud : Umbrella Cloud : SSL ok (green)
        Subject Name: C=US; ST=California; L=San Jose; O=CISCO SYSTEMS, INC.; CN=api.opendns.com
        Issuer name: C=US; O=DigiCert Inc; CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
updates : Updates : SSL GET ok (green)
        SSL Get from https://disthost.umbrella.com:443/enterprise/upgrade/va/internal/MANIFEST : 13355 bytes
ssh : Support Tunnel : Disabled (white)
current_resolver : 3rd Party Resolver (1.1.1.1) : DNS ok (green)
        UDP lookup of 1.1.1.1 @ 1.1.1.1,53 ok : one.one.one.one.
        TCP connection to 1.1.1.1,53 ok : one.one.one.one.
10.128.135.75 ~ $
```

```
10.128.135.75 ~ $ config va show
            Virtual Appliance Configuration

                Name:  10.128.135.75

                Local DNS -
                    ip address :
                    DNSSEC     : disabled

                Internal Domains Count: 4

                Resolvers: 208.67.220.220 208.67.222.222

                SSH access : enabled

                HTTPS status : disabled

                SSL Certificate Start Time : NA

                SSL Certificate Expiry Time : NA

                Issuer : NA

                Common Names : NA

                Subject Alternative Name : NA

                Per-IP based Rate Limiting  : Disabled

                Primary Adapter   : ens160
                    MAC Adress    : 00:50:56:96:3e:5d
                    IP Address    : 10.128.135.75
                    Netmask       : 255.255.255.0
                    Gateway       : 10.128.135.1
                    IPv6 Address  :
                    IPv6 Gateway  : fe80::2fc:baff:fe63:bb37

                Current Resolver  : 1.1.1.1
```

Deploy Virtual Appliances

Describes Deploy Virtual Appliances in Cisco Secure Access. Secure Access requires that you deploy two Virtual Appliances (VAs) for a given site.

Secure Access requires that you deploy two Virtual Appliances (VAs) for a given site. It is critical that these VAs are not cloned or copied in any way.

Guidelines

- Set up and configure your virtual appliances manually. Do not copy or clone your virtual appliances.

  Cloning your virtual appliances may disrupt syncs with Secure Access if you have to restore the VAs.

- VAs do not cache any data that would require backing up. Deploy two VAs on a site in order to avoid downtime if one of the VAs is not available.
- You should understand how to deploy a virtual machine in your environments.

Deploy the Secure Access Virtual Appliances

Choose a deployment procedure based on your OS and software:

- Deploy VAs in Hyper-V for Windows 2012 or Higher
- Deploy VAs in VMware
- Deploy VAs in Microsoft Azure
- Deploy VAs in Amazon Web Services
- Deploy VAs in Google Cloud Platform
- Deploy VAs in KVM
- Deploy VAs in Nutanix
- Deploy VAs in Alibaba Cloud

Deploy VAs in Hyper-V for Windows 2012 or Higher

Describes Deploy VAs in Hyper-V for Windows 2012 or Higher in Cisco Secure Access. Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.

Deploy Cisco Secure Access Virtual Appliances in Microsoft Hyper-V for Windows Server 2012 or higher.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- One of the following Windows Server operating systems:
  - Windows Server 2012, SP1, or R2 (Standard or Datacenter), 2016 or 2019 with Hyper-V role.
  - Hyper-V Server 2012, 2012 R2, 2016 or 2019.
- Basic knowledge of Hyper-V.

> **Note**
>
> Secure Access does not support Virtual Appliances that are deployed using System Center Virtual Machine Manager (SCVMM).

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure for Deploying VAs in Hyper-V for Windows 2012 or Higher

Describes Procedure for Deploying VAs in Hyper-V for Windows 2012 or Higher in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Step 1 – Download and Extract the Hyper-V Installer
- Step 2 – Import the Virtual Appliance
- Step 3 – Copy and Rename Image Files

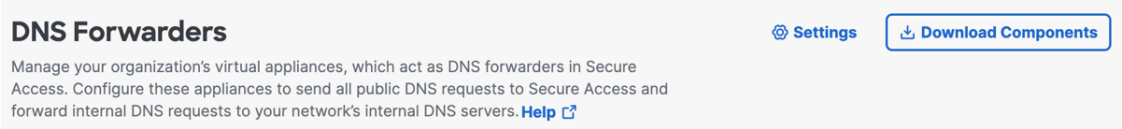
- Step 4 - Select Network Adapter
- Step 5 - Select Hard Drive
- Step 6 - Power on the Virtual Machine
- Step 7 - Repeat for the Second Virtual Appliance

Step 1 – Download and Extract the Hyper-V Installer

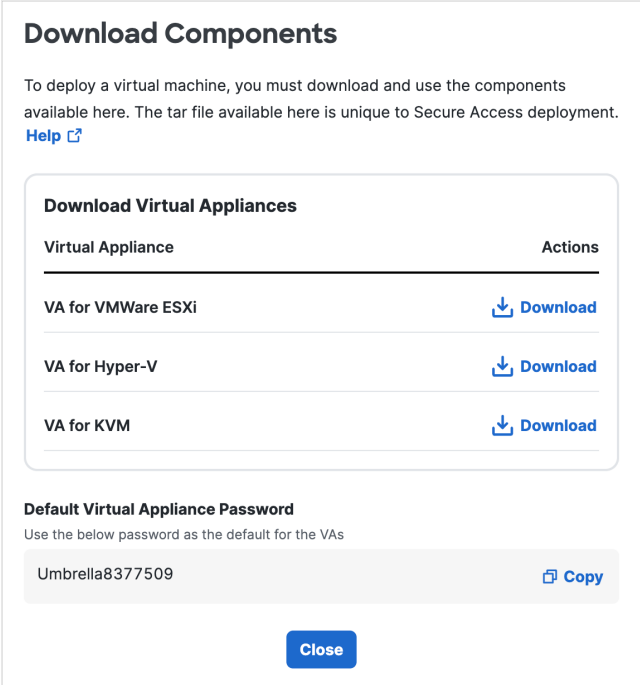
Provides instructions for completing the Step 1 - Download and Extract the Hyper-V Installer workflow in Cisco Secure Access. Navigate to Connect DNS Forwarders and click Download Components.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** next to **VA for Hyper-V**.



   Secure Access generates and downloads a tar file unique to your deployment.

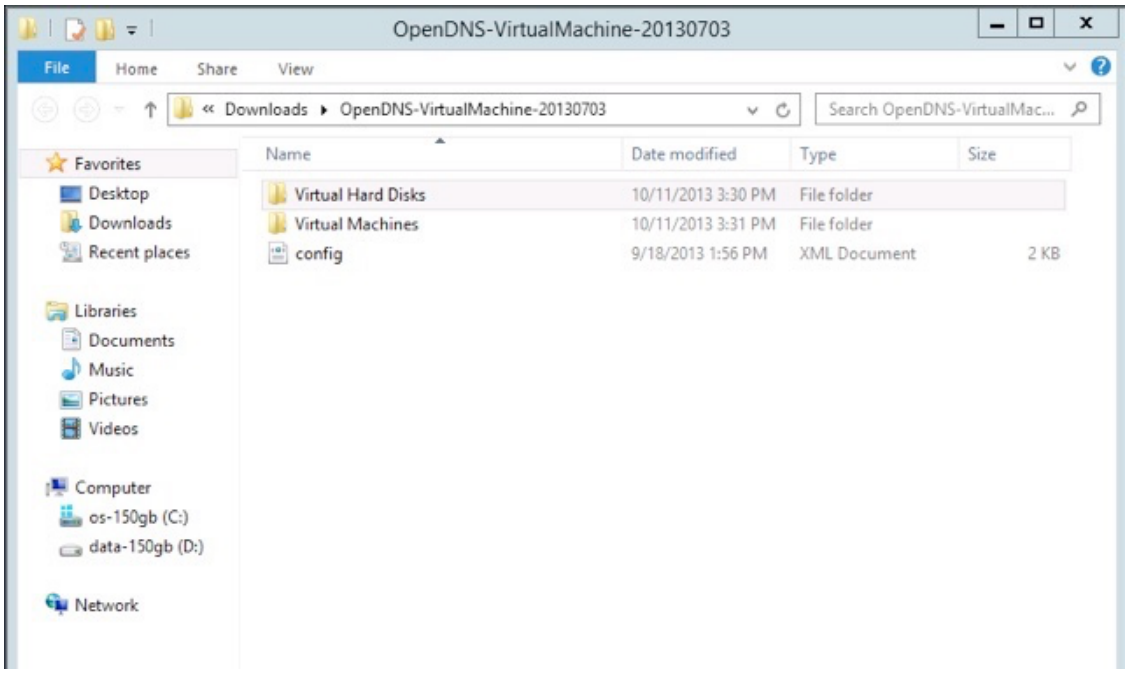
   This tar file includes:

   - a zip file containing the virtual hard disks that need to be deployed on Hyper-V
   - a signature file
   - a Cisco public certificate to validate the signature
   - a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. When successful, you will see a message saying “Verified OK."

4. Extract the .zip file. You'll find two folders–`Virtual Hard Disks` and `Virtual Machines`–and a `config` file.



Step 2 – Import the Virtual Appliance

Provides instructions for completing the Step 2 – Import the Virtual Appliance workflow in Cisco Secure Access. Microsoft has introduced a "Generation 2" style of VM profile on Hyper-V for Windows 2012 R2 and higher versions.

Tip

Using Windows 2012 R2 or Higher Versions

Microsoft has introduced a "Generation 2" style of VM profile on Hyper-V for Windows 2012 R2 and higher versions. As a result, the import steps below will fail with the error: "*Hyper-V did not find virtual machines to import from location [path]*"

You will need to create a new virtual machine as "Generation 1", then skip to 3. Copy and Rename Image Files.

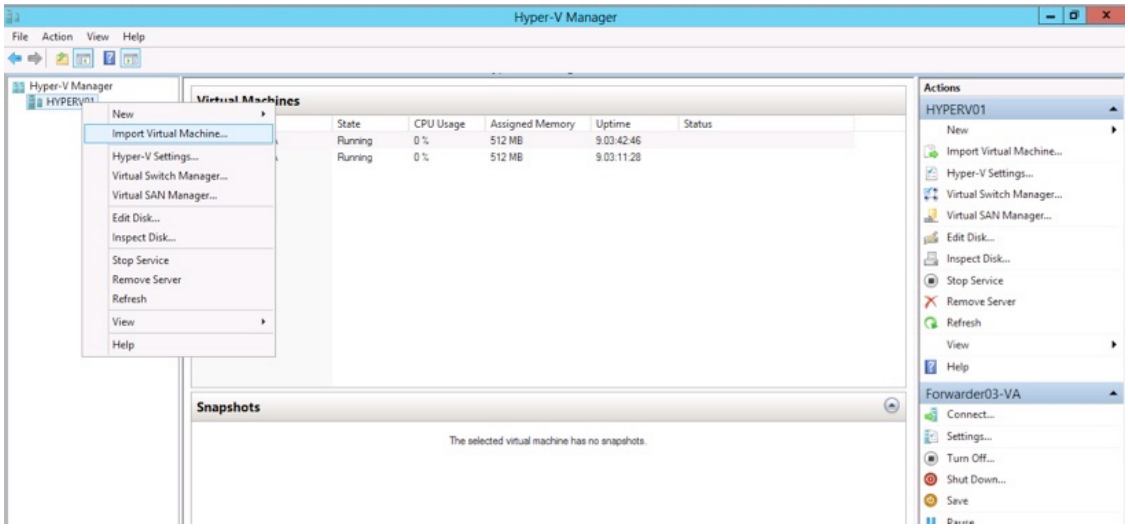
For more information about Generation 1 vs. Generation 2, see Generation 2 Virtual Machine Overview.

Note

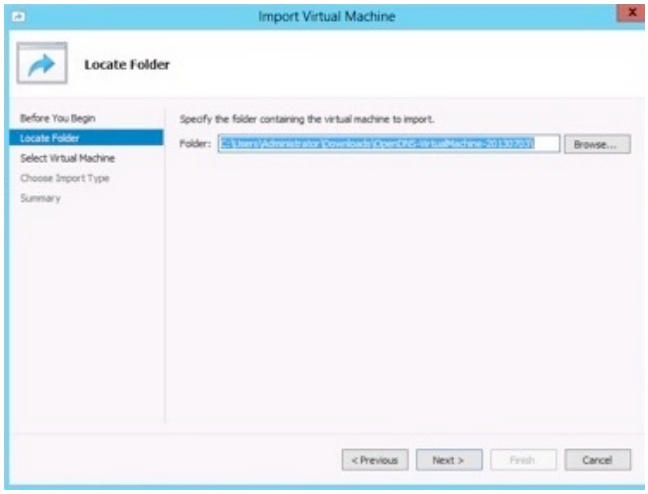
Step 2 in this procedure applies to **Windows 2012** only, and not **Windows 2012 *R2***.

Procedure

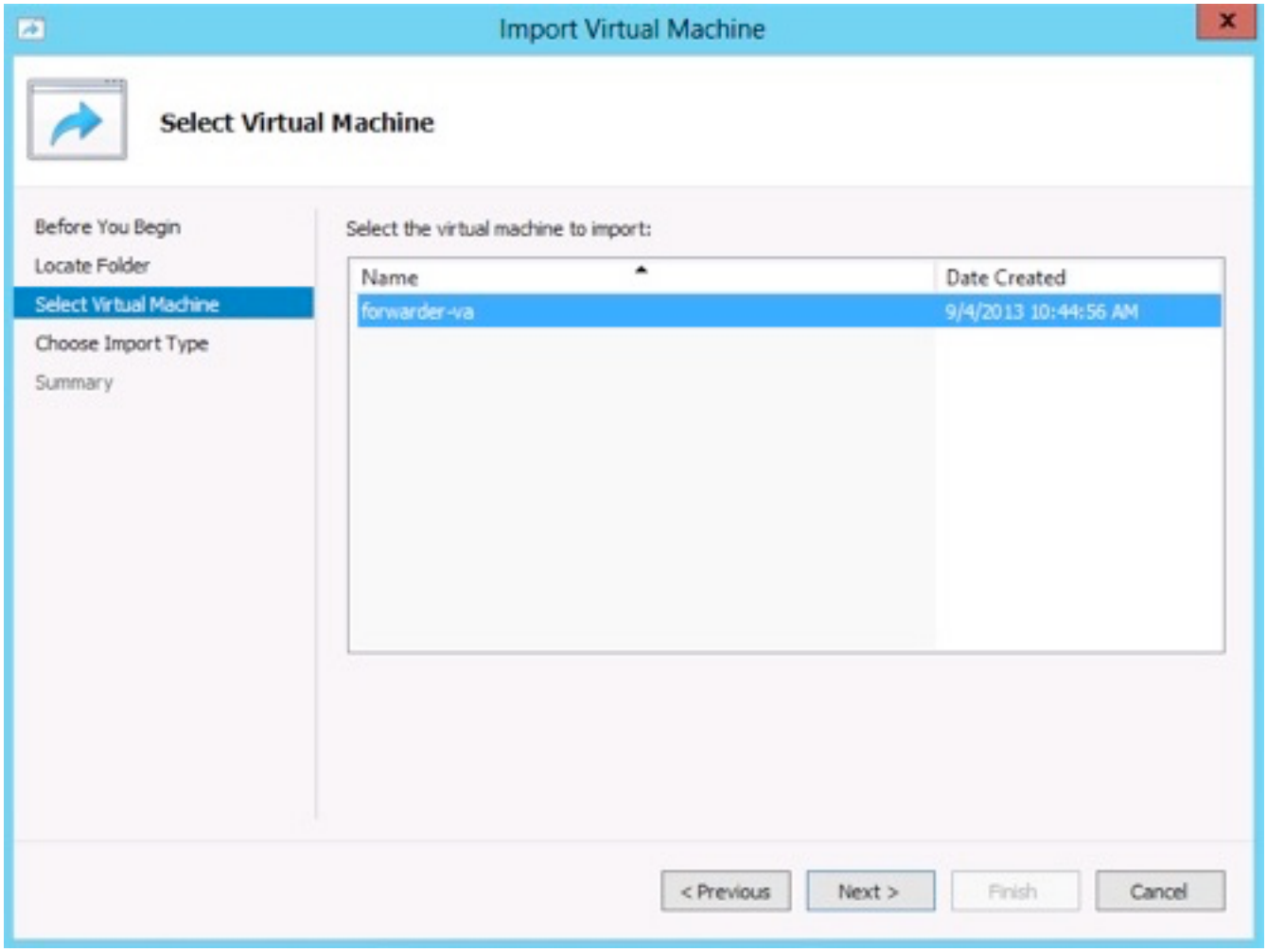
1. Select your Hyper-V server, right-click its name and select **Import Virtual Machine** from the menu.



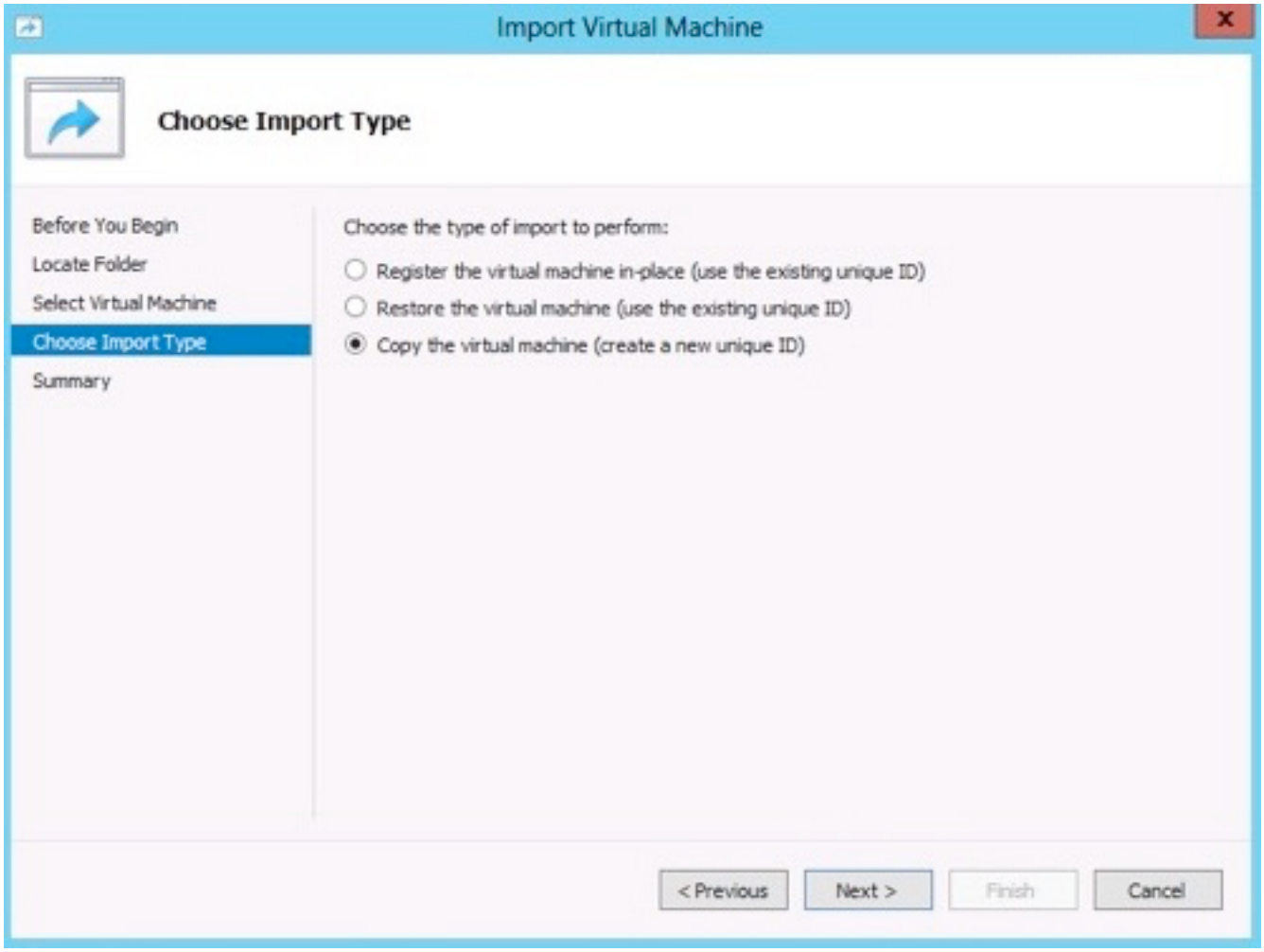
2. Navigate to the extraction folder from your download, select that folder to import, and then click **Next**.



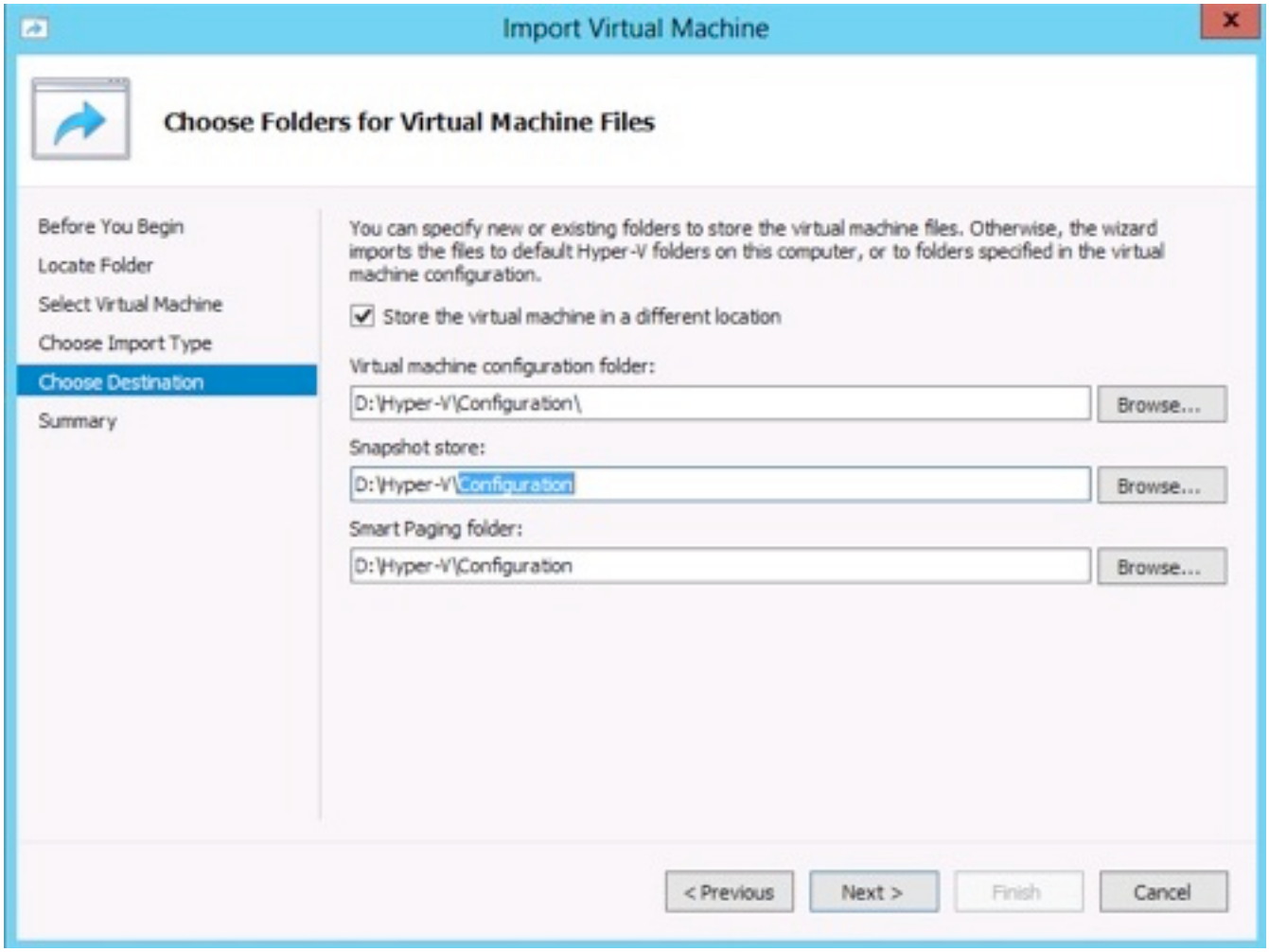
3. Select **forwarder-va** as the virtual machine to import and click **Next**.



4. Select **Copy the virtual machine (create a new unique ID)** and click **Next**.



5. Choose destination folders to install to. By default, these are the **Hyper-V Configuration** folders, but you can choose another folder.



Note

If selecting a different folder, pick a drive with sufficient space and create a folder with a specific name for the virtual machine, such as \opendnsforwarder-1. This can be helpful to ensure you're able to distinguish between the two virtual appliances in your file structure.

6. Click **Finish**.

Step 3 – Copy and Rename Image Files

Provides instructions for completing the Step 3 - Copy and Rename Image Files workflow in Cisco Secure Access. In Windows Explorer, navigate to the \Virtual Hard Disks subfolder within the extracted download folder created in Step 1.

Procedure

---

1. In Windows Explorer, navigate to the **\Virtual Hard Disks** subfolder within the extracted download folder created in **Step 1**.
2. Copy the two files from that location to the Virtual Machine Configuration Folder you specified in the previous step.

3. The two files, **dynamic** and **forwarder-va** must be renamed per the VA that is being installed. For example, rename:

   dynamic to **Dynamic-VA-1**

   and

   forwarder-va to **Forwarder-VA-1**

   If configuring your second VA, change the number accordingly. This can help ease the management of multiple virtual appliances and avoids conflicts between filenames when configuring your second VA.

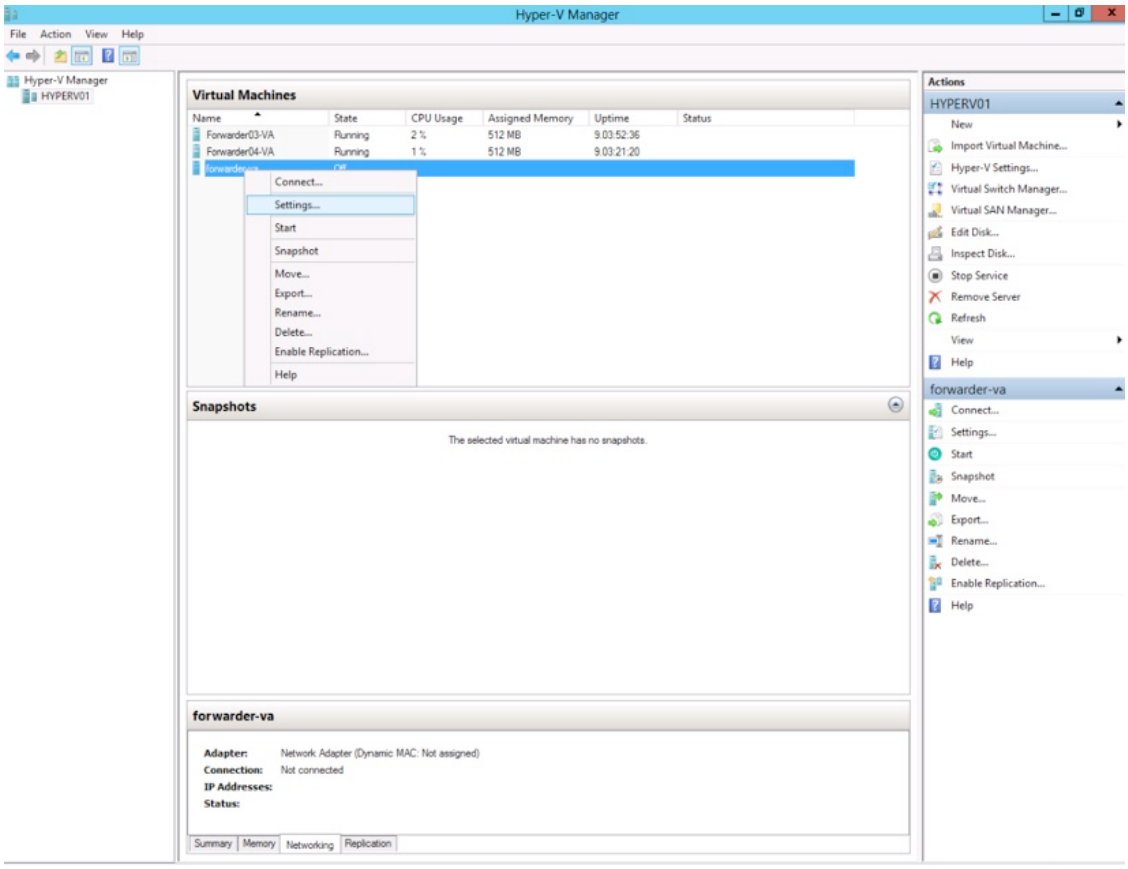
Step 4 – Select Network Adapter

Provides instructions for completing the Step 4 - Select Network Adapter workflow in Cisco Secure Access. In the Hyper-V Manager, select the virtual machine you've created, right-click and choose Settings.

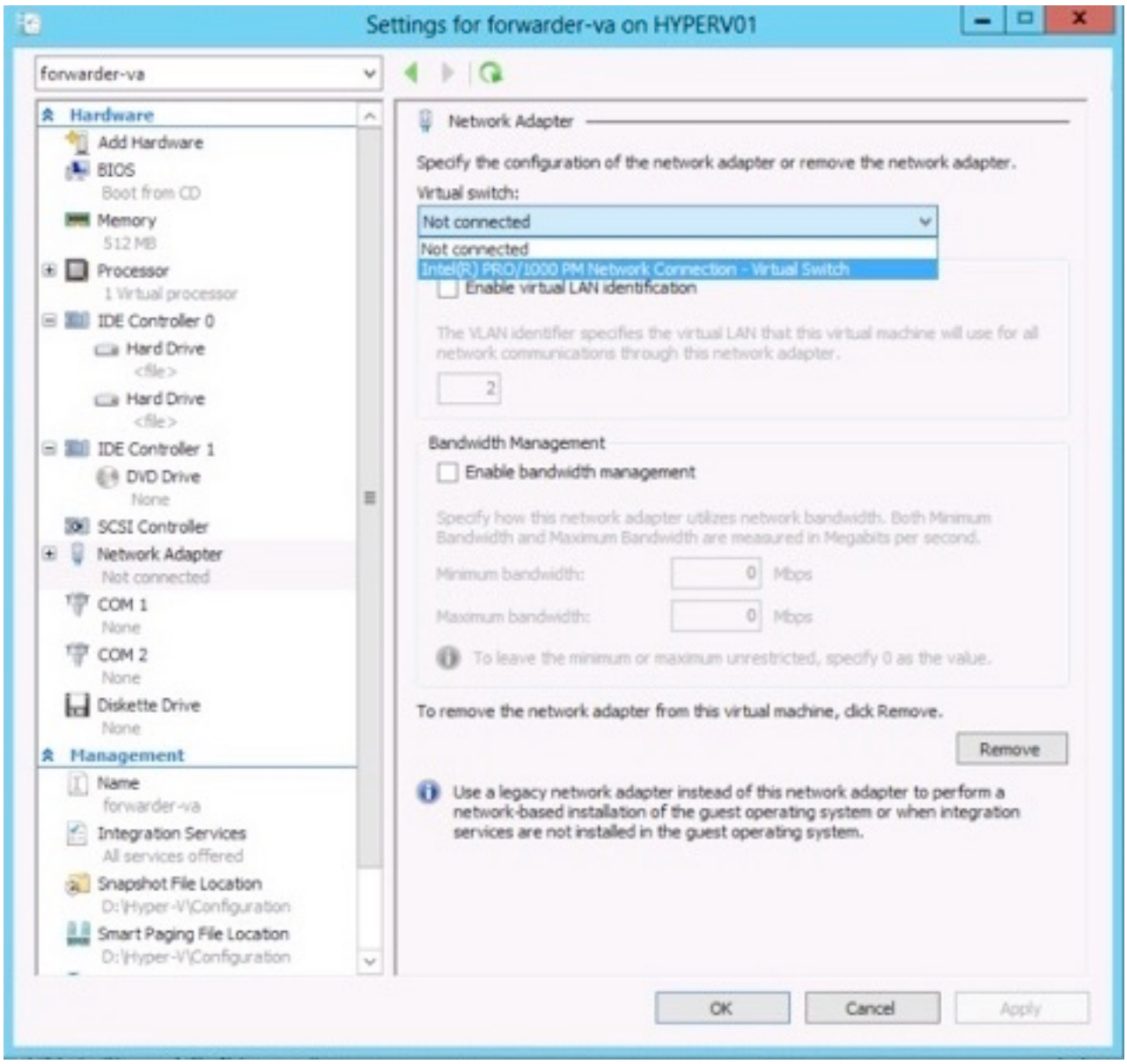
Procedure

---

1. In the Hyper-V Manager, select the virtual machine you've created, right-click and choose **Settings**.



2. Under **Hardware**, select **Network Adapter**, and then assign a virtual switch that has internet access.



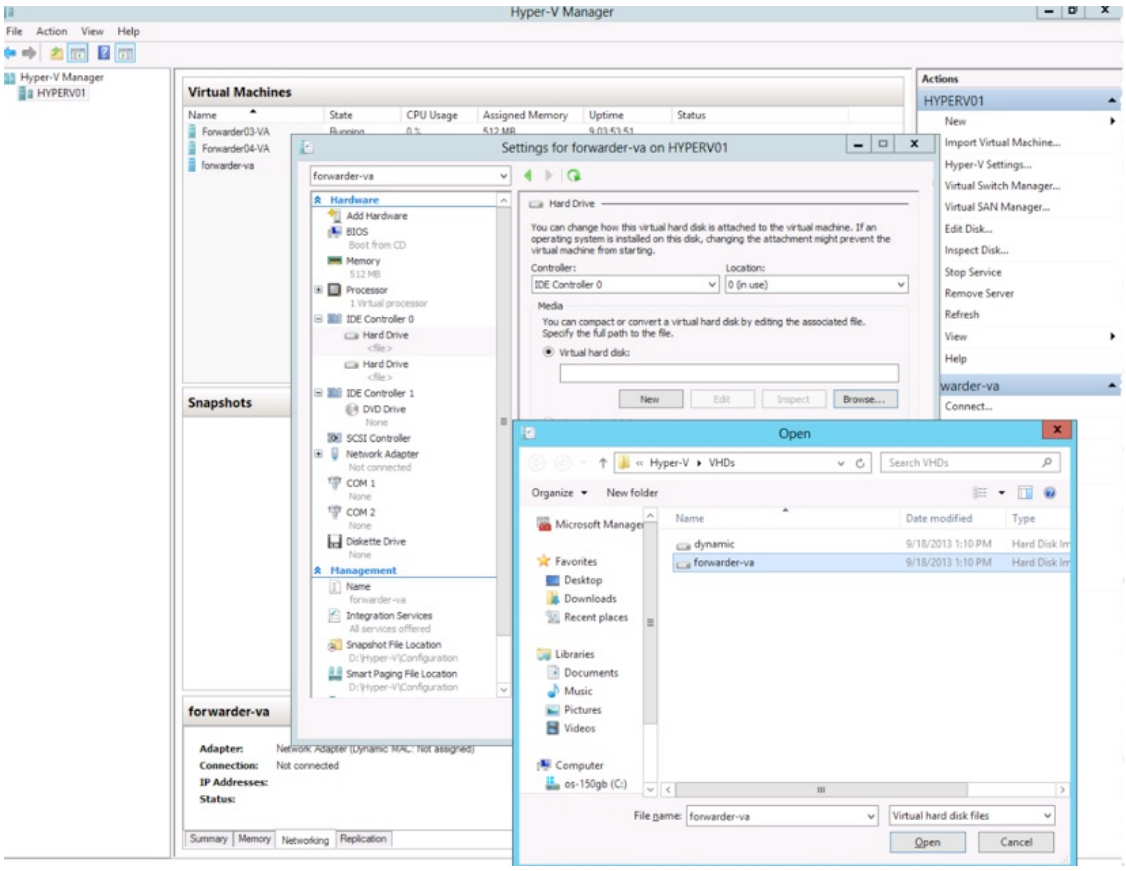
Step 5 – Select Hard Drive

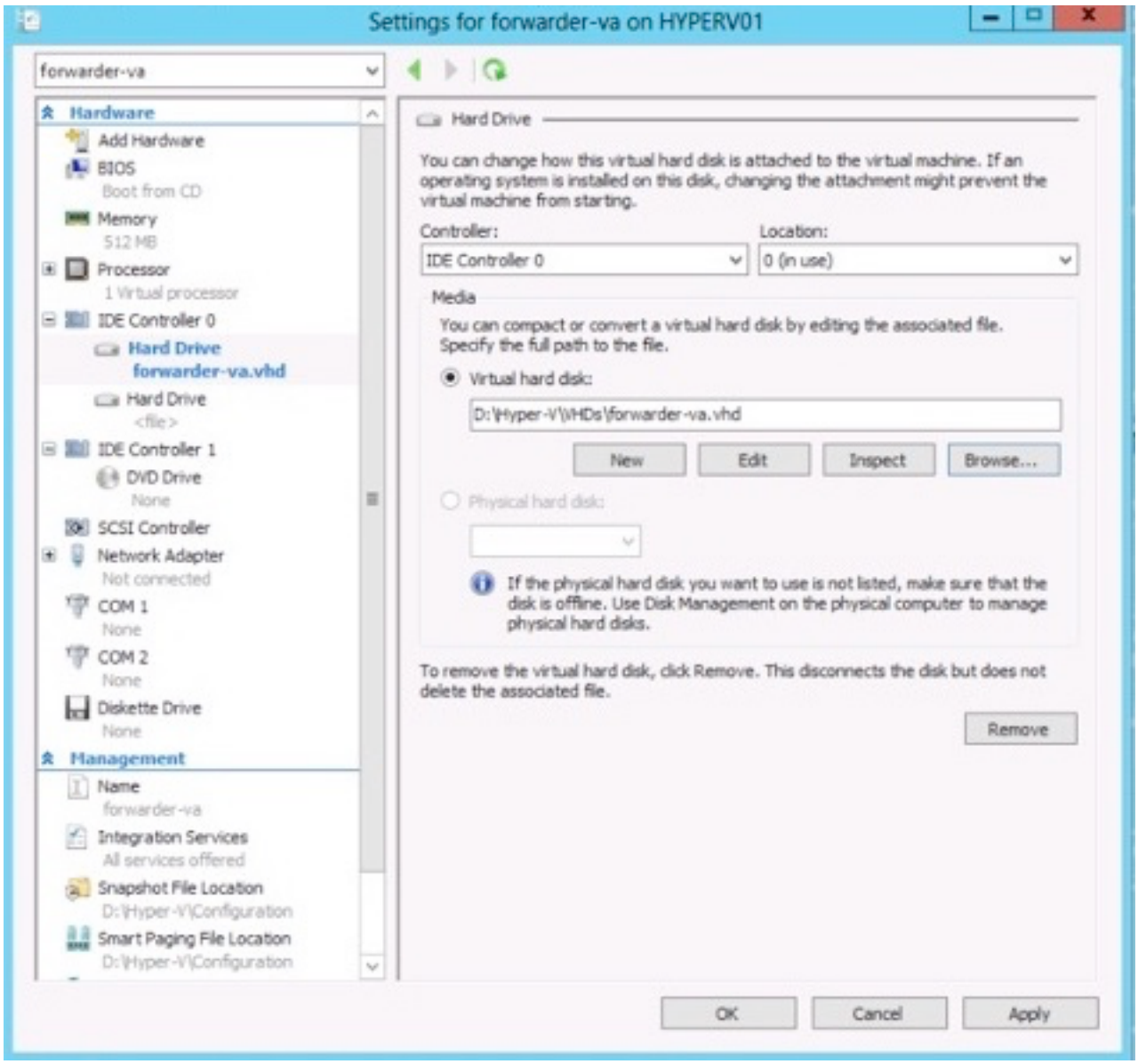
Provides instructions for completing the Step 5 – Select Hard Drive workflow in Cisco Secure Access. In Settings for Hardware, select the hard drives.

Procedure

1. In **Settings for Hardware**, select the hard drives.

   Ideally, they should be under the same IDE controller. For hard drive settings, browse to the Virtual Machine Configuration Folder and the first hard drive should be set to the forwarder file (Forwarder-va) and the second hard drive should be set to the dynamic (Dynamic) file.


Hyper-V Manager
File Action View Help
Hyper-V Manager
HYPERV01
Virtual Machines
Name State CPU Usage Assigned Memory Uptime Status
Forwarder03-VA
Forwarder04-VA
forwarder-va
Snapshots
forwarder-va
Adapter:
Connection: Not connected
IP Addresses:
Status:
Summary Memory Networking Replication
Settings for forwarder-va on HYPERV01
forwarder-va
Hardware
Add Hardware
BIOS
Boot from CD
Memory
512 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Hard Drive
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Not connected
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
forwarder-va
Integration Services
All services offered
Snapshot File Location
D:\Hyper-V\Configuration
Smart Paging File Location
D:\Hyper-V\Configuration
Hard Drive
You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.
Controller:
IDE Controller 0
Location:
0 (in use)
Media
You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.
Virtual hard disk:
New
Edit
Inspect
Browse...
Actions
HYPERV01
New
Import Virtual Machine...
Hyper-V Settings...
Virtual Switch Manager...
Virtual SAN Manager...
Edit Disk...
Inspect Disk...
Stop Service
Remove Server
Refresh
View
Help
warder-va
Connect...
Open
Hyper-V ▸ VHDs
Search VHDs
Organize
New folder
Microsoft Manager
Favorites
Desktop
Downloads
Recent places
Libraries
Documents
Music
Pictures
Videos
Computer
os-150gb (C:)
Name
Date modified
Type
dynamic
9/18/2013 1:10 PM
forwarder-va
9/18/2013 1:10 PM
File name: forwarder-va
Virtual hard disk files
Open
Cancel



2. Click **Apply**.

Step 6 – Power on the Virtual Machine

Describes Step 6 – Power on the Virtual Machine in Cisco Secure Access. If all is well, you'll see the Virtual Appliance console screen.

If all is well, you'll see the Virtual Appliance console screen. For information about configuring VAs, see Configure Virtual Appliances.

Step 7 – Repeat for the Second Virtual Appliance

Describes Step 7 – Repeat for the Second Virtual Appliance in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Two VAs are required per Umbrella site. It is critical that these VAs are **not** cloned or copied in any way. Each VA must be set up and configured manually.

To build your second VA, repeat procedures starting at 2. Import Virtual Appliance.

Deploy VAs in VMware

Describes Deploy VAs in VMware in Cisco Secure Access and explains Prerequisites and Configure Authentication for the Virtual Appliances. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Deploy Cisco Secure Access Virtual Appliances (VAs) in VMware.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Basic knowledge of VMware ESXi. For more information, see the VMware documentation.

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure for Deploying VAs in VMware

Describes Procedure for Deploying VAs in VMware in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

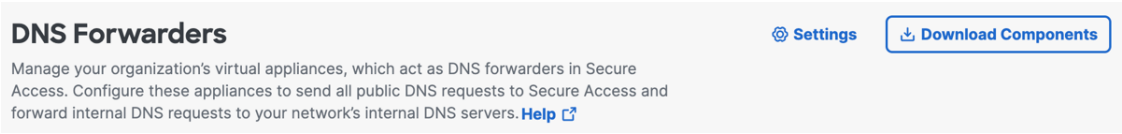
- Step 1 – Download OVF Template
- Step 2 – Deploy OVF Template
- Step 3 – Deploy a Second Virtual Appliance
- Step 4 – Power on the Virtual Machines

Step 1 – Download OVF Template

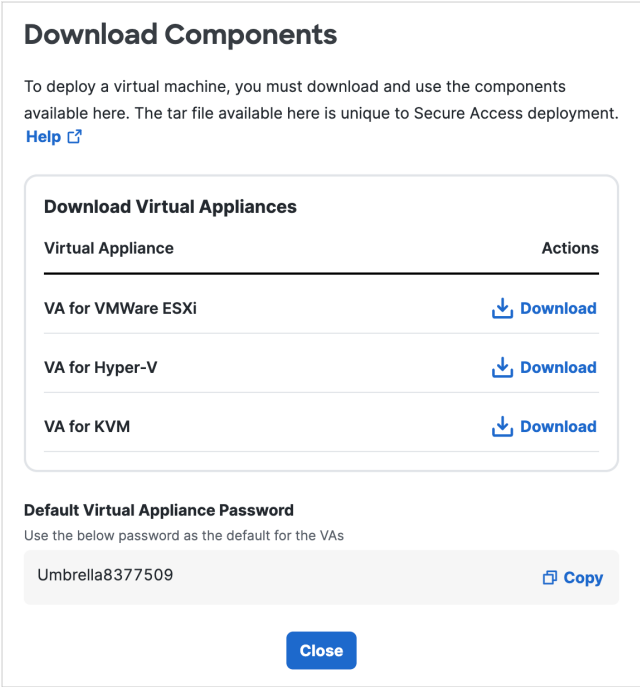
Provides instructions for completing the Step 1 – Download OVF Template workflow in Cisco Secure Access. Navigate to Connect DNS Forwarders and click Download Components.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** next to **VA for VMWare ESXi**.



Umbrella generates and downloads a .tar file unique to your deployment.

This tar file includes:

- an .ovf template containing the virtual hard disks that need to be deployed on VMware
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. On successful signature validation, you should see a message saying “Verified OK."

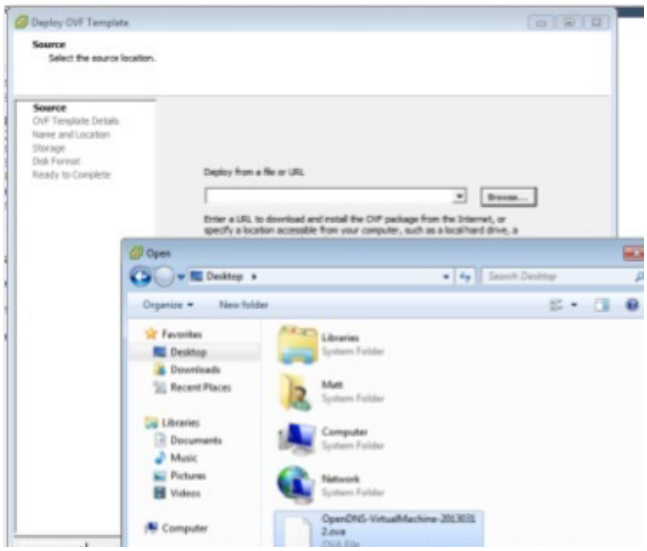
Step 2 – Deploy OVF Template

Provides instructions for completing the Step 2 - Deploy OVF Template workflow in Cisco Secure Access. Log into your VMware vSphere client and select the File tab.

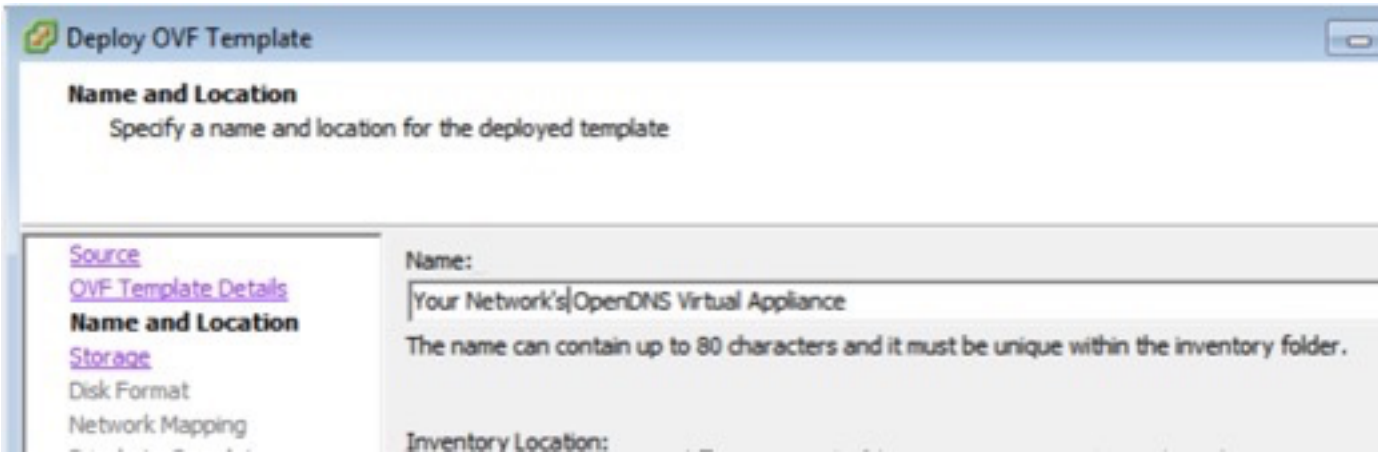
Procedure

---

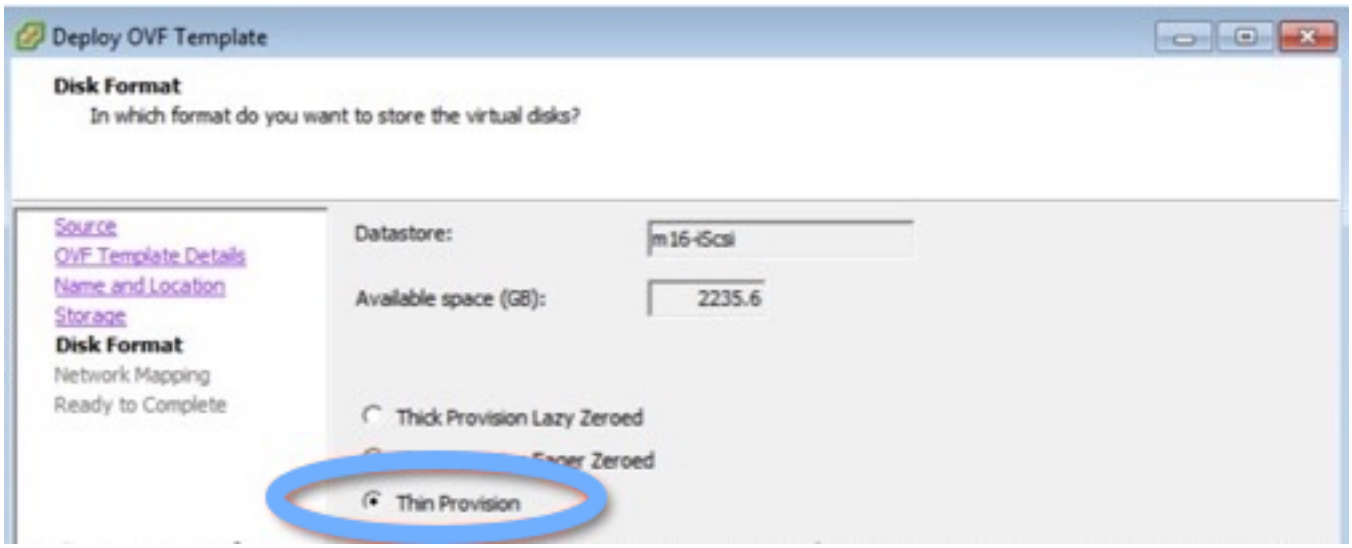
1. Log into your VMware vSphere client and select the **File** tab.
2. Click **Deploy OVF Template**, choosing the downloaded .ova template.



3. Follow the deployment wizard prompts, but be sure to follow these steps:
   - For the source, browse to the .ova file you just downloaded.
   - Specify a unique name and location for your VA.



4. Select the disks appropriate to your environment. It is recommended to select **Thin Provision** for the disk format, but it is not mandatory.



5. Select or map a network.



6. Click **Finish**.

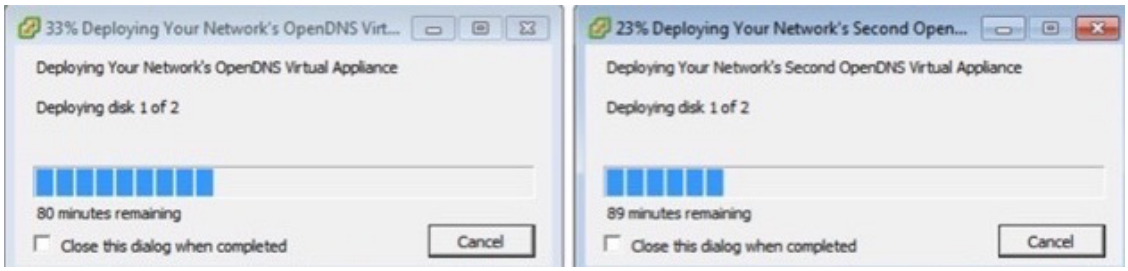
   The system begins to deploy the VA. During the deployment, subsequent prompts update you about the status of the deployment.

Step 3 – Deploy a Second Virtual Appliance

Describes Step 3 – Deploy a Second Virtual Appliance in Cisco Secure Access. While the first VA is deploying, repeat the previous two steps to configure your second VA.Two VAs are required per Umbrella site.

While the first VA is deploying, repeat the previous two steps to configure your second VA.

> **Note**
>
> Two VAs are required per Umbrella site. It is **critical** that these VAs are **not** cloned or copied in any way. Each VA must be set up and configured manually.



Step 4 – Power on the Virtual Machines

Describes Step 4 – Power on the Virtual Machines in Cisco Secure Access. If the deployment succeeded, you'll see the VA console screen.

If the deployment succeeded, you'll see the VA console screen. For information about configuring VAs, see Configure Virtual Appliances.

Deploy VAs in Microsoft Azure

Describes Deploy VAs in Microsoft Azure in Cisco Secure Access. Deploy Cisco Secure Access Virtual Appliances (VAs) in Microsoft Azure.

Deploy Cisco Secure Access Virtual Appliances (VAs) in Microsoft Azure.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- If you use the VA on Azure as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA. The VA should receive DNS packets with the source IP as the internal IP of the endpoints. An ExpressRoute or dedicated MPLS or site-to-site VPN connection from your on-premise environment to Azure will meet this requirement.
- A system running Windows 10 with the Hyper-V role enabled to convert VHD images to an Azure-acceptable format.
- Only VAs running version 2.4 or above can be deployed in Microsoft Azure.

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure for Deploying VAs in Microsoft Azure

Provides instructions for completing the Procedure for Deploying VAs in Microsoft Azure workflow in Cisco Secure Access. Add internal.cloudapp.net to the internal domains list for VAs.

Before you begin

- Add **internal.cloudapp.net** to the internal domains list for VAs.
- Unless you are using your own DNS server in Azure, you should configure **168.63.129.16** as the local DNS server in the VA settings. This is the virtual IP used by Azure for recursive and local DNS queries.

Procedure

1. Step 1 – Prepare the Virtual Appliance Image on Azure. This is a one time task.
2. Step 2 – Launch the Virtual Appliance on Azure. Perform this task for each VA after you have performed the one-time task of preparing the VA image.

Step 1 – Prepare the Virtual Appliance Image on Azure

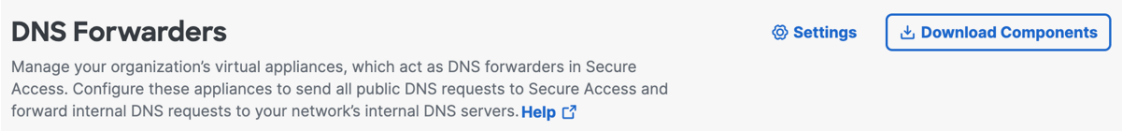
Provides instructions for completing the Step 1 - Prepare the Virtual Appliance Image on Azure workflow in Cisco Secure Access. This is a one-time task to create an image in Azure that can be used to launch multiple VAs.Generation 2 VMs are not supported for VA deployments.

This is a one-time task to create an image in Azure that can be used to launch multiple VAs.

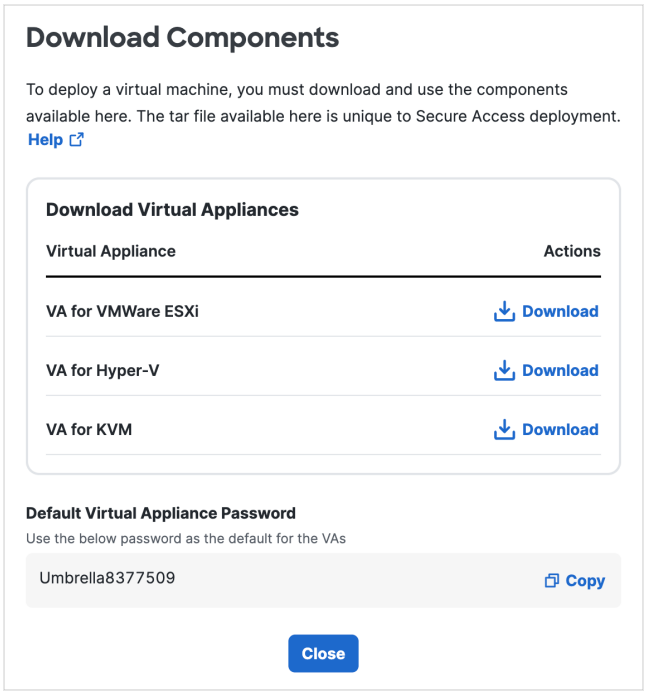
> **Note**
>
> Generation 2 VMs are not supported for VA deployments.

Procedure

1. Navigate to **Connectors** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** next to **VA for Hyper-V**.



Umbrella generates and downloads to your computer a .tar file unique to your deployment.

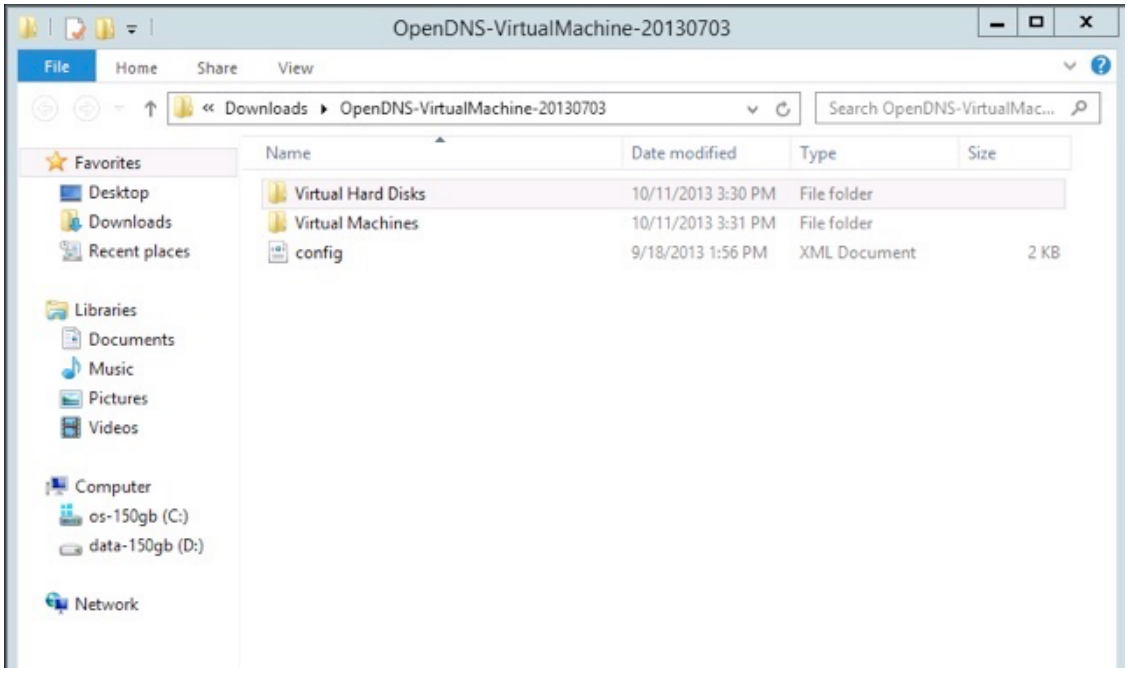
This tar file includes:

- a .zip file containing the virtual hard disks that need to be deployed on Azure
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. On successful signature validation, you should see a message saying “Verified OK."

4. Extract the downloaded zip file. You'll find two folders–`Virtual Hard Disks` and `Virtual Machines`–and a `config` file.



5. Open Windows PowerShell as Administrator, navigate to the `Virtual Hard Disks` folder, and convert the vhd files (forwarder and dynamic) in their respective folders to a fixed type format acceptable by Azure.

   To convert and resize the forwarder file, run the following commands:

```
Convert-VHD -Path .\forwarder-va.vhd -DestinationPath forwarder-fixed.vhd
-VHDType fixed
Resize-VHD .\forwarder-fixed.vhd  -SizeBytes 8GB
```

   To convert and resize the dynamic file, run the following commands:

```
Convert-VHD -Path .\dynamic.vhd -DestinationPath dynamic-fixed.vhd -VHDType
fixed
Resize-VHD .\dynamic-fixed.vhd -SizeBytes 30MB
```

   Important

   Conversion free disk space requirements

   Conversion requires at least 9GB of free disk space to create the modified disks. The new forwarder-fixed.vhd will consume approximately 8GB of space. Machines with less than 9GB of space will fail to convert with a red error message.

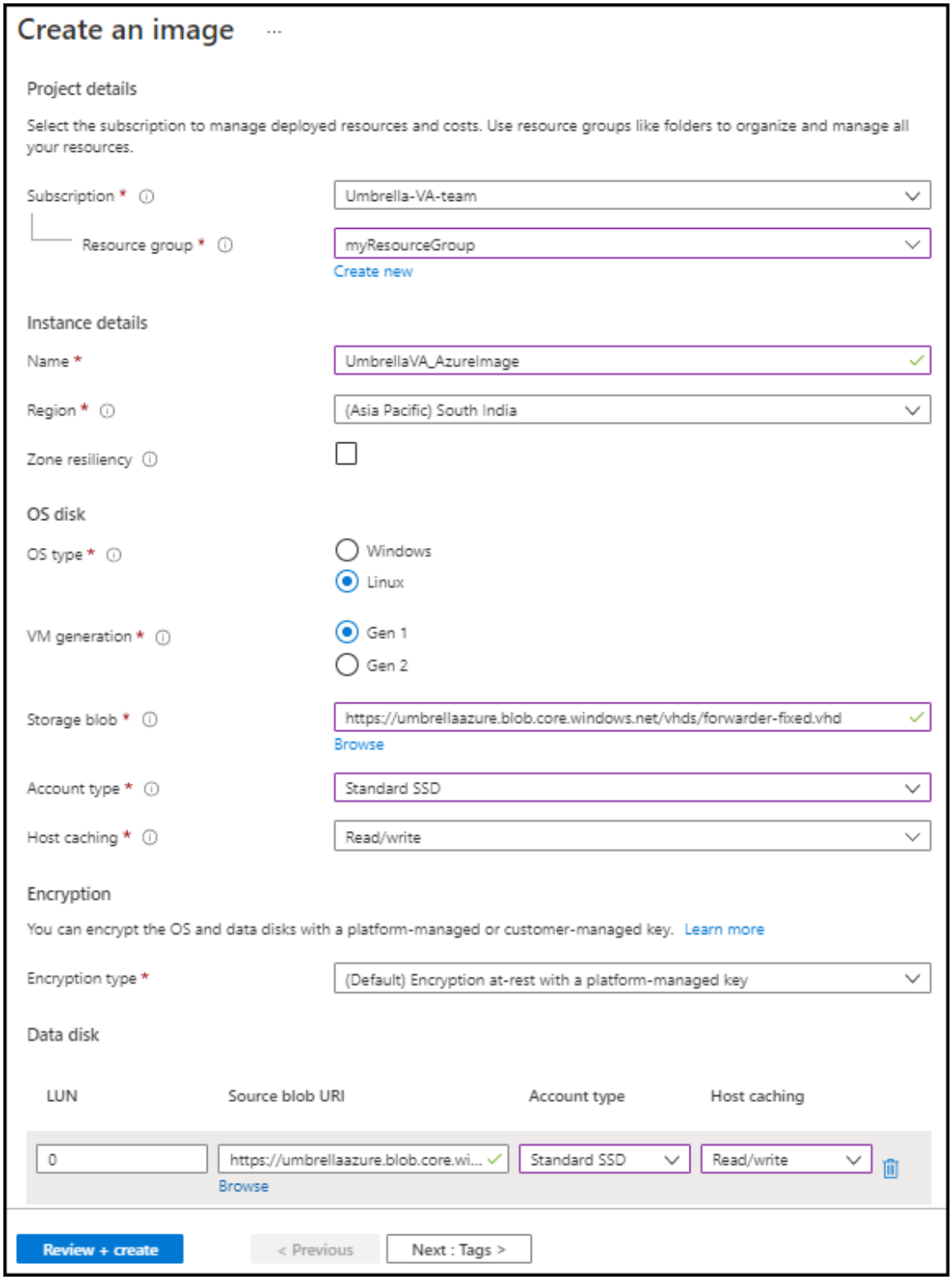
6. Upload the `forwarder-fixed.vhd` and `dynamic-fixed.vhd` to a blob in your Azure storage account using the Azure portal or the AZ CLI.

> **Note**
>
> This is a one-time upload.

7. Create an image in Azure from these virtual hard disks using the Azure portal.

   Use the `forwarder-fixed.vhd` as the OS disk (OS type: Linux) and the `dynamic-fixed.vhd` as the data disk.

> **Note**
>
> Ensure that **Host caching** for both the OS disk and data disk is set to `Read/write`. Since second generation VMs are not supported for VA deployments, ensure that you set **VM Generation** to `Gen 1`.



8. Once the VA image is created in Azure, use this image to launch multiple VAs. For more information, see Step 2: Launch the Virtual Appliance on Azure.

Step 2 – Launch the Virtual Appliance on Azure

Provides instructions for completing the Step 2 – Launch the Virtual Appliance on Azure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

> **Note**
>
> Before performing this task, you must complete the one-time task of preparing the virtual appliance image on Azure. For more information, see Step 1: Prepare the Virtual Appliance Image on Azure.

Procedure

---

1. Use the Azure portal to launch Secure Access VAs in Azure using the VA image you created in Step 1: Prepare the Virtual Appliance Image on Azure:
   - Choose a VM size with at least one VCPU and 1024 MB RAM.

     > **Note**
     >
     > VM sizes above eight VCPUs are not supported.

   - For the Administrator account, set the Authentication type to **Password**.

     > **Note**
     >
     > It is a security risk to specify a public IP address for the VA, and is not recommended except in case of SNAT port exhaustion issues. If you need to configure a public IP for the VA on Azure for these issues, ensure that inbound access from the Internet is not permitted. For more information, see Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed in Azure.

   - Provide the username as **vmadmin** and enter a password that meets complexity requirements.

     > **Note**
     >
     > The admin-password you create here is not actually set on the VA.

2. You may also use the Azure Cloud Shell to launch VAs in Azure using the VA images you created in Step 1: Prepare the Virtual Appliance Image on Azure. VM sizes above eight VCPUs are not supported.

   You may specify the static IP as part of the command. For example:

```
az vm create --resource-group MyResourceGroup --size Standard_B2s --name
UmbrellaVA
```

```
--image VAImage --authentication-type password --admin-username vmadmin
--admin-password <password> --vnet-name MyVnet --subnet MySubnet
--private-ip-address 10.0.0.1
```

3. In Secure Access, navigate to **Connector** > **DNS Forwarders**. Secure Access displays your list of deployed VAs.
4. Use the same image to launch multiple VAs as required. Provide a different name and different static IP for each VA.

> **Note**
>
> If you do not specify the private IP address, the VA will automatically pull a DHCP IP and register to Umbrella with this IP address. This IP address will be listed as the VA name in Secure Access.

What to do next

> **Tip**
>
> **Diagnostic Settings**
>
> It is not recommended to turn on Diagnostic Settings (Guest-level monitoring) or install any extension for a VA on Azure. Enabling diagnostics results in huge log files being generated on the VA, which causes the VA to run out of disk space.
>
> If your VA on Azure is reporting disk space issues, navigate to the **Settings** > **Extensions** page against your VA on the Azure portal and remove any extensions. Also, navigate to the **Monitoring** > **Diagnostic Settings** page against your VA on the Azure portal and verify that Guest-level monitoring is turned off.

Deploy VAs in Amazon Web Services

Describes Deploy VAs in Amazon Web Services in Cisco Secure Access. Deploy Cisco Secure Access Virtual Appliances (VAs) in Amazon Web Services.

Deploy Cisco Secure Access Virtual Appliances (VAs) in Amazon Web Services.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- If you are using the VA on Amazon Web Services as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA.

The VA should receive DNS packets with the source IP as the internal IP of the endpoints. An AWS Direct Connect or dedicated MPLS or VPN connection from your on-premise environment to AWS will meet this requirement.

- Only VAs running version 2.6 or above can be deployed in AWS.

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure for Deploying VAs in Amazon Web Services

Describes Procedure for Deploying VAs in Amazon Web Services in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

1. Prepare the Virtual Appliance Amazon Machine Image. This is a one time task.
2. Launch the Virtual Appliance on Amazon Web Services. Perform this task for each VA after you have performed the one-time task of preparing the VA image.

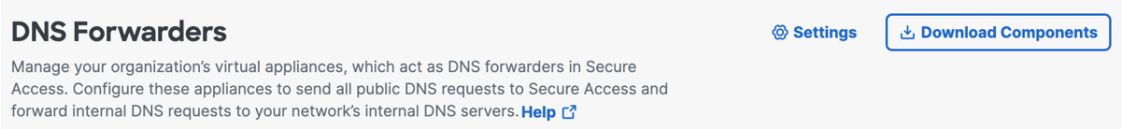
Step 1 – Prepare the Virtual Appliance Amazon Machine Image

Provides instructions for completing the Step 1 – Prepare the Virtual Appliance Amazon Machine Image workflow in Cisco Secure Access. Navigate to Connect DNS Forwarders and click Download Components.

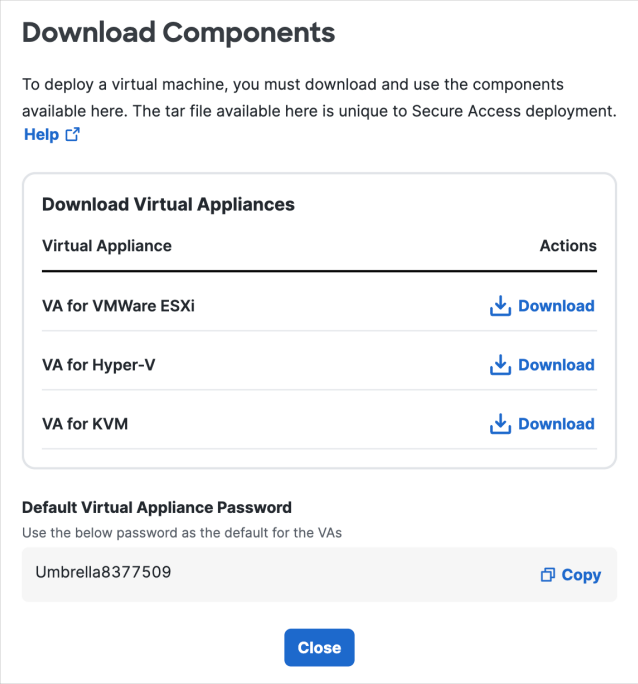
> **Note**
>
> This is a one-time task to create an Amazon Machine Image (AMI) that can be used to launch multiple VAs.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** for **VA for Hyper-V**.



Secure Access generates and downloads a .tar file to your computer unique to your deployment.

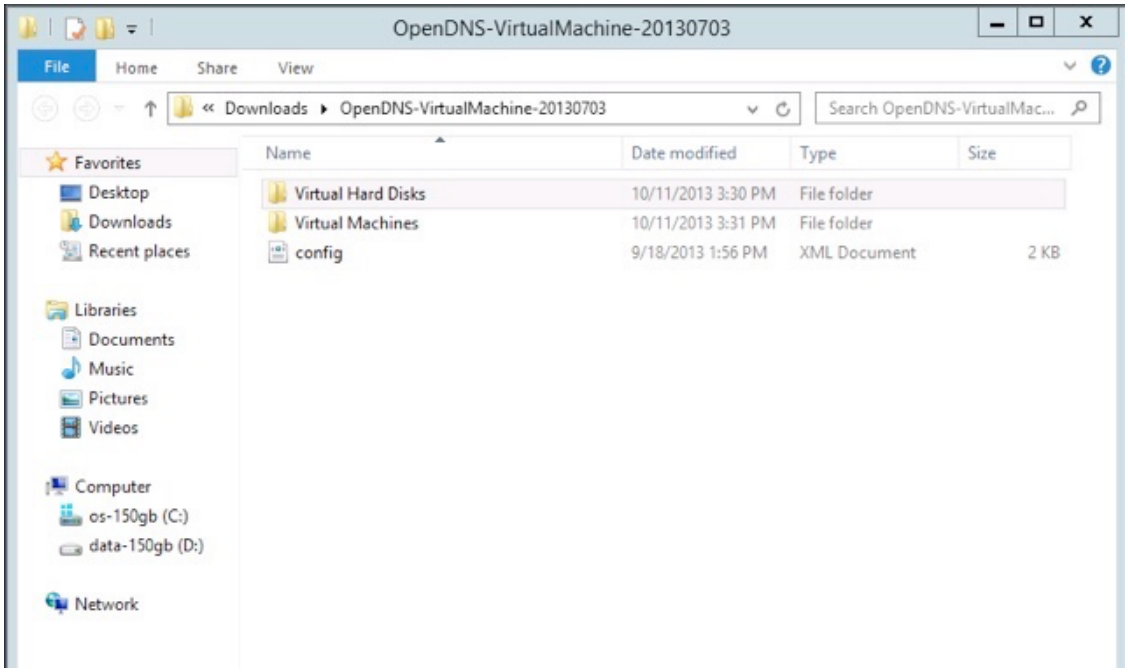
This .tar file includes:

- a .zip file containing the virtual hard disks that need to be deployed on AWS
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. On successful signature validation, you see a message saying “Verified OK.“

4. Extract the .zip file. You'll find two folders–**`Virtual Hard Disks`** and **`Virtual Machines`**–and a **`config`** file.



5. Follow the steps provided by AWS to (optionally) create an S3 bucket and to create the vmimport service role.
6. Upload the downloaded vhd files (forwarder-va.vhd and dynamic.vhd) to the S3 bucket.

   This should be the same S3 bucket as specified in the role-policy.json file.

7. Use the AWS CLI to import the image.

   Create a file locally named "containers.json" for importing the image. The following is an example of a containers.json file. Specify the S3 bucket where you have saved the vhd images in this file.

```
\[
  {
    "Description": "Forwarder",
    "Format": "vhd",
    "UserBucket": {
        "S3Bucket": "va-vhd-bucket",
        "S3Key": "forwarder-va.vhd"
    }
  },
  {
    "Description": "Dynamic",
    "Format": "vhd",
    "UserBucket": {
        "S3Bucket": "va-vhd-bucket",
        "S3Key": "dynamic.vhd"
    }
  }
\]
```

Important

You must use the .vhd files to create the Amazon Machine Image and *not* the .ova file. Creating the AMI using the .ova file will result in the VA not being able to register to Umbrella.

8. Use the AWS CLI command `import-image` to create import tasks:

```
aws ec2 import-image --description "Umbrella VA" --license-type BYOL
--disk-containers "file://containers.json"
```

9. Note the AMI ID and verify that the import has been completed through the `describe-import-image-tasks` command:

   ```
   aws ec2 describe-import-image-tasks --import-task-ids <AMI ID>
   ```

10. Once the VA Amazon Machine Image is created, use this image to launch multiple VAs. For more information, see Step 2. Launch the Virtual Appliance on Amazon Web Services.

Step 2 – Launch the Virtual Appliance on Amazon Web Services

Provides instructions for completing the Step 2 - Launch the Virtual Appliance on Amazon Web Services workflow in Cisco Secure Access. Use the AWS console to launch Secure Access VA instances in AWS using the VA image you created in Step 1.

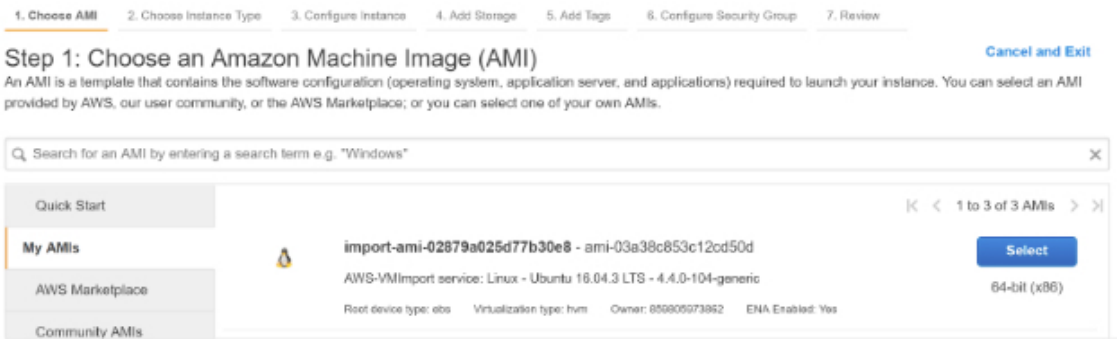
> **Note**
>
> Before performing this task, you must complete the one-time task of preparing the virtual appliance image on AWS.

> **Tip**
>
> Nitro based instance types and instance types that enable the Elastic Networking Adapter (ENA) are currently not supported. Refer to AWS documentation to determine if the instance type is Nitro based or uses ENA.

Procedure

1. Use the AWS console to launch Secure Access VA instances in AWS using the VA image you created in Step 1. Prepare the Virtual Appliance Image on Amazon Web Services. Choose a VM size with at least 1 VCPU and 1 GB RAM.

   > **Note**
   >
   > Specifying a public IP address for the VA is a security risk and is not a supported configuration.



2. In Secure Access, navigate to **Connectors** > **DNS Forwarders**.

You should see the VA listed here with the dynamic IP address as its name.

You can now configure the VA. For more information and the procedure, see Enter Configuration Mode on a VA Deployed in Azure, AWS, or Google Cloud Platform.

> **Tip**
>
> Route 53 Resolver can also be used to apply network-level protection to your AWS workloads. See How to Point AWS to Umbrella with New Route 53 Feature for more information.

3. For a VA deployed on AWS, in addition to configuring the IP of the VA via the VA command line, you will also need to assign this IP to the VA instance through the AWS console. If this IP is different from the DHCP IP assigned by AWS, you can add it as the secondary IP for the instance.

Deploy VAs in Google Cloud Platform

Describes Deploy VAs in Google Cloud Platform in Cisco Secure Access. Deploy Cisco Secure Access Virtual Appliances (VAs) in Google Cloud Platform.

Deploy Cisco Secure Access Virtual Appliances (VAs) in Google Cloud Platform.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- If you are using the VA on Google Cloud Platform (GCP) as a DNS server for your on-premise endpoints, then DNS traffic from these endpoints should not traverse through a Network Address Translation (NAT) device en route to the VA. The VA should receive DNS packets with the source IP as the internal IP of the endpoints. A Google Cloud Interconnect or dedicated MPLS or site-to-site VPN connection from your on-premise environment to GCP meets this requirement.
- A Linux system with the qemu-utils package installed, on which you can run qemu-img and tar commands.
- Only VAs running version 2.6 or above can be deployed in GCP.

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure

Describes Procedure in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

- Step 1 – Prepare the Virtual Appliance Instance Template on GCP. This is a one time task.

- Step 2 - Launch the Virtual Appliance on Google Cloud Platform. Perform this task for each VA after you have performed the one-time task of preparing the VA image.

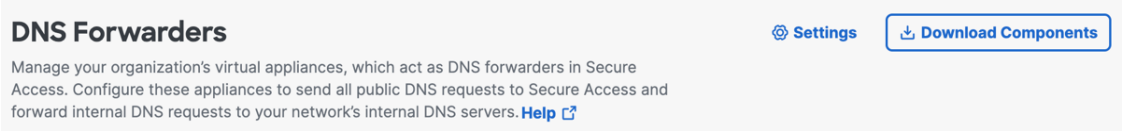
Step 1 – Prepare the Virtual Appliance Instance Template on GCP

Provides instructions for completing the Step 1 - Prepare the Virtual Appliance Instance Template on GCP workflow in Cisco Secure Access. Navigate to Deployments Configuration Sites and Active Directory and click Download Components.

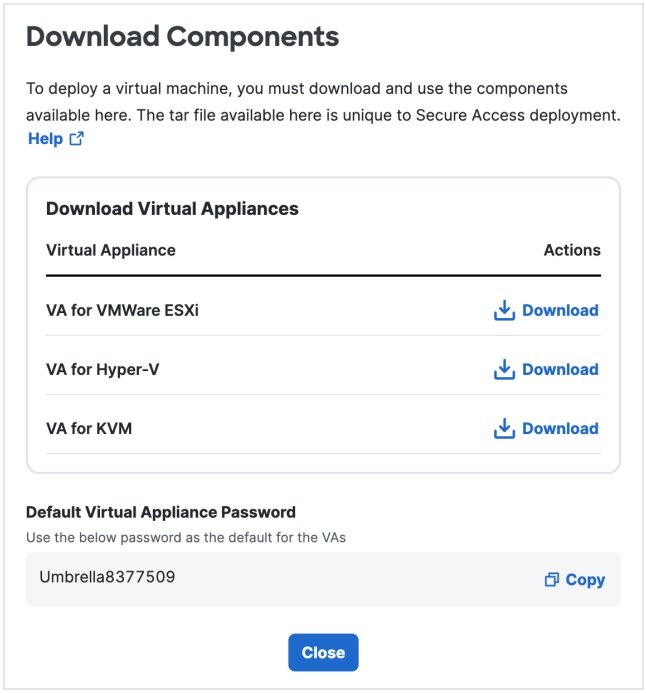
> **Note**
>
> This is a one-time task to create an Instance Template that can be used to launch multiple virtual appliances in GCP.

Procedure

1. Navigate to **Deployments** > **Configuration** > **Sites and Active Directory** and click **Download Components**.



2. Click **Download** for **VA for Hyper-V**.



Secure Access generates and downloads a .tar file unique to your deployment.

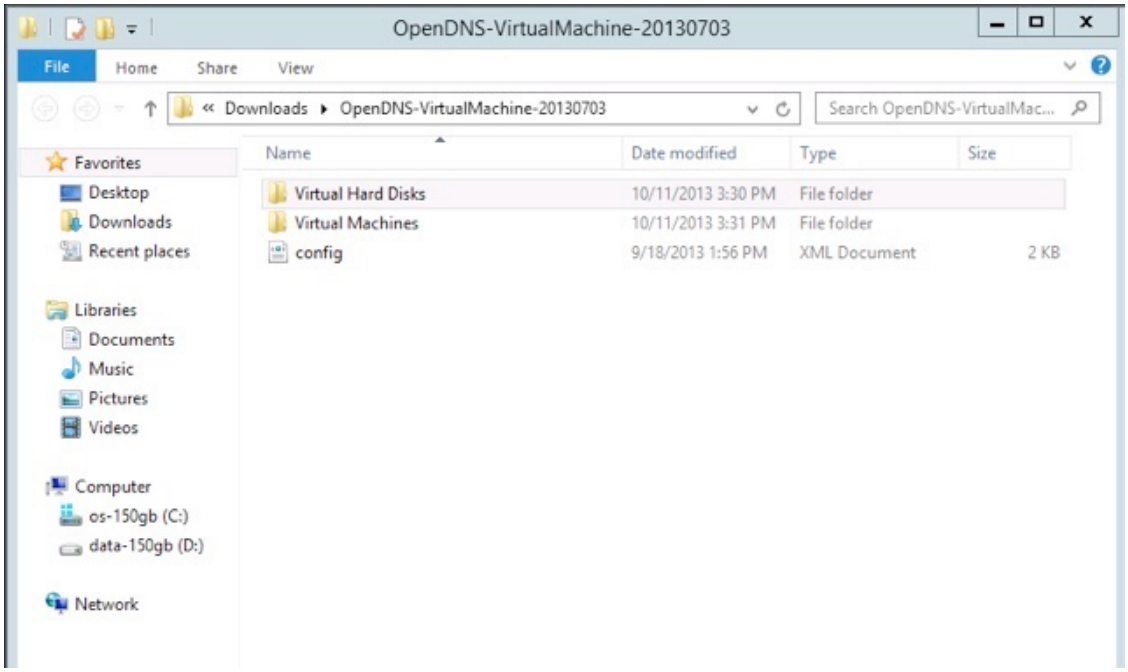
This .tar file includes:

- .zip file containing the virtual hard disks that need to be deployed on Google Cloud Platform
- Signature file
- Cisco public certificate to validate the signature
- README file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. When successful, you should see a message saying “Verified OK."

4. Extract the .zip file. The .zip file contains two folders–`Virtual Hard Disks` and `Virtual Machines`–and a `config` file.



5. Use the qemu-img convert commands to convert each of the VHD files to RAW format and resize them to a multiple of 1 GB.

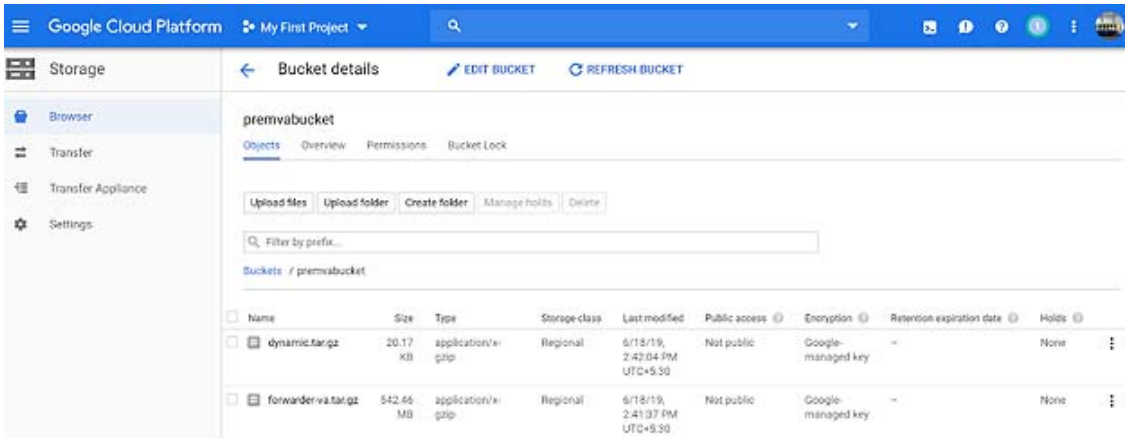
```
qemu-img convert -f vpc -O raw forwarder-va.vhd forwarder-va.raw
qemu-img resize forwarder-va.raw -f raw 7G
qemu-img convert -f raw -O raw dynamic.vhd dynamic.raw
qemu-img resize dynamic.raw -f raw 1G
```

6. Tar each raw file.

> **Note**
>
> GCP requires that each file be renamed as `disk.raw` before you tar it. GCP also requires tar to use the oldgnu format.

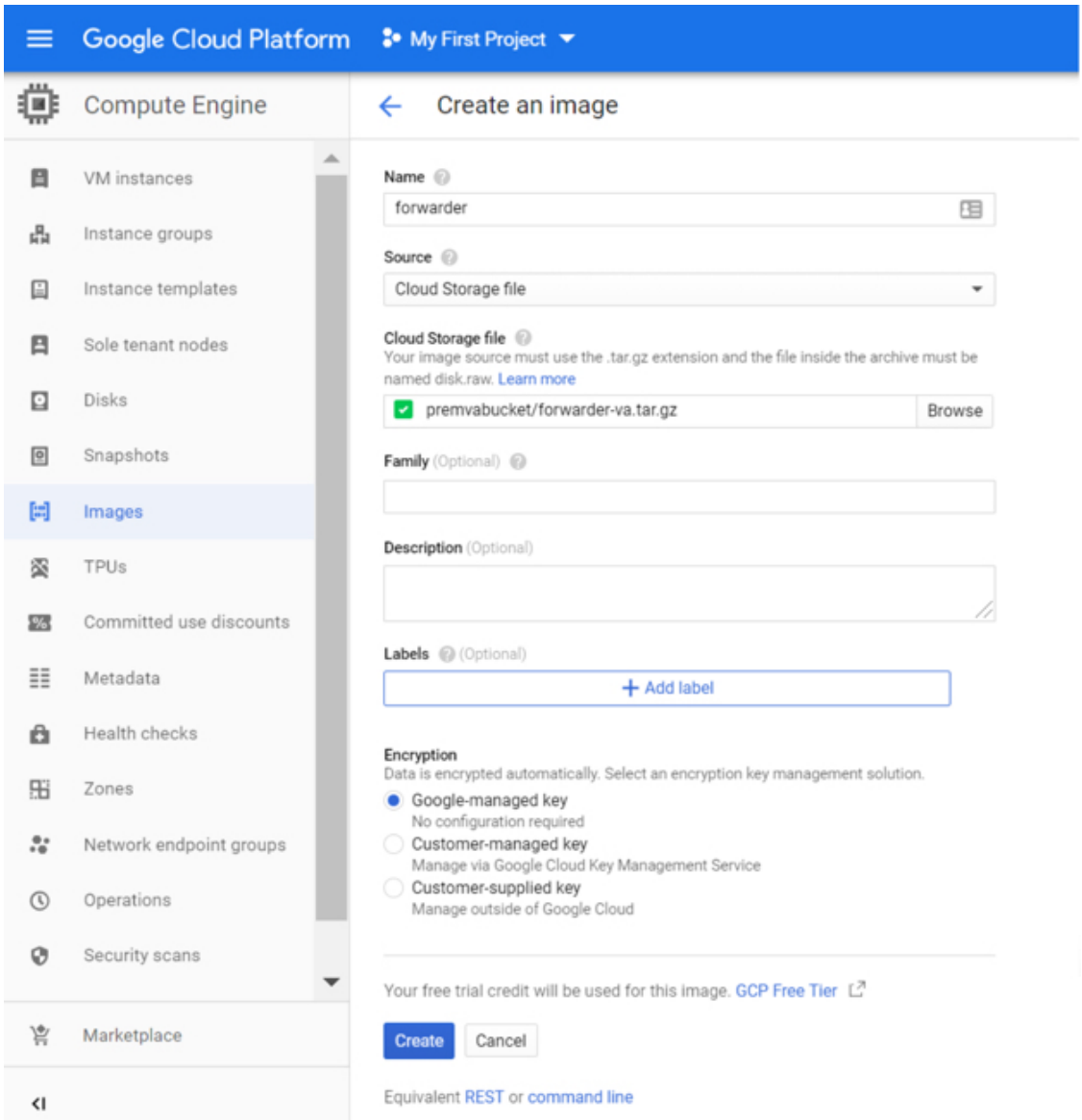
```
mv forwarder-va.raw disk.raw
tar --format=oldgnu -Sczf forwarder-va.tar.gz disk.raw
mv disk.raw forwarder-va.raw
mv dynamic.raw disk.raw
tar --format=oldgnu -Sczf dynamic.tar.gz disk.raw
mv disk.raw dynamic.raw
```

7. Create a bucket in GCP Storage Engine or use an existing bucket and then upload both the `forwarder-va.tar.gz` and `dynamic.tar.gz` files to this bucket.



8. Create two images in Google Compute Engine: one with source as the `forwarder-va.tar.gz` file and the other with source as the `dynamic.tar.gz` file.

   Each image is created with roughly the same size as its respective .tar.gz file (7 GB or 1 GB).

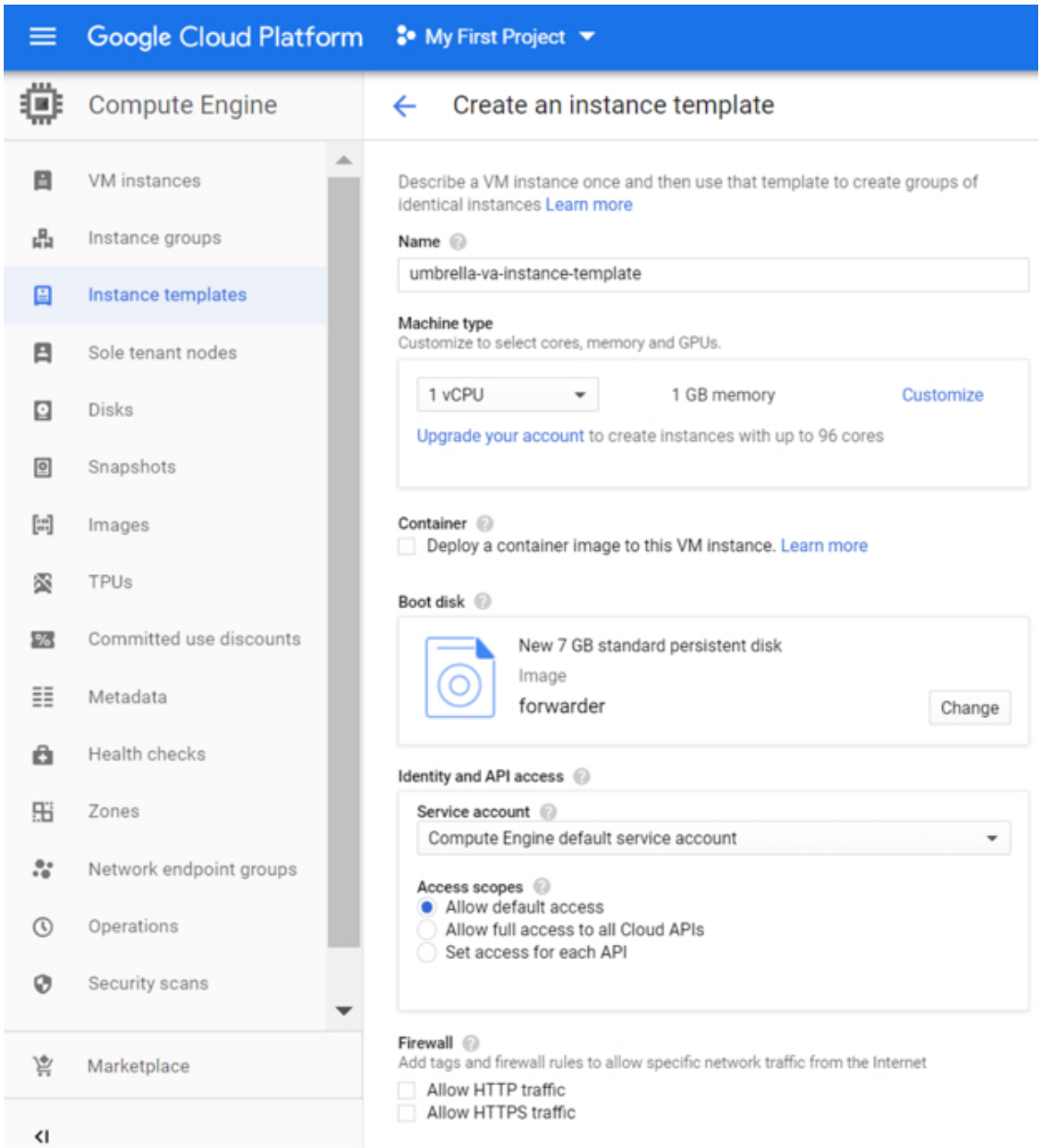


9. Create an Instance Template in the Google Compute Engine using the forwarder image as the boot image and the dynamic image attached as a data disk.

   Choose a machine type with at least 1 vCPU and 1 GB memory.

   To select the 'forwarder' image as the boot disk, choose **Change** on the boot disk, and then choose the forwarder image from the Custom Images category.

   > **Note**
   >
   > Do not click **Create**.

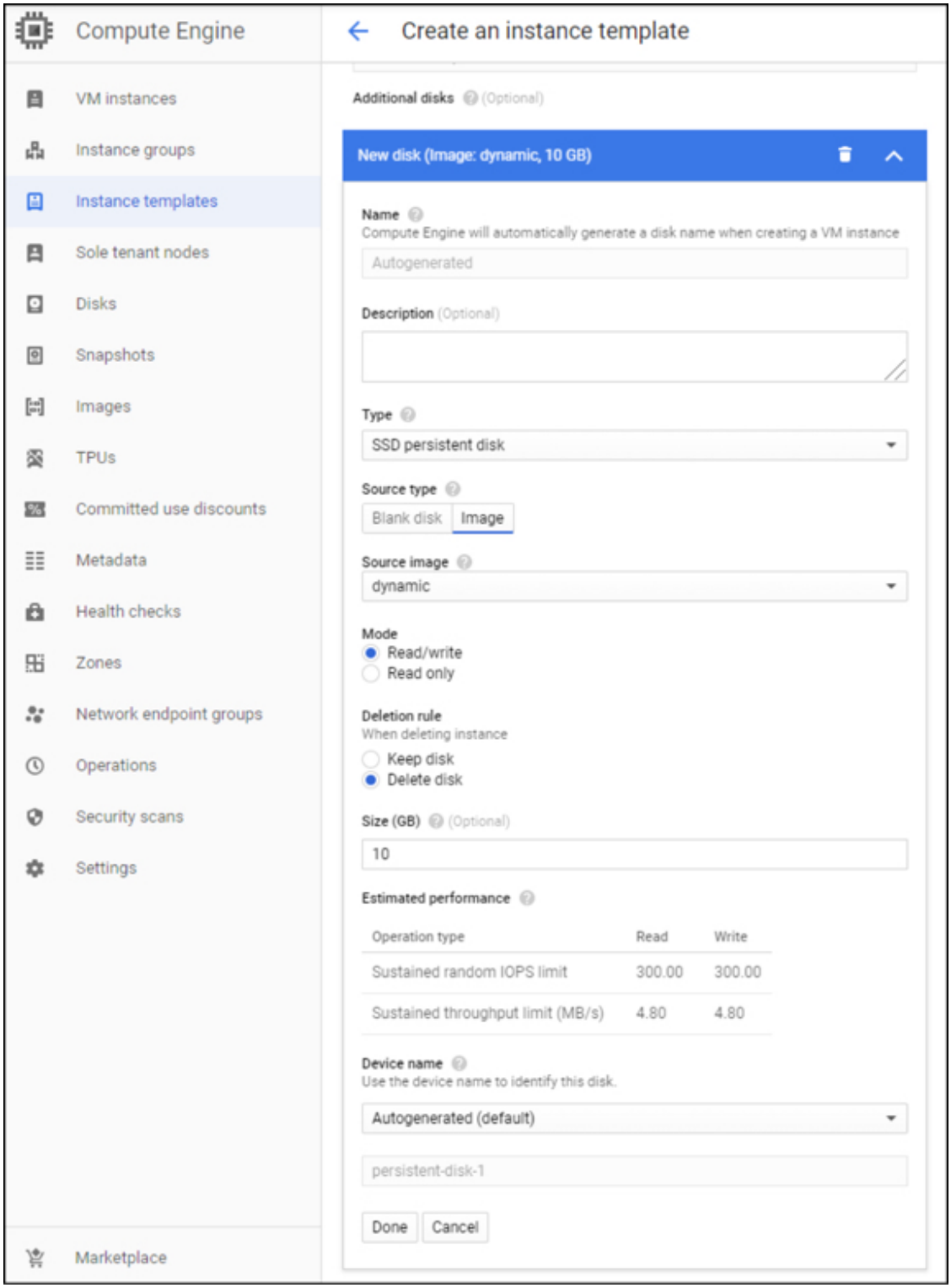


10. Click **Disks**, **Add new disk** to attach the dynamic disk to the instance template.

    You must create a new disk with the source as the 'dynamic' image you created earlier. Failure to do so results in your VA not registering with Umbrella.

Note

Google Cloud does not allow you to create a disk of size less than 10 GB from the dynamic image.



11. After you have added the new disk created from the dynamic image, you can click on Create to create the VA Instance template.
12. Once the VA Instance template is created, use this image to launch multiple VAs. For more information, see Step 2. Launch the Virtual Appliance on Google Cloud Platform.

Step 2 – Launch the Virtual Appliance on Google Cloud Platform

Provides instructions for completing the Step 2 – Launch the Virtual Appliance on Google Cloud Platform workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

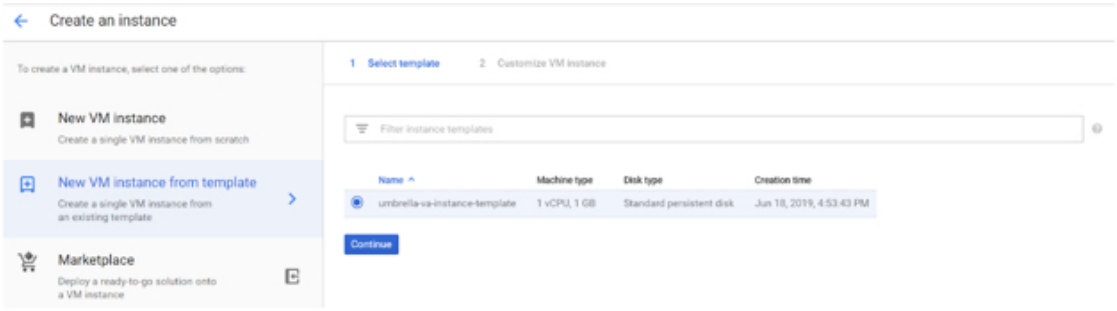
> **Note**
>
> Before performing this task, you must complete the one-time task of preparing the virtual appliance instance template

Procedure

1. Create VA instances based on the template.

   The VA will automatically pull a DHCP IP and register to Secure Access with this IP address.

   > **Note**
   >
   > Specifying a public IP address for the VA is a security risk and is not a supported configuration.



2. In Secure Access, navigate to **Connectors** > **DNS Forwarders**.

   You should see the VA listed here with the dynamic IP address as its name. You can now configure the VA. For information about configuring VAs, see Configure Virtual Appliances.

Deploy VAs in KVM

Describes Deploy VAs in KVM in Cisco Secure Access and explains Prerequisites and Configure Authentication for the Virtual Appliances. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Deploy Cisco Secure Access Virtual Appliances (VAs) in KVM.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- A Linux system with **qemu-utils** package installed.
- Only VAs running 2.5 or above can be deployed in KVM.
- Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
  - KVM on Ubuntu Linux (supported LTS versions)
  - KVM on Red Hat Linux (supported versions)

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure for Deploying VAs in KVM

Describes Procedure for Deploying VAs in KVM in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- A Linux system with **qemu-utils** package installed.
- Only VAs running 2.5 or above can be deployed in KVM.
- Virtual Appliance deployments in KVM are supported with specific Red Hat Linux and Ubuntu Linux versions only.
  - KVM on Ubuntu Linux (supported LTS versions)
  - KVM on Red Hat Linux (supported versions)

To successfully deploy a virtual appliance in a KVM environment, follow the steps as they are listed below:

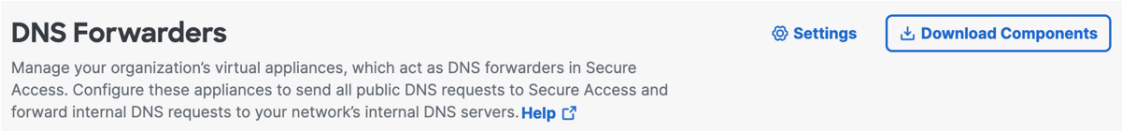
1. Step 1 – Download and Extract the KVM Installer
2. Step 2 – Launch the Virtual Appliance on KVM

Step 1 – Download and Extract the KVM Installer

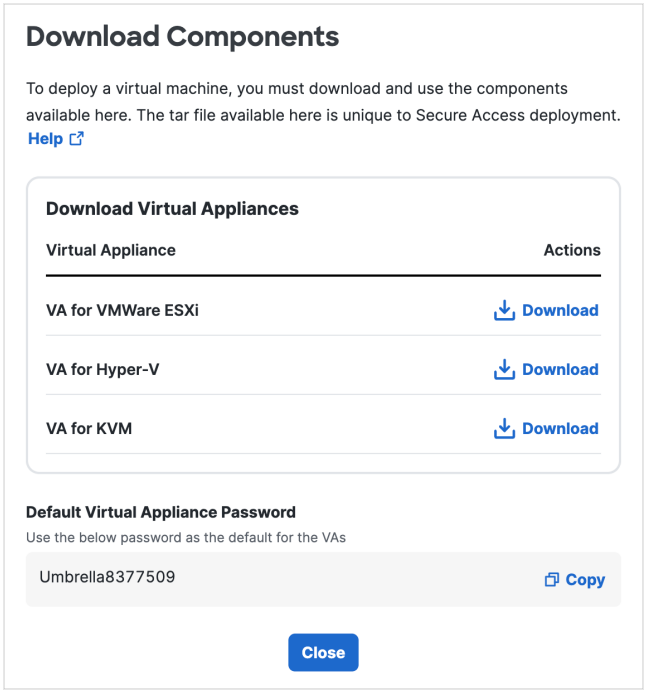
Download and extract Cisco Secure Access VA images for KVM. This topic covers navigating DNS Forwarders, extracting .tar/.zip files, and verifying .qcow2 disk integrity for secure deployment.

Procedure

1. Navigate to **Connect** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** next to **VA for KVM**.



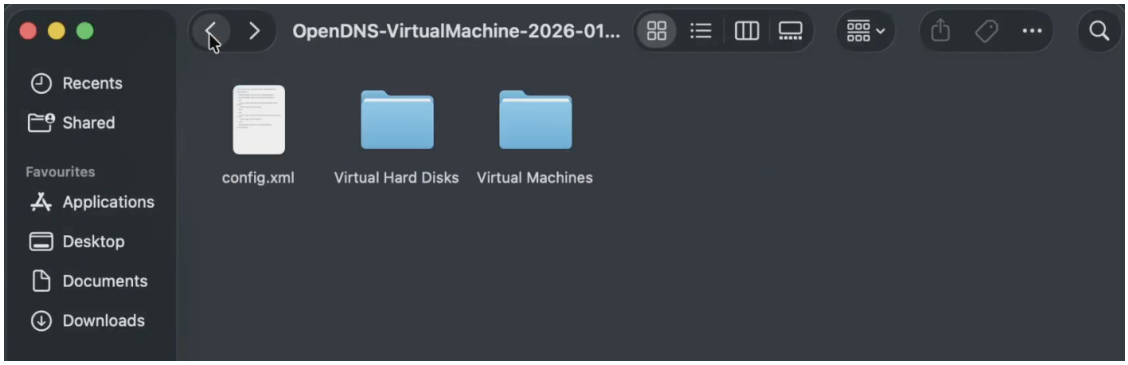
   Secure Access generates and downloads a .tar file unique to your deployment.

   This tar file includes:

   - A zip file containing the KVM-compatible virtual hard disk images (.qcow2 format) and configuration files
   - A signature file
   - A Cisco public certificate to validate the signature
   - A readme file

3. Extract the contents of the tar file using the `tar -xvf <tar filename> -C <Destination folder>` command.
4. Verify the integrity of the downloaded file by following the signature validation instructions in the readme file. On a successful verification, the message `Verified OK` is displayed.
5. Extract the .zip file.

   The extracted contents include the **Virtual Hard Disks** folder, the **Virtual Machines** folder, and a configuration file.



The `Virtual Hard Disks` folder contains the KVM-compatible .qcow2 files (namely, dynamic.qcow2 and forwarder-va.qcow2).

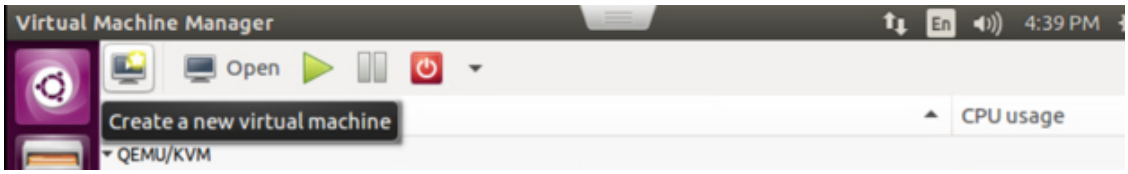
Step 2 – Launch the Virtual Appliance on KVM

Provides instructions for completing the Step 2 – Launch the Virtual Appliance on KVM workflow in Cisco Secure Access. Open the Virtual Machine Manager on your Linux system running KVM and click Create a new virtual machine.

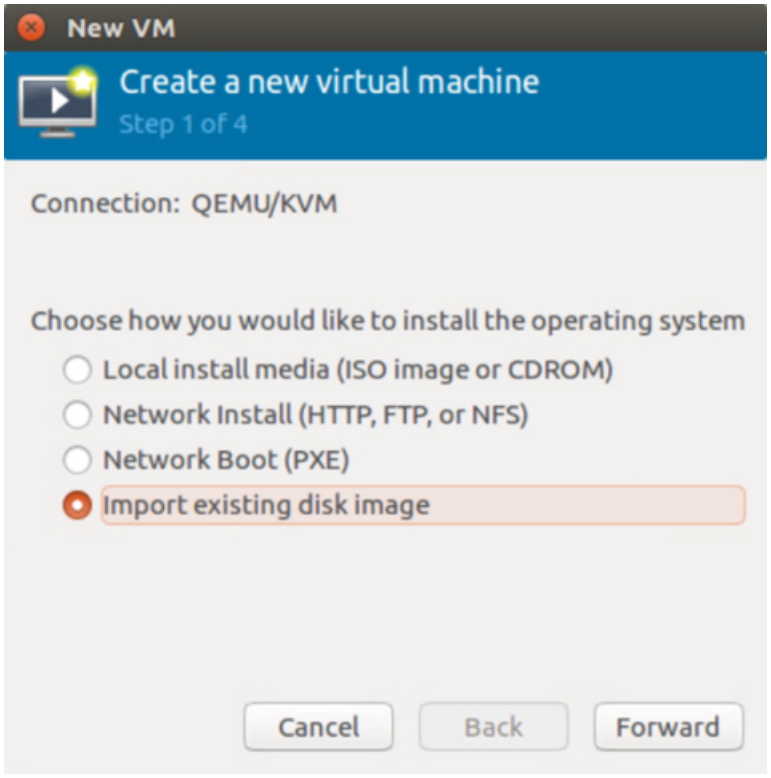
Procedure

---

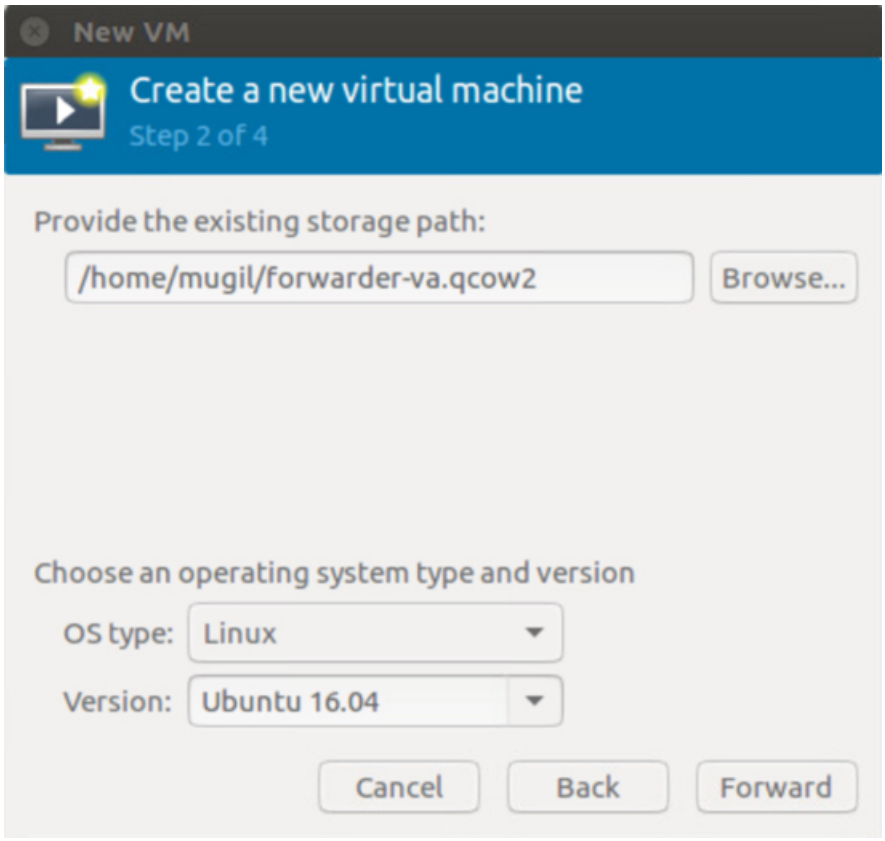
1. Open the Virtual Machine Manager on your Linux system running KVM and click **Create a new virtual machine**.



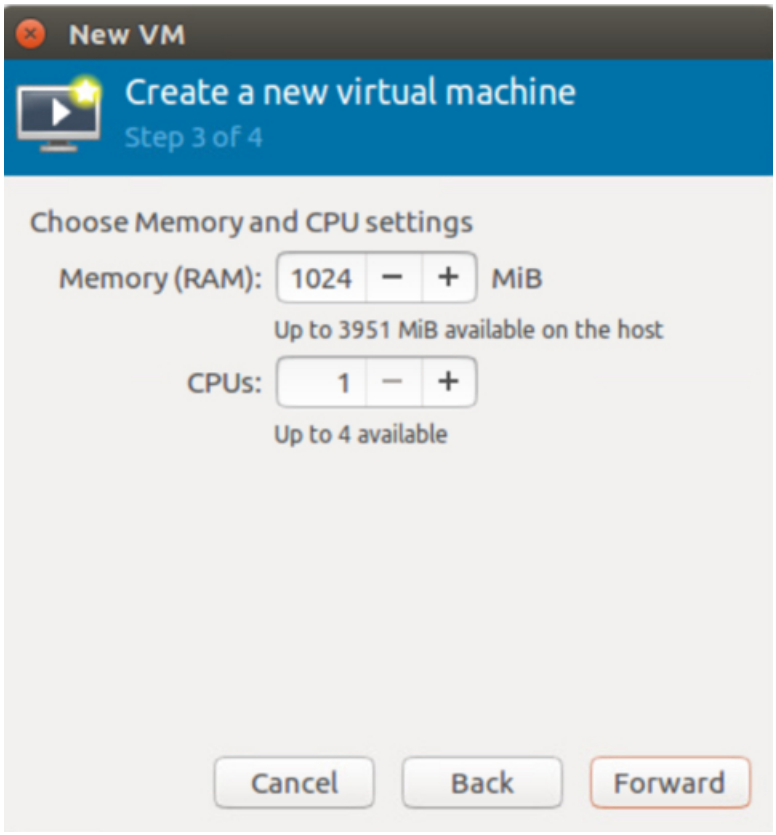
2. In the first step of the wizard, choose **Import existing disk image**.



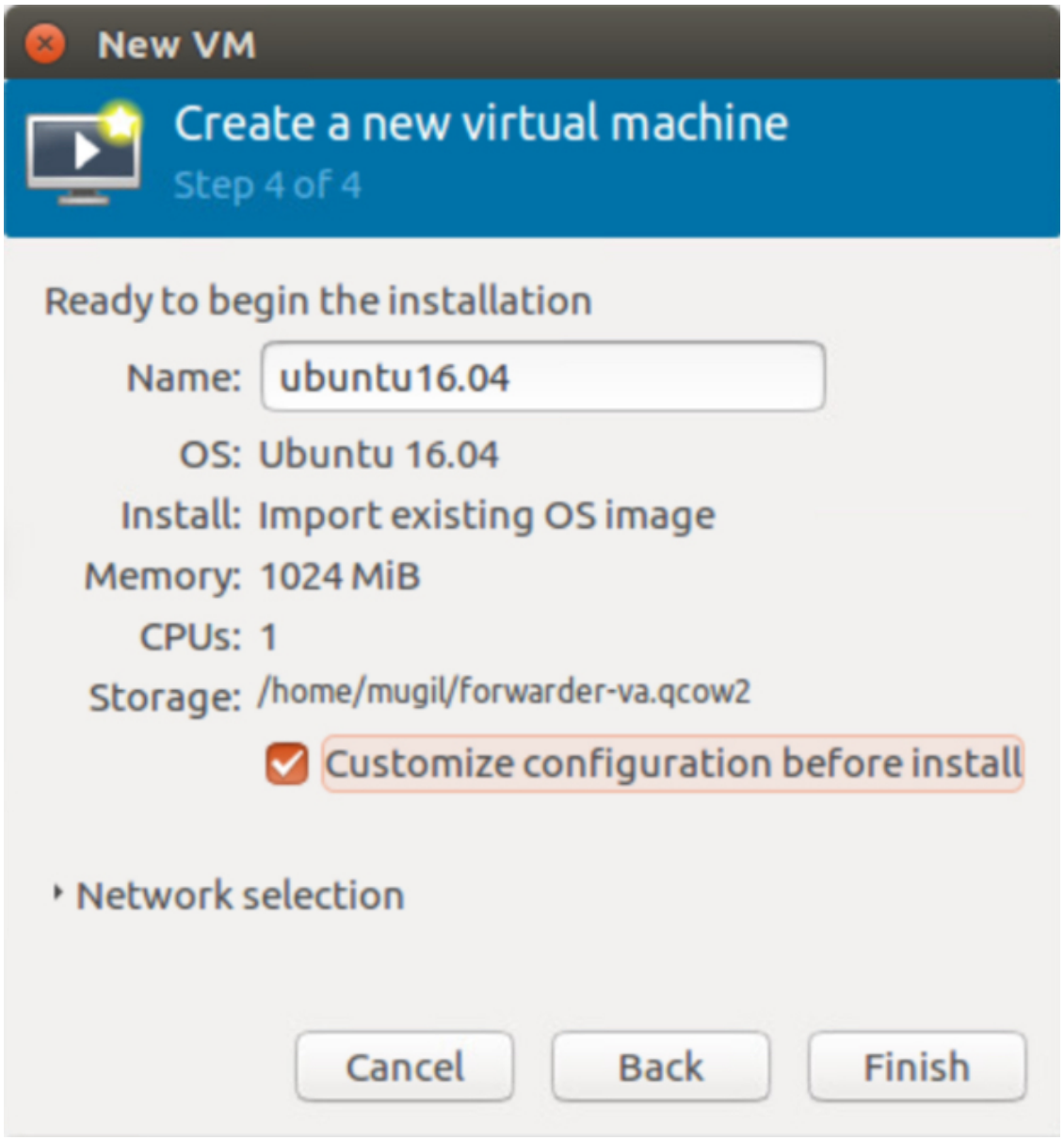
3. **Provide the existing storage path** to your **forwarder-va.qcow2**. Set the **OS type** to **Linux** and click **Forward**.



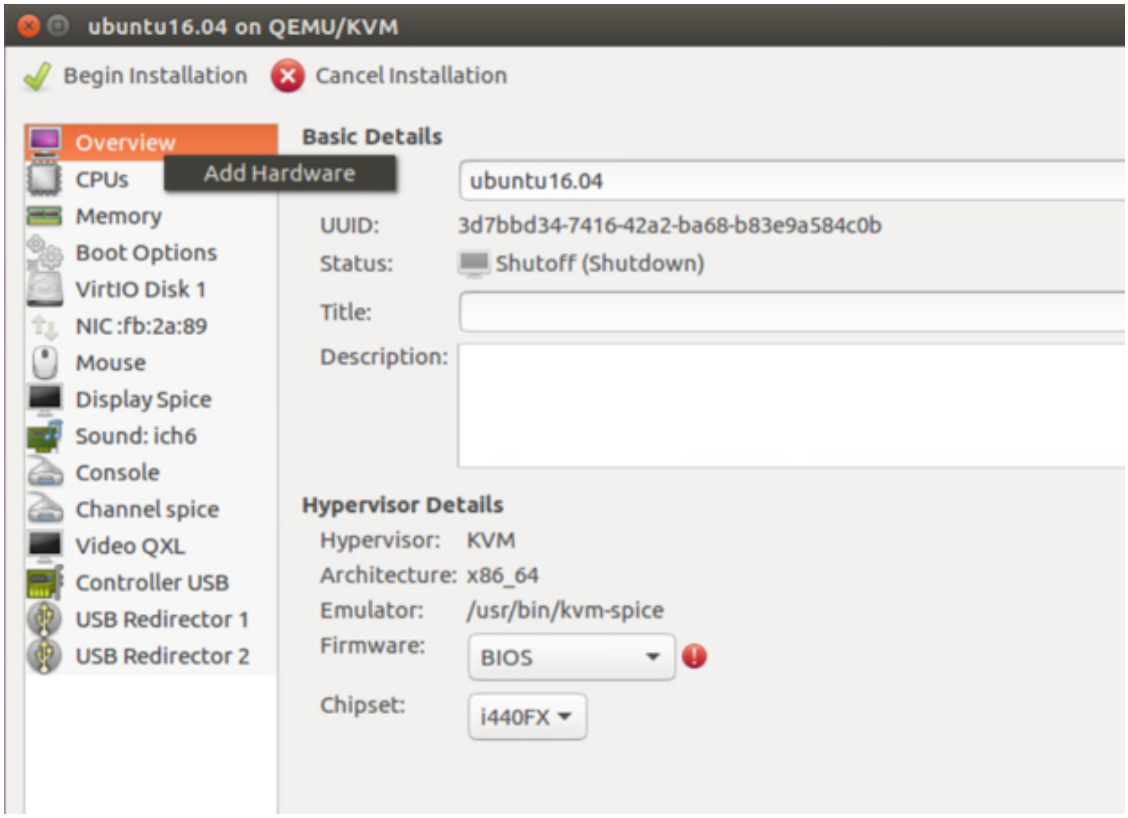
4. Set the memory and CPU settings to at least 1 CPU and 1 GB RAM and click **Forward**.



5. In the last step of the wizard, select **Customize configuration before install** and then click **Finish**.

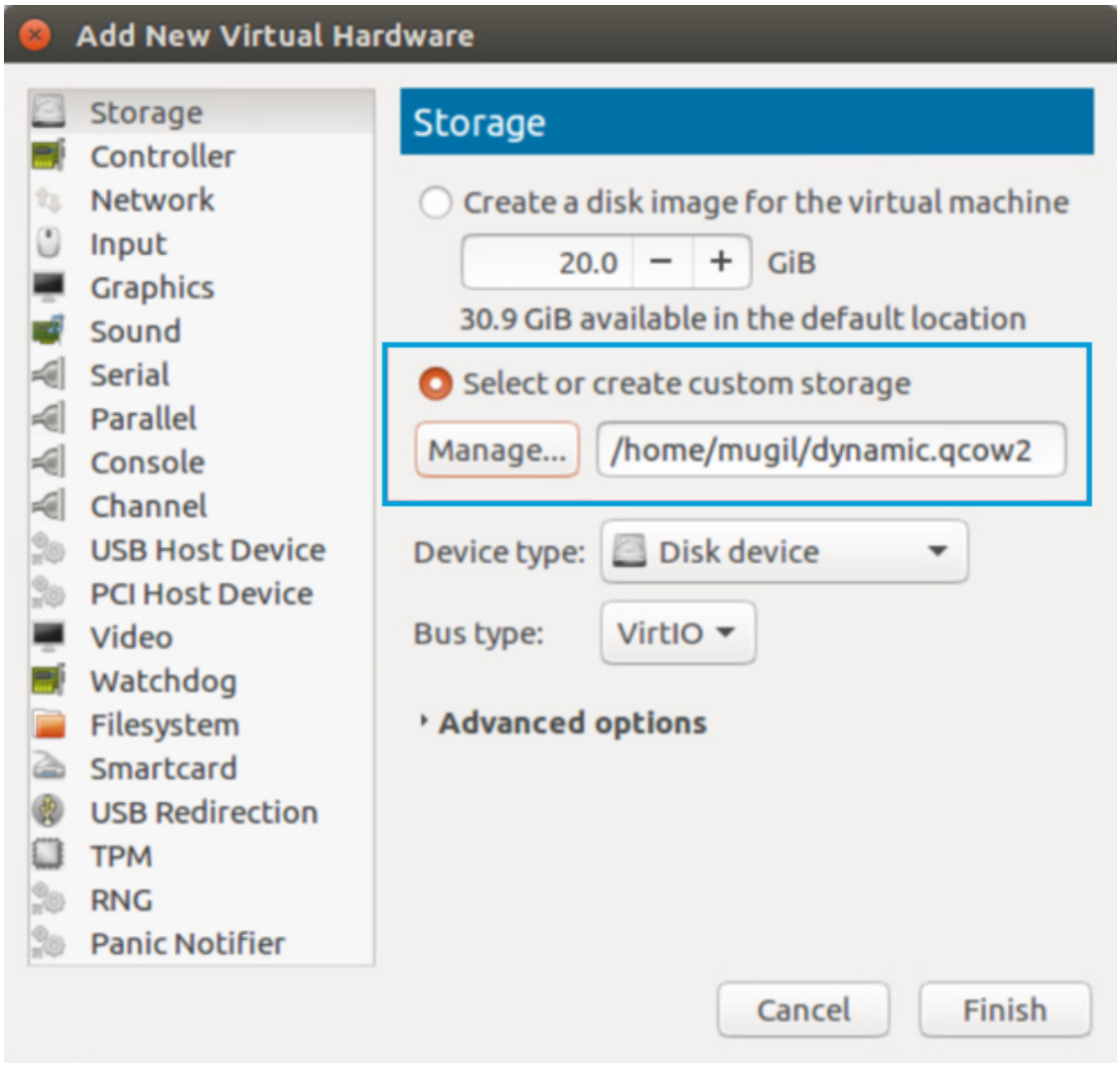

New VM
Create a new virtual machine
Step 4 of 4
Ready to begin the installation
Name: ubuntu16.04
OS: Ubuntu 16.04
Install: Import existing OS image
Memory: 1024 MiB
CPUs: 1
Storage: /home/mugil/forwarder-va.qcow2
Customize configuration before install
Network selection
Cancel
Back
Finish

6. Select **Add Hardware**.

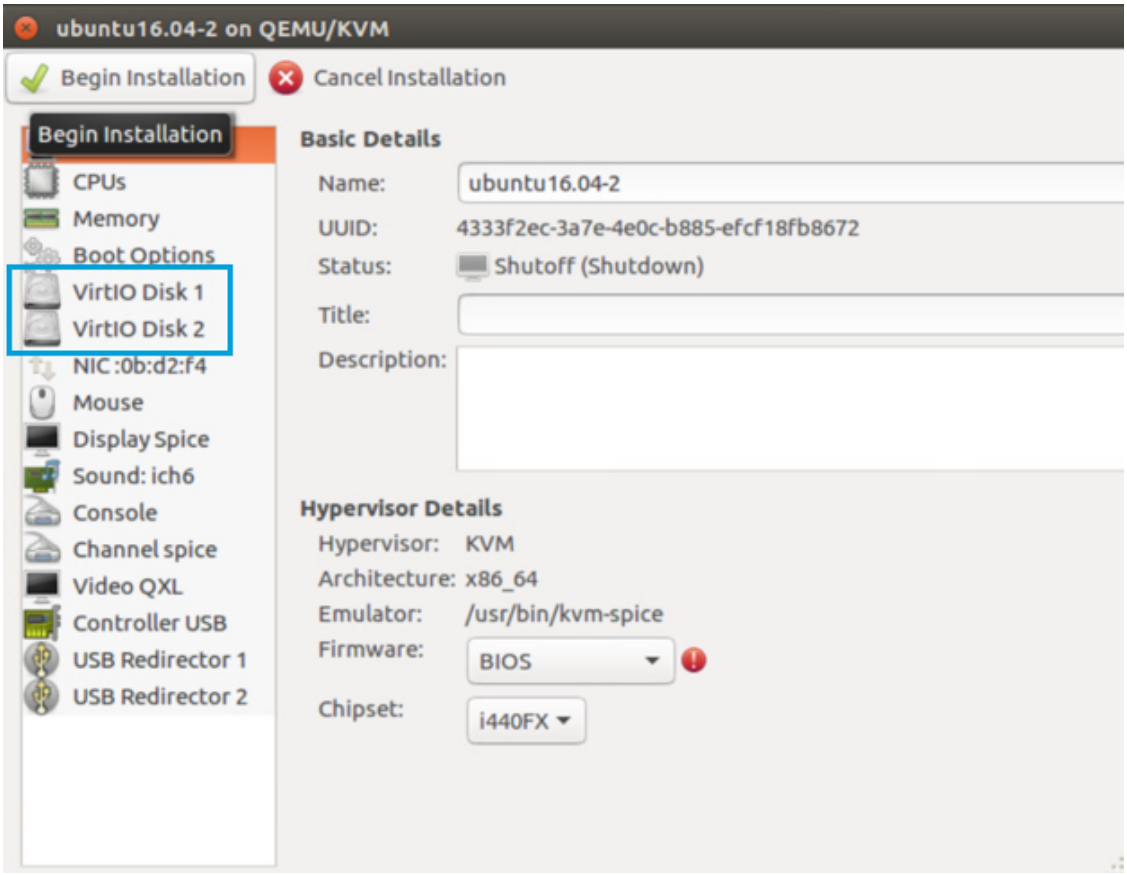


7. Select **Storage**, add or create custom storage, add the dynamic disk, and then click **Finish**.

   You should then see two disks.



8. Click **Begin installation** to create the VA.



9. If your network supports DHCP, the VA will get auto-configured with a DHCP IP address and will register to Umbrella using this IP. You can configure the VA on KVM through two mechanisms:

   - Press **Ctrl+B** on the VA console and entering the Configuration mode.

     Or

   - Initiate an SSH connection to the DHCP IP—this IP can be retrieved in Secure Access—and enter Configuration mode.

What to do next

You can now configure the VA. For information about configuring VAs, see Configure Virtual Appliances.

Deploy VAs in Nutanix

Provides instructions for completing the Deploy VAs in Nutanix workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Deploy Cisco Secure Access Virtual Appliances in Nutanix.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied in any way. Configure and set up each VA manually.

Before you begin

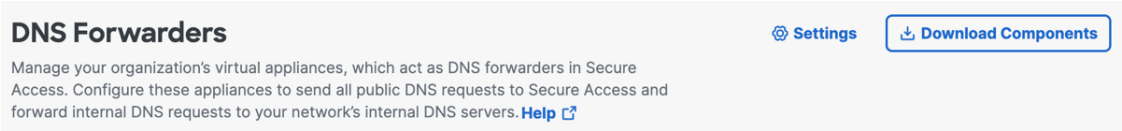
- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- Virtual Appliance deployments are supported on the current LTS version of Nutanix AHV only.

Configure Authentication for the Virtual Appliances

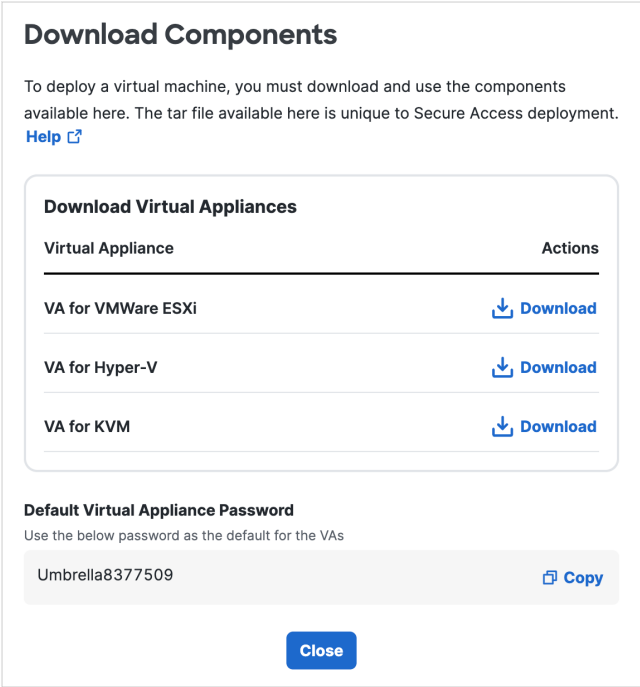
Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** button only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure

1. Navigate to **Connectors** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** for **VA for hyper-V**.



   a. Secure Access generates and downloads to your computer a .tar file unique to your deployment.

      This tar file includes:

- a .zip file containing the virtual hard disks that need to be deployed on Nutanix
- a signature file
- a Cisco public certificate to validate the signature
- a readme file

3. Extract the contents of the tar file.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. When successful, a message saying **Verified OK** will appear.

   Run:

   ```
   tar -xvf <tar filename> -C <Destination folder>
   ```

4. Extract the downloaded zip file.

   You will find two folders–`Virtual Hard Disks` and `Virtual Machines`–and a config file. Navigate to the `Virtual Hard Disks` folder and find the forwarder-va.vhd and dynamic.vhd files.

5. Log into the Nutanix AHV console, navigate to **Settings** > **Image Configuration**, and create two images (VAForwarder and VADynamic) by uploading the forwarder-va.vhd and dynamic.vhd respectively.
6. Create a new VM with at least 1 VCPU (1 core), 1 GB RAM, and 1 NIC.
7. Add a new disk using the VAForwarder image. Choose the operation **Clone from Image Service** and Bus Type as **SCSI**.
8. Remove the CD-ROM. Add another disk using the VADynamic image with operation as **Clone from Image Service** and Bus Type as **SCSI**.

   > **Note**
   >
   > The disk order is important. The VAForwarder should be Disk 0, the VADynamic should be Disk 1.

   You can now power on the VA and configure it using either the console or by initiating an SSH connection to the VA. For information about configuring VAs, see Configure Virtual Appliances.

   For more information about how to enhance throughput of the VA on Nutanix, see Enabling RSS Virtio-Net Multi-Queue by Increasing the Number of VNIC Queues.

Deploy VAs in Alibaba Cloud

Describes Deploy VAs in Alibaba Cloud in Cisco Secure Access. This guide describes how to deploy Cisco Secure Access Virtual Appliances in the Alibaba Cloud environment.

This guide describes how to deploy Cisco Secure Access Virtual Appliances in the Alibaba Cloud environment.

> **Note**
>
> You must deploy at least two Virtual Appliances (VAs) in a Secure Access Site. It is critical that these VAs are not cloned or copied. Configure and set up each VA manually.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- For information about the network requirements for deploying VAs, see Prerequisites for Virtual Appliances.
- An Alibaba account. Create your account at https://www.alibaba.com/.
- A **qemu-utils** package installed, such as Homebrew, to run the `qemu-img` and `tar` commands.
- A VA running version 3.6.1 or above. Only VAs running version 3.6.1 or above can be deployed in Alibaba.
- An SSH client (for example, PuTTY on Windows or Terminal on Macintosh) to access the VA console.

Configure Authentication for the Virtual Appliances

Before you can download the Virtual Appliance images in Secure Access, you must configure your Secure Access API keys for the Virtual Appliances in your organization. Secure Access enables the **Download Components** only after the API keys for the VAs are configured. For more information, see Configure Authentication for Virtual Appliances.

Procedure

Provides a high-level order of steps for deploying VA's in Alibaba Cloud.

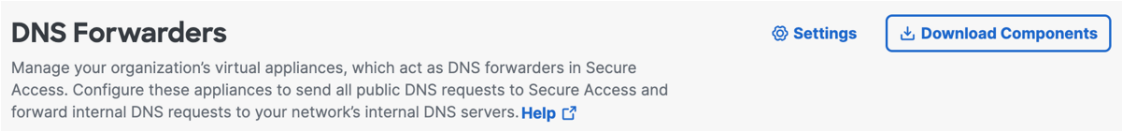
1. Download and Extract the Hyper-V Installer. This is a one time task.
2. Alibaba Cloud Setup
3. Create a Custom Image. Perform this task for each VA after performing the one-time task of preparing the VA images.
4. Deploy the Secure Access VAs from the Imported Custom Image
5. First-time Login to Secure Access VA
6. Related Topics
   a. Dual-NIC Support on the Secure Access VA
   b. IP Addressing
   c. Anycast Configuration Support
   d. DNS Performance on Alibaba ECS Instances
   e. Extensions on Alibaba ECS Instances

Download and Extract the Hyper-V Installer

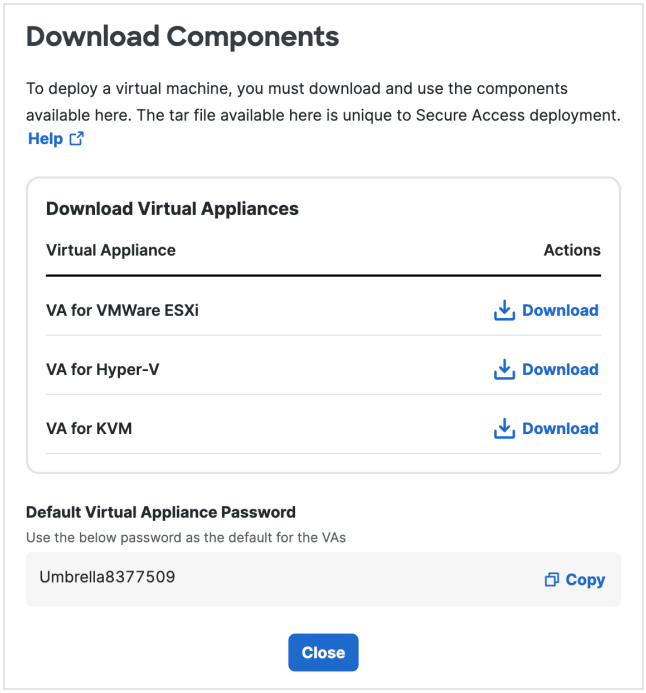
Provides instructions for completing the Download and Extract the Hyper-V Installer workflow in Cisco Secure Access. Navigate to Connectors DNS Forwarders and click Download Components.

Procedure

1. Navigate to **Connectors** > **DNS Forwarders** and click **Download Components**.



2. Click **Download** for **VA for Hyper-V**.



   Secure Access generates and downloads a tar file unique to your deployment.

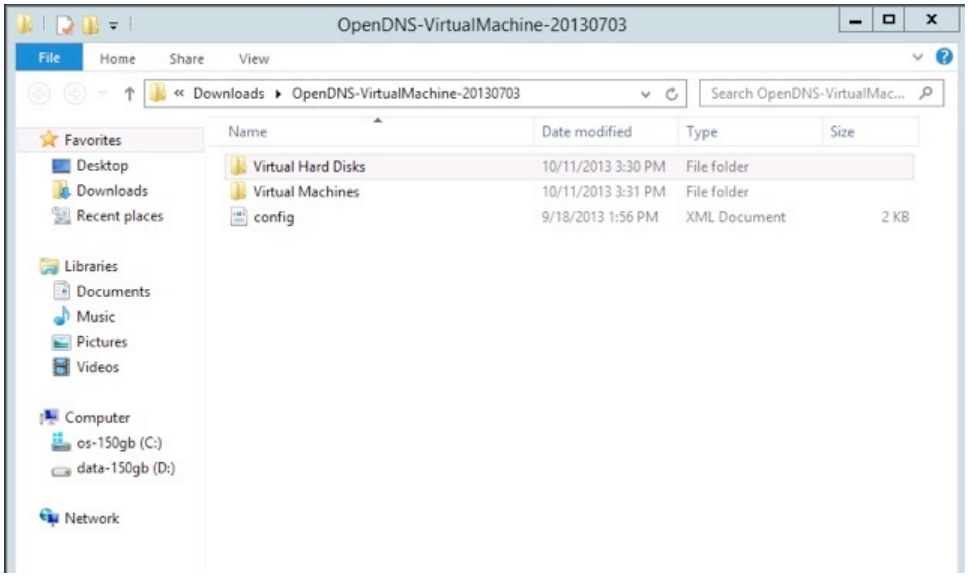
   This tar file includes:

   - a zip file containing the virtual hard disks that need to be deployed on Hyper-V
   - a signature file
   - a Cisco public certificate to validate the signature
   - a readme file

3. Extract the contents of the tar file using the command `tar -xvf <tar filename> -C <Destination folder>`.

   To verify the integrity of the downloaded file, validate the signature by following the instructions provided in the readme file. When successful, there will be a message saying “Verified OK."

4. Extract the .zip file. You'll find two folders–`Virtual Hard Disks` and `Virtual Machines`–and a `config` file.



5. In Windows Explorer, navigate to the `Virtual Hard Disks` subfolder within the extracted download folder created in Step 1.
6. Note the two VA files, `dynamic` and `forwarder-va`. Convert the forwarder-va.vhd file to .raw format:
   ```
   qemu-img convert -f vpc -O raw forwarder-va.vhd forwarder-va.raw
   ```
7. Zip the forwarder-va.raw file.

> **Note**
>
> Alibaba only allows for 5Gb uploads.

Alibaba Cloud Setup

Describes Alibaba Cloud Setup in Cisco Secure Access. This section describes the configuration requirements within Alibaba Cloud to support deploying the Secure Access VA instances to your virtual private cloud (VPC).

This section describes the configuration requirements within Alibaba Cloud to support deploying the Secure Access VA instances to your virtual private cloud (VPC). For more details on setting up a VPC and other components, please refer to Alibaba's Cloud Documentation here.

1. Create an Alibaba Virtual Private Cloud (VPC)
2. Create a Bucket for the Umbrella VAs
3. Configure a ZIP Package Decompression Rule
4. Upload the Secure Access VHD Images to the OSS Bucket

Create an Alibaba Virtual Private Cloud (VPC)

Provides instructions for completing the Create an Alibaba Virtual Private Cloud (VPC) workflow in Cisco Secure Access. A virtual private cloud (VPC) is required to deploy your Alibaba Cloud resources, such as Secure Access VAs.

A virtual private cloud (VPC) is required to deploy your Alibaba Cloud resources, such as Secure Access VAs.

Procedure

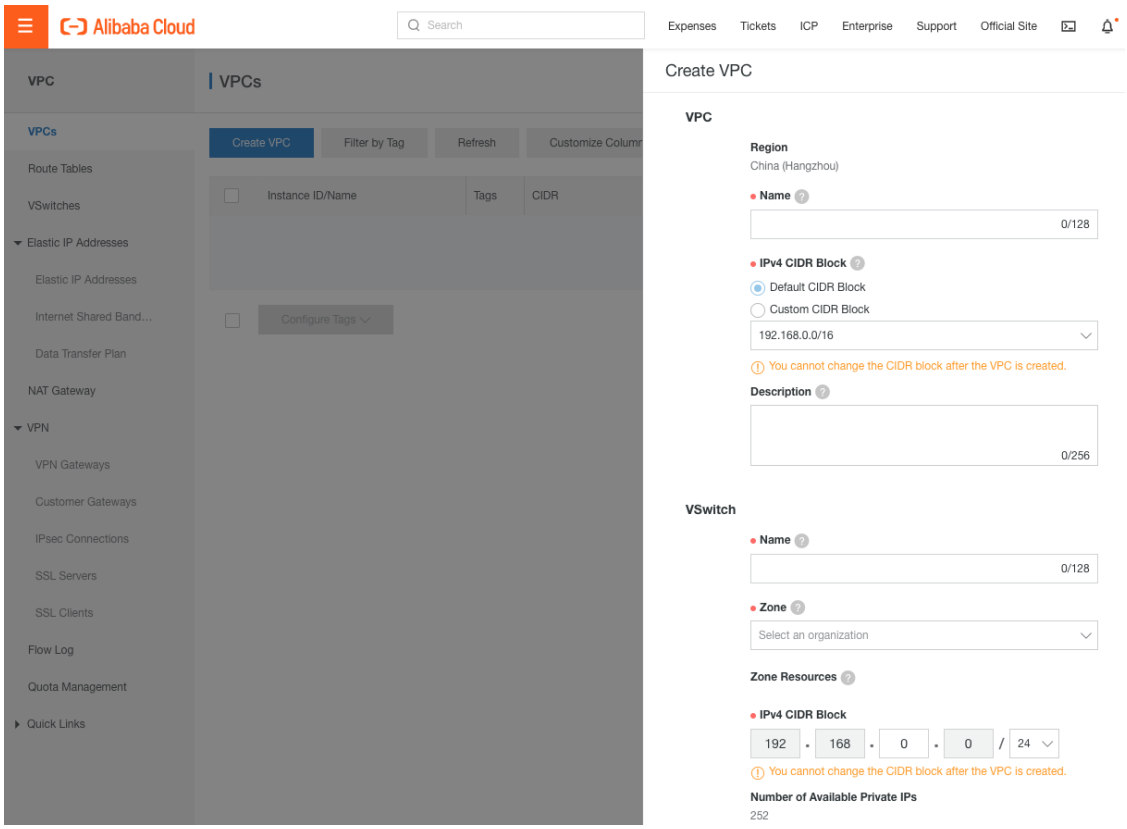
1. Log in to your Alibaba Cloud Account and log on to the VPC console.
2. In the top navigation bar, select the region where you want to deploy the VPC.

> **Note**
>
> The VPC and the cloud resources that you want to deploy in the VPC must belong to the same region.

3. On the VPCs page, click **Create VPC**.
4. On the **Create VPC** page, set the required parameters and click **OK**.

What to do next

To find more information about this, please click here.



Create a Bucket for the Secure Access VAs

Provides instructions for completing the Create a Bucket for the Secure Access VAs workflow in Cisco Secure Access. On the Alibaba Cloud Console home page, select Object Storage Service (OSS).

An Object Storage Service (OSS) bucket is needed. Alibaba OSS is a secure, cost-effective, and highly reliable cloud storage service that allows for the storage of large amounts of data.

Procedure

1. On the Alibaba Cloud Console home page, select Object Storage Service (OSS).
2. In the left-side navigation pane, click **Buckets**. On the Buckets page, click **Create Bucket**.
3. In the **Create Bucket** panel, enter the **Bucket Name** and **Region**.

   The bucket must be in the same region as the VPC in which the Secure Access VAs are to be deployed. Keep the default settings for other parameters or configure the parameters after the bucket is created.
4. Click **OK**.

   After the bucket is created, the **Created** message is displayed.

Configure a ZIP Package Decompression Rule

Provides instructions for completing the Configure a ZIP Package Decompression Rule workflow in Cisco Secure Access. Alibaba Cloud accepts uploads of objects up to 5 GB in size using the OSS console.

Alibaba Cloud accepts uploads of objects up to 5 GB in size using the OSS console. Because the Secure Access Forwarder VA is larger than 5 GB, the forwarder-va.vhd file needs to be converted to .raw format and then compressed to a zip file, as described in Download and Extract the Hyper-V Installer.

Procedure

1. In the left navigation pane of the OSS console, click **Buckets**. On the Buckets page, find and click the desired bucket.
2. In the left navigation tree, choose **Data Processing** > **Decompress ZIP Package**.
3. Click **Start Activation** and follow the prompts.
4. Once activation is complete, go to the bucket and click **Decompress ZIP Package**. In the Decompress ZIP Package panel, configure the following parameters:
   a. **Service Authorization** - Authorize Function Compute to read data from and write data to OSS and to execute functions. Click **Authorize**. Complete authorization on the page that appears.
   b. **Authorize Trigger** - Authorize OSS to access Function Compute. Click **Authorize**. Complete authorization on the page that appears. If OSS is authorized to access Function Compute, the Trigger Role parameter is displayed instead of the Authorize Trigger parameter.
   c. **Destination Directory** - To store the objects extracted from a ZIP package in a subdirectory that has the same name as the package in the destination directory, select **Add the compressed object name to the destination directory**.
5. Click **OK**.

What to do next

Now that the bucket is created, click **Go to Bucket**. Alternatively, click **Buckets** in the left-side navigation pane and click the name of the created bucket.

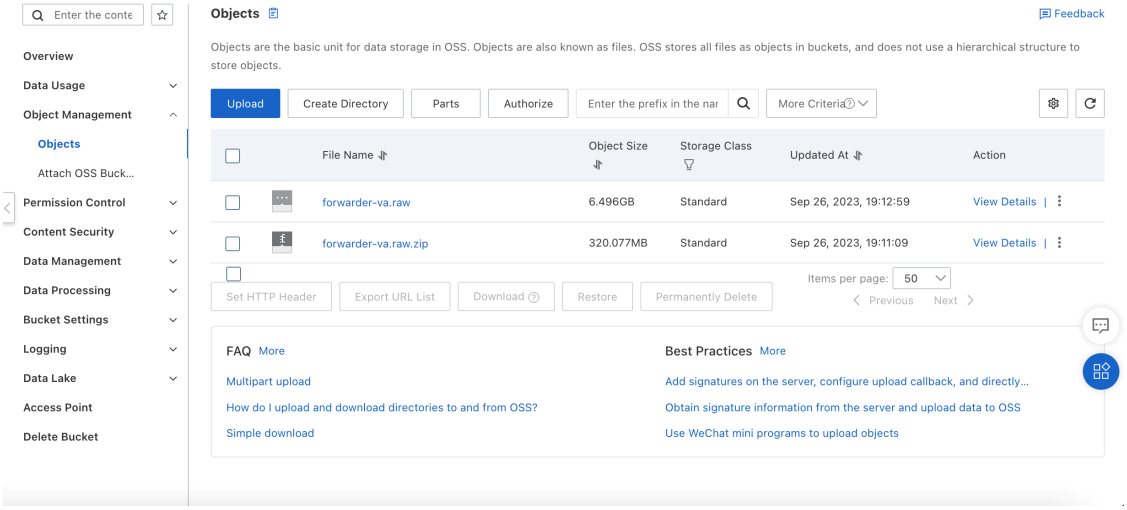
Upload the Secure Access VHD Images to the OSS Bucket

Provides instructions for completing the Upload the Secure Access VHD Images to the OSS Bucket workflow in Cisco Secure Access. Upload the Secure Access VHD images that were downloaded in Download and Extract the Hyper-V Installer to your bucket.

Upload the Secure Access VHD images that were downloaded in Download and Extract the Hyper-V Installer to your bucket.

Procedure

1. Select your bucket, choose **Files** > **Upload**, and **click here to upload**.
2. Select the compressed forwarder-va zip file on your local drive. Wait for the automatic decompression to be triggered before continuing. The forwarder-va.raw file should be seen in the table on the **Upload** page if it is uploaded successfully.



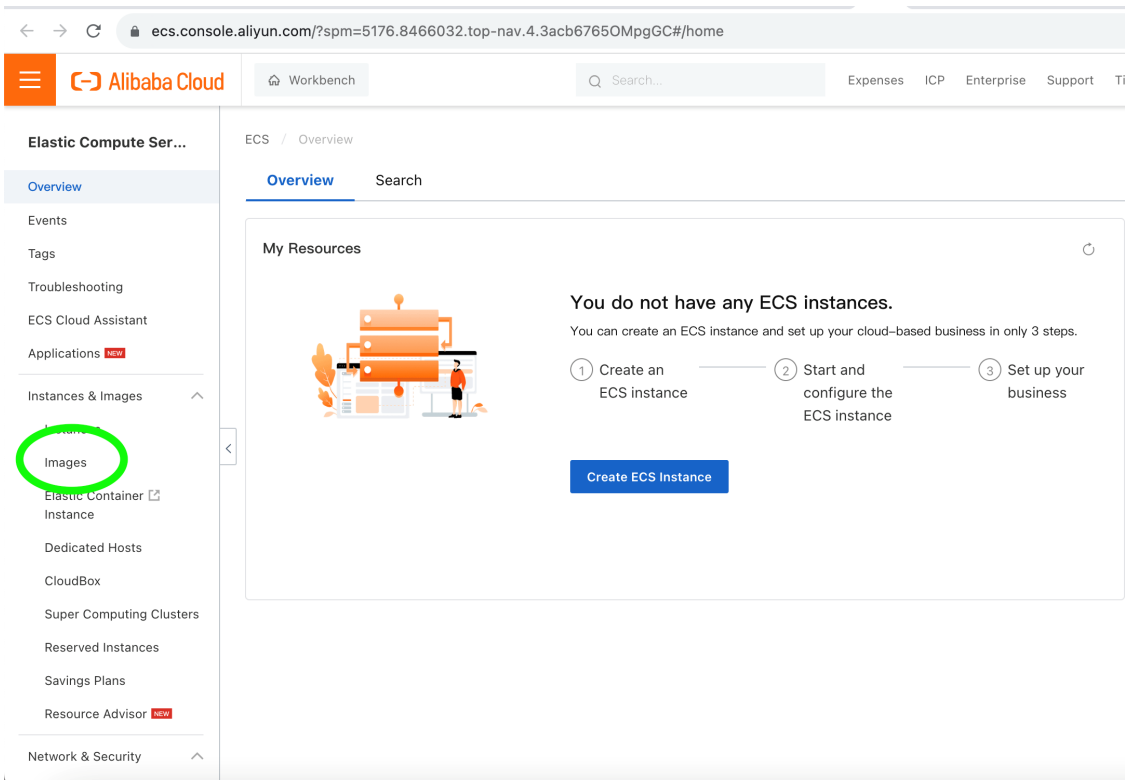
3. Select the dynamic.vhd on your local drive. Given the small size of this file, no conversion or compression is required.
4. The file will be displayed in the table on the **Upload** page if it is uploaded successfully.
5. Click **View Details**, the click **Copy File URL**. This URL is needed in later steps when creating a custom image.

Create a Custom Image

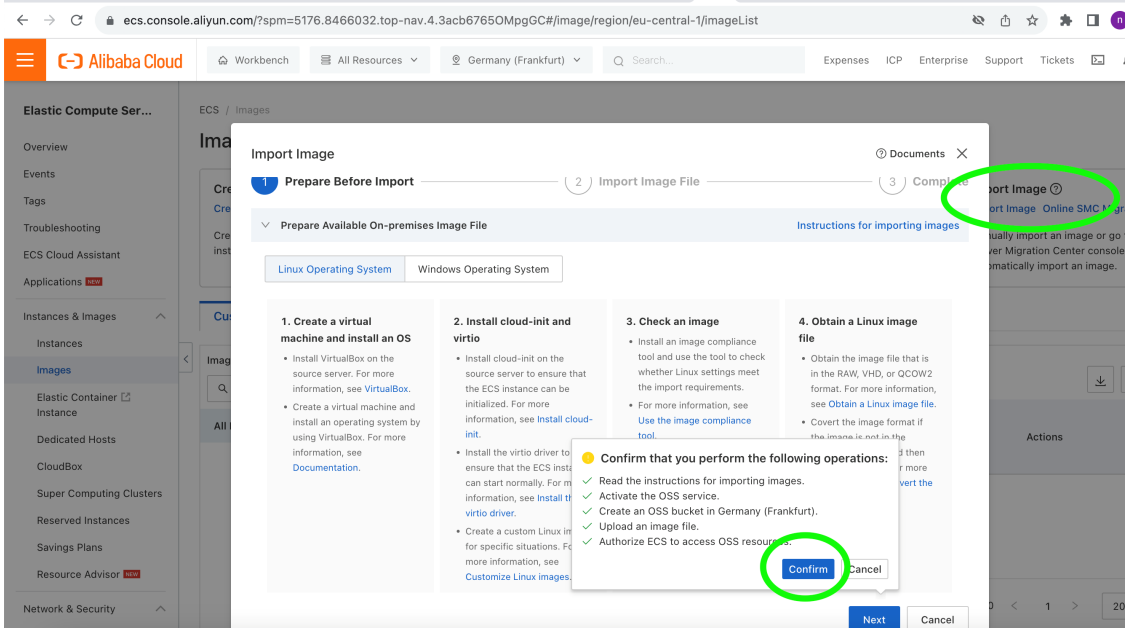
Provides instructions for completing the Create a Custom Image workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Select the Alibaba Elastic Compute Service (ECS).
2. Select **Instances & Images** > **Images** > **Custom Images**.

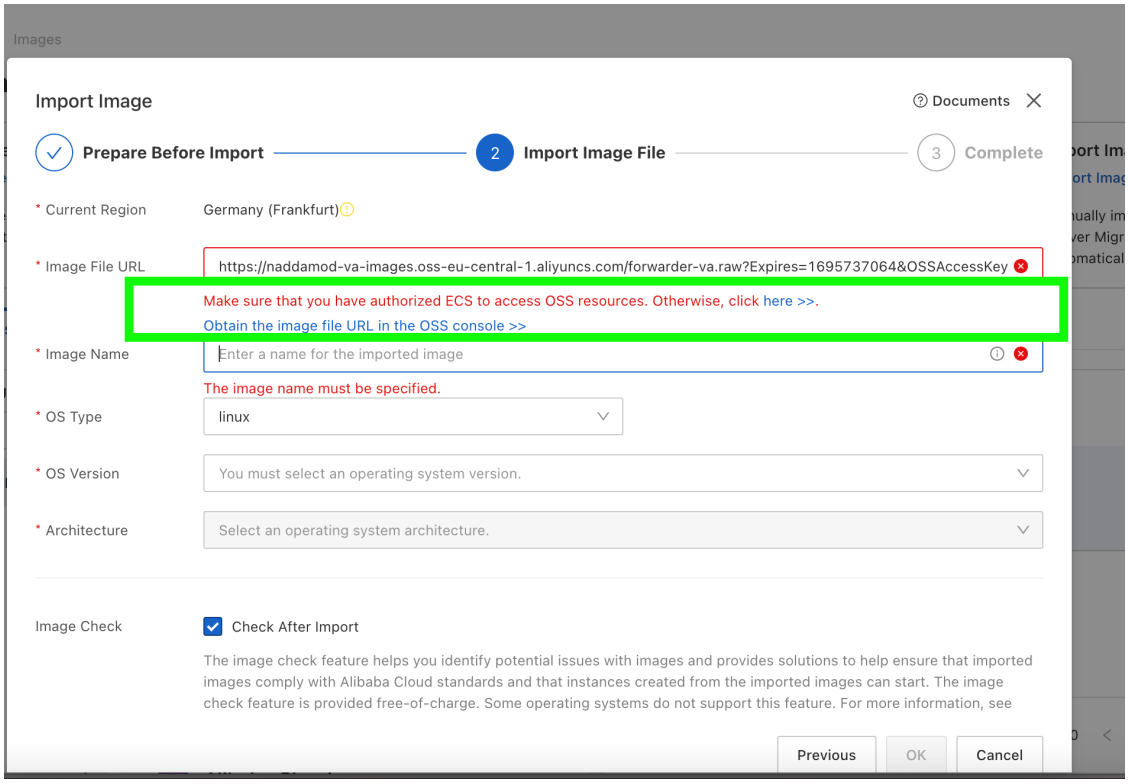


3. Click **Import Image**.

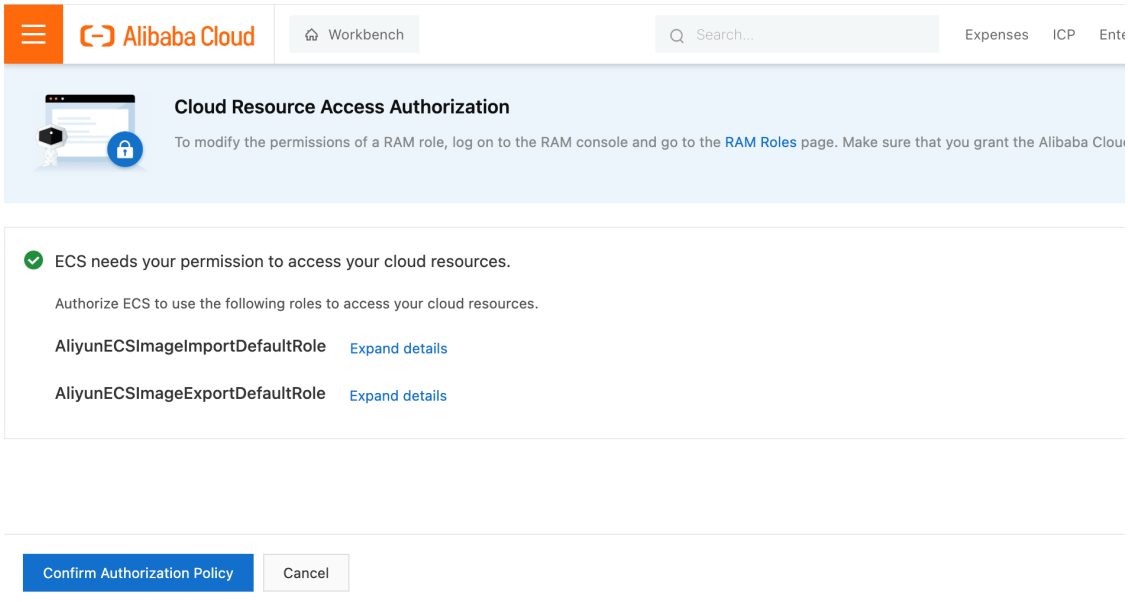


4. Paste the forwarder-va.raw URL in the **Import Image** window. See Upload the Secure Access VHD Images to the OSS Bucket for where to find the URL.

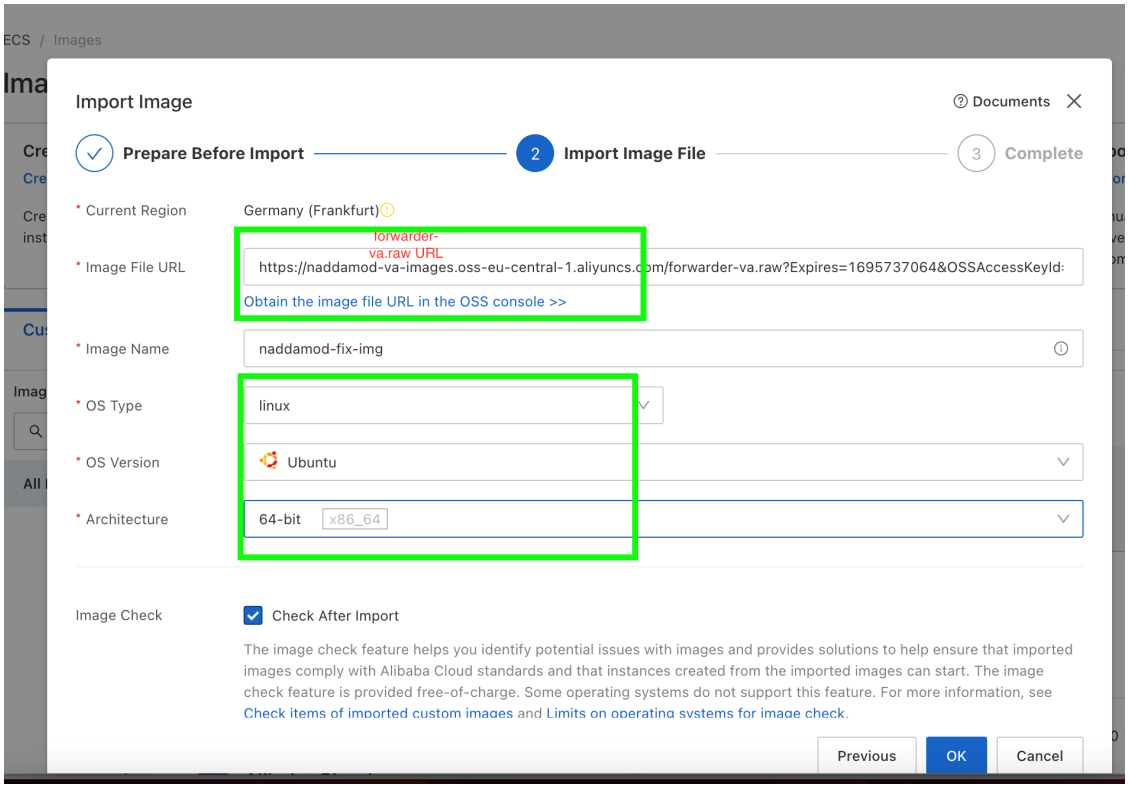
> **Note**
>
> If the following error is seen, ECS does not have access to the OSS resources. Enable access by clicking the **here** hyperlink shown.



5. If necessary, click **Confirm Authorization Policy**.



6. Repeat the **Import Image** action and fill the necessary fields as below.

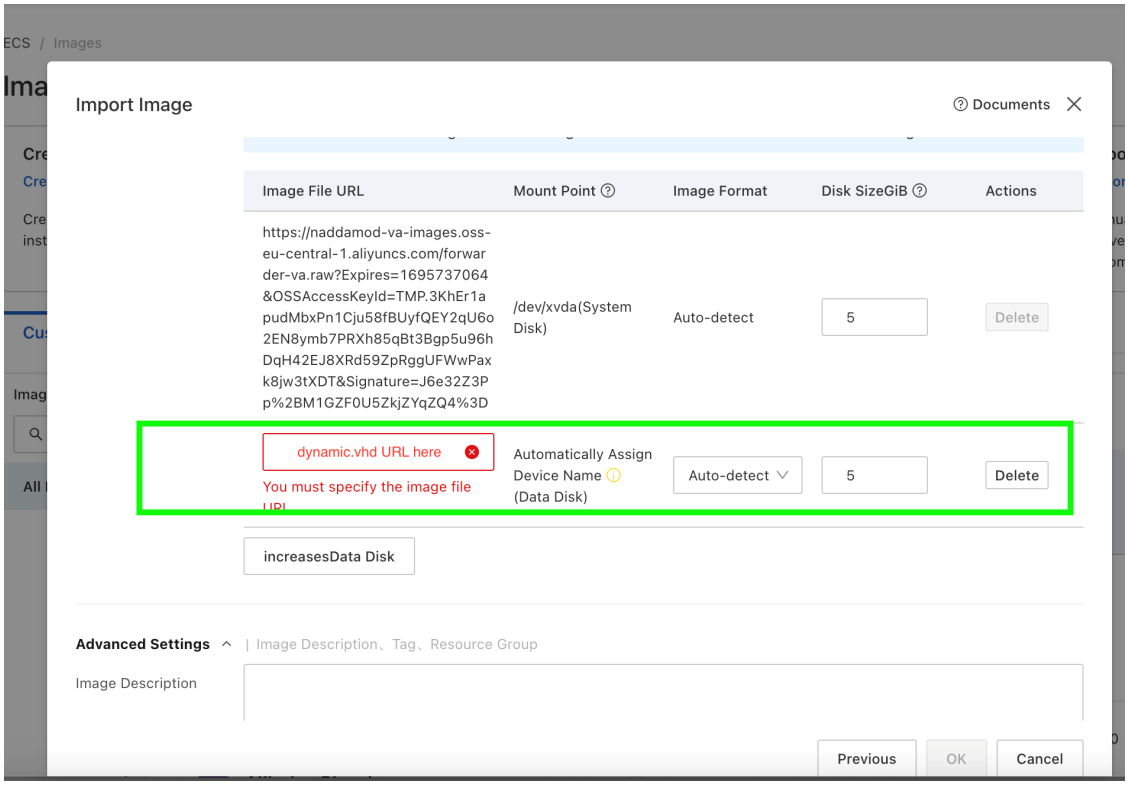


7. Check the **Configure Disk Attributes** box and adjust the **Disk SizeGiB** setting.

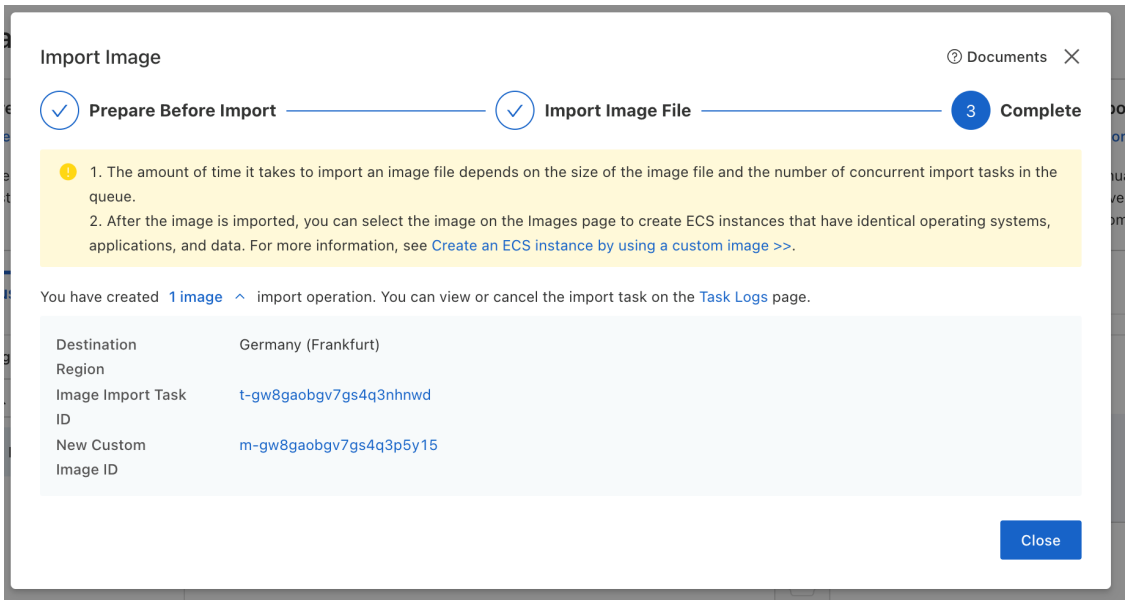
> **Note**
>
> Make sure that the forwarder-va.raw disk size is 6.5 GB.

8. Repeat for the dynamic.vhd file.

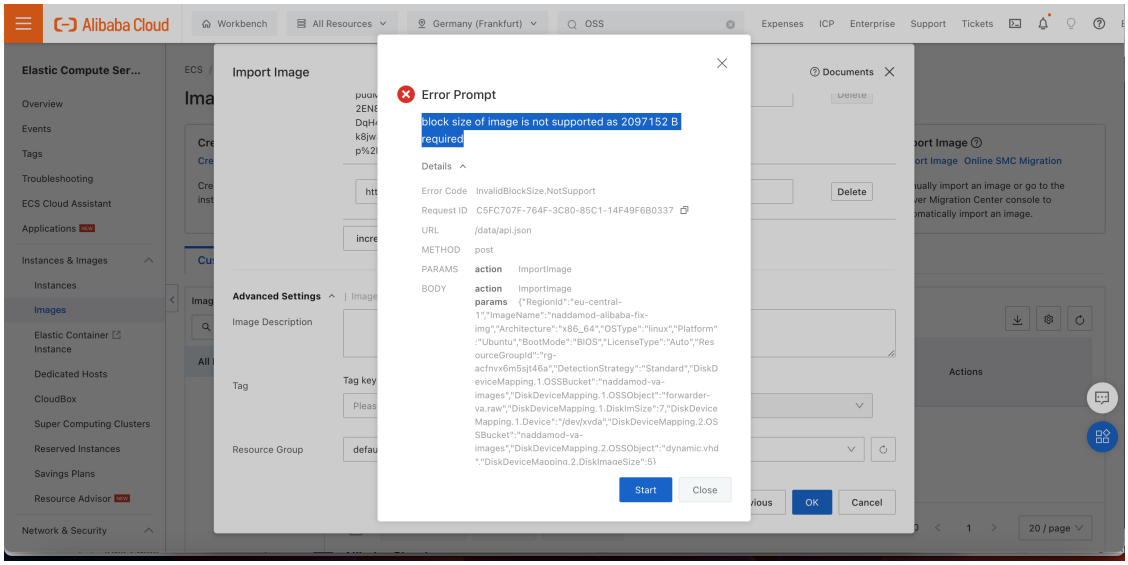
> **Note**
>
> Make sure that the dynamic.vhd disk size is 20 MB.



9. If the image is successfully created, the following window is shown.



10. Note that if the forwarder-va.vhd is uploaded instead of .raw image, or if the size is not supported, the following error is shown.



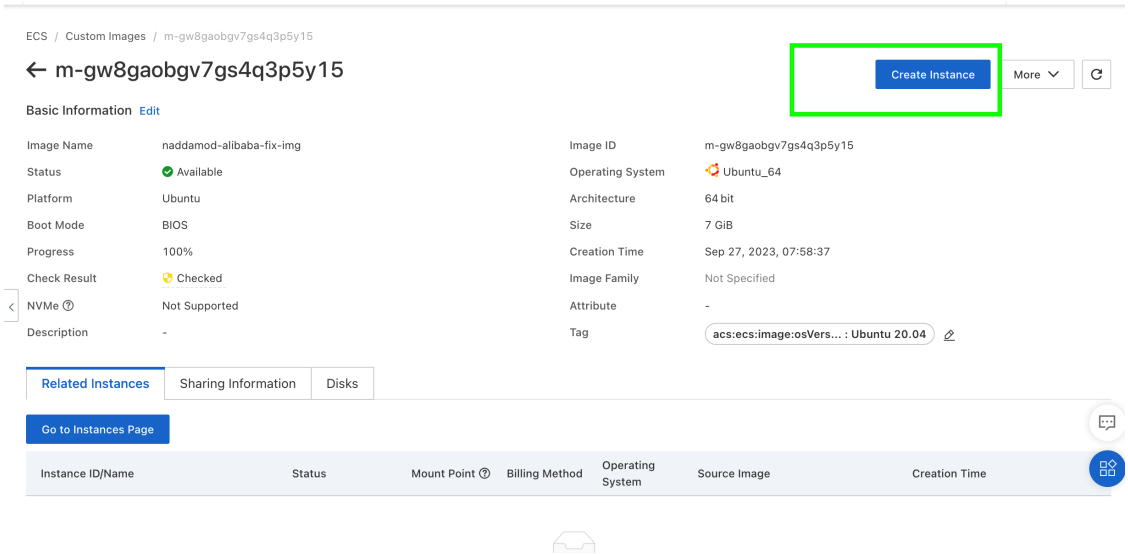
Deploy the Secure Access VAs from the Imported Custom Image

Provides instructions for completing the Deploy the Secure Access VAs from the Imported Custom Image workflow in Cisco Secure Access. An Elastic Compute Service (ECS) image provides the information that is required to create an ECS instance.

An Elastic Compute Service (ECS) image provides the information that is required to create an ECS instance. An image must be specified when creating an ECS instance. An image is a copy of data from one or more disks. An instance image can contain data from only the system disk or from both the system disk and data disks.

Procedure

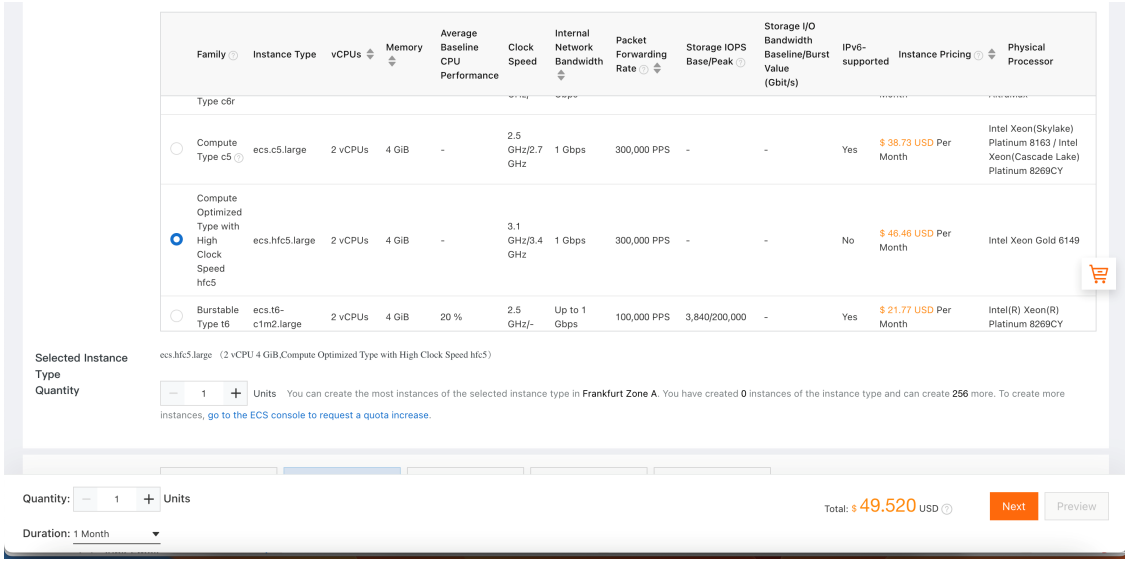
1. Navigate to **Elastic Compute Service** > **Instances**. Click **Create Instance**.



2. Complete the following Basic Configuration settings:
   a. Select the **Region and zone**. Select a region that is close to your geographical location to reduce latency. After an instance is created, the region and the zone of the instance cannot be changed.

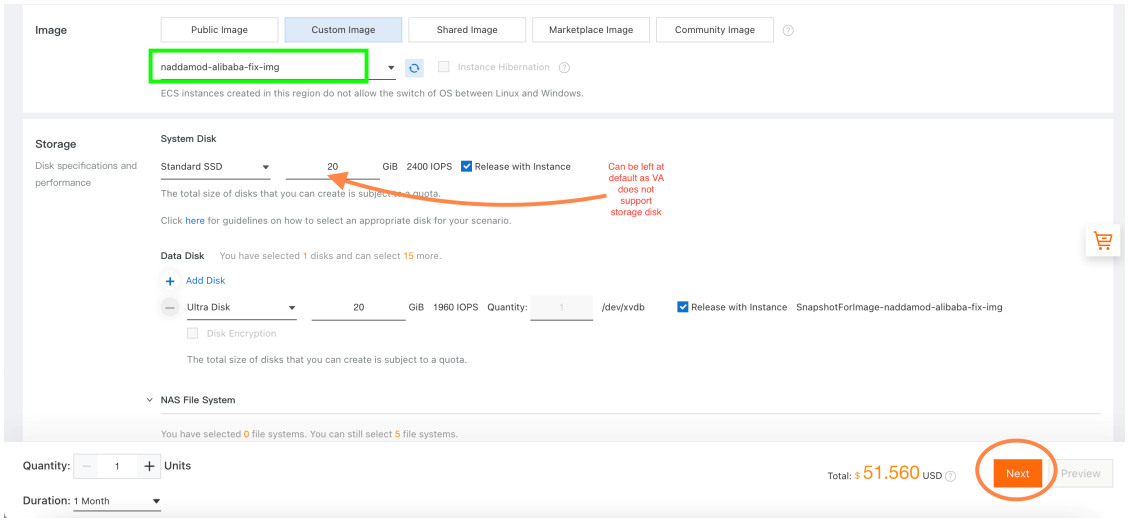
b. Select the **Instance type**. Different instance types have different CPU, RAM and throughput capacity.

> **Note**
>
> It is recommended to have an instance type having a minimum capability of **ecs.c6.xlarge** for optimal DNS performance, with enhanced clock speed as the VA is a DNS proxy.



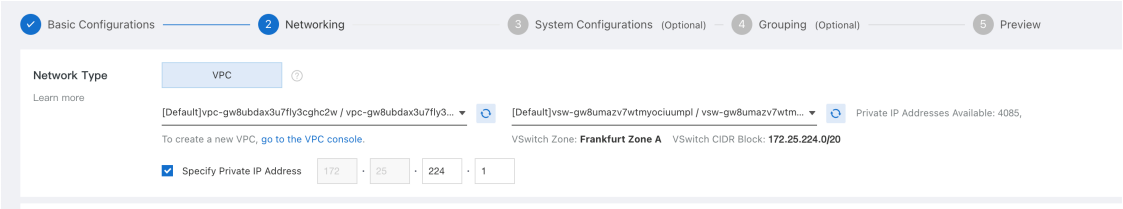
3. Select the Custom image, Duration and click **Next**.

> **Note**
>
> The **System Disk** size increase will not help scale the VA as dynamic disk size change is not supported. The VA only supports a 7 GB system and 1 GB data disk.

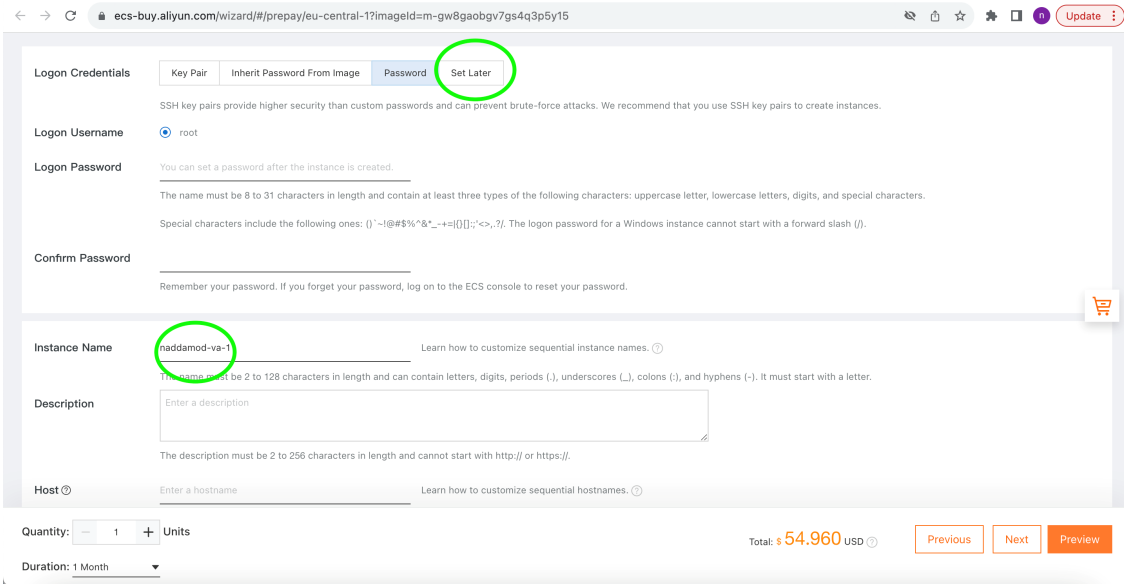


4. Select the VPC and VSwitch as per the topology. In this example, default values are selected.

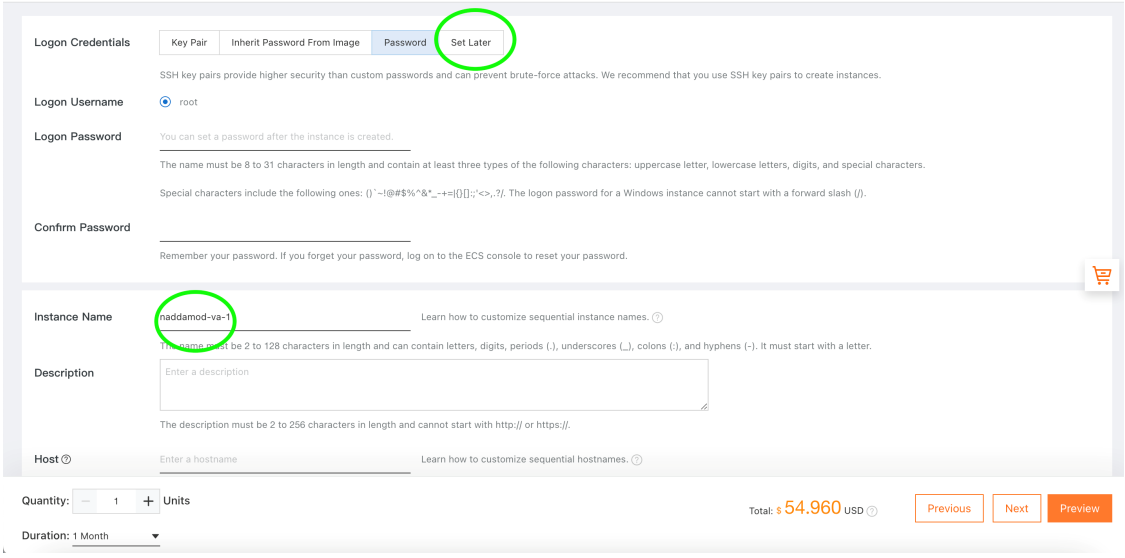
The Virtual Appliance will have a private IP with which it will be registered with the dashboard. Specify the private IP so that it does not change on power cycle.



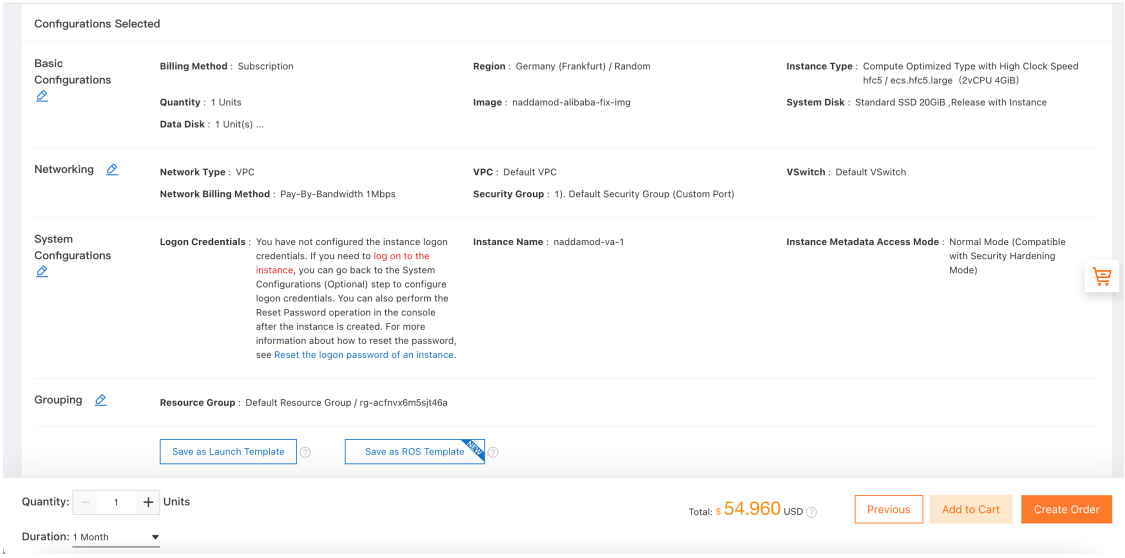
5. If a **Security Group** has already been created, the same can be reused. This example proceeds with basic configuration and enable the ports later as per VA pre-requisites.



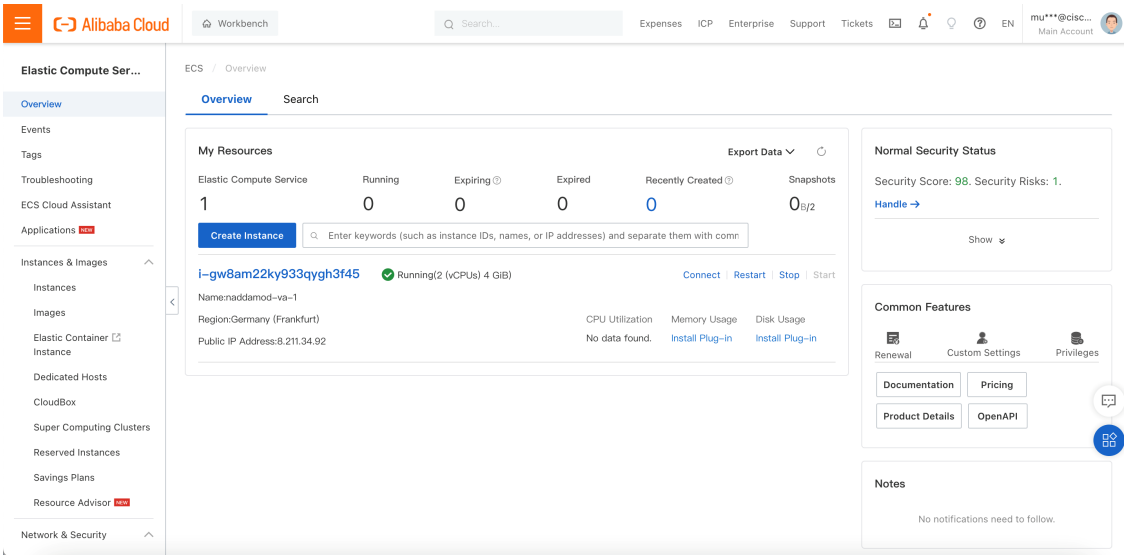
6. Alibaba cloud does not support password setting for users other than "root", so the **vmadmin** password cannot be set through the Cloud and it has to be **Set Later** through SSH or console access.



7. Select the **Resource Group** in the next window. In this example, the **Default Resource Group** is used.
8. Click **Create Order** and proceed.



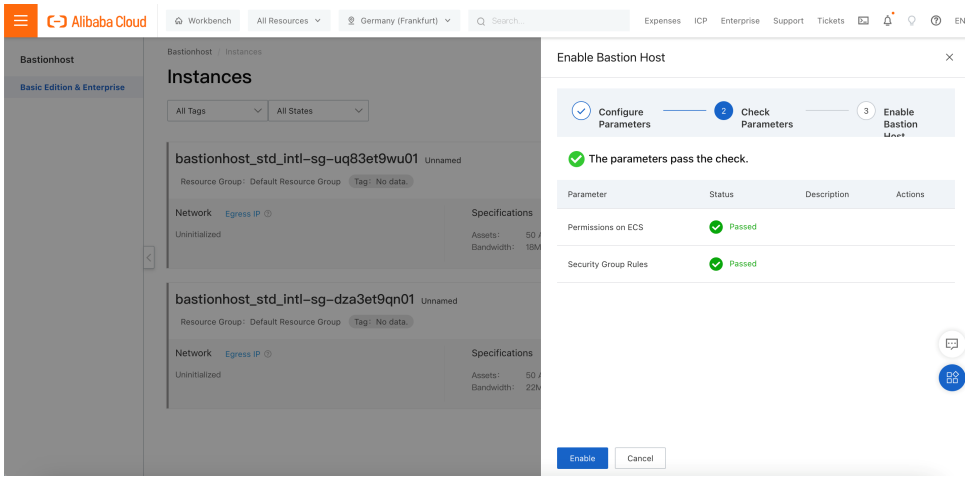
9. Once the subscription is created, the instance will show up on the ECS console.



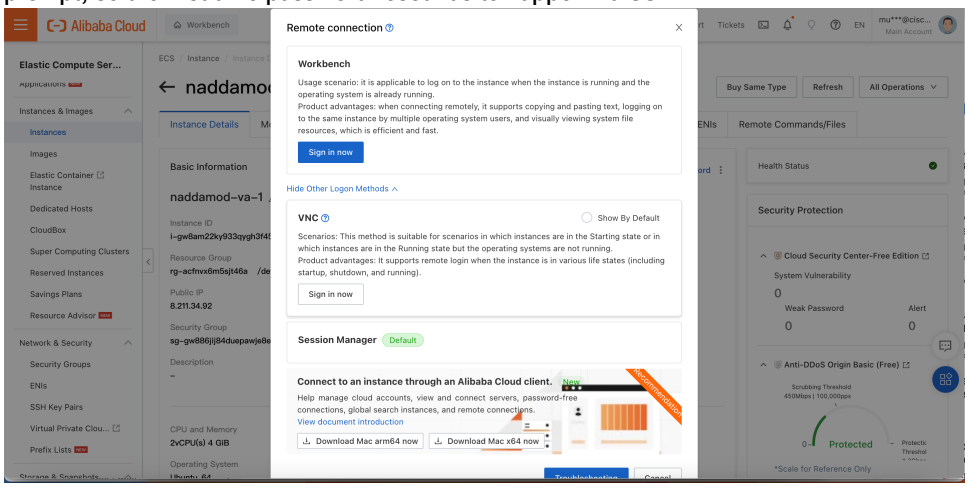
What's Next

Describes What's Next in Cisco Secure Access. Go to the newly created instance and edit Security Group rules; see the virtual appliances (VA) network requirements.

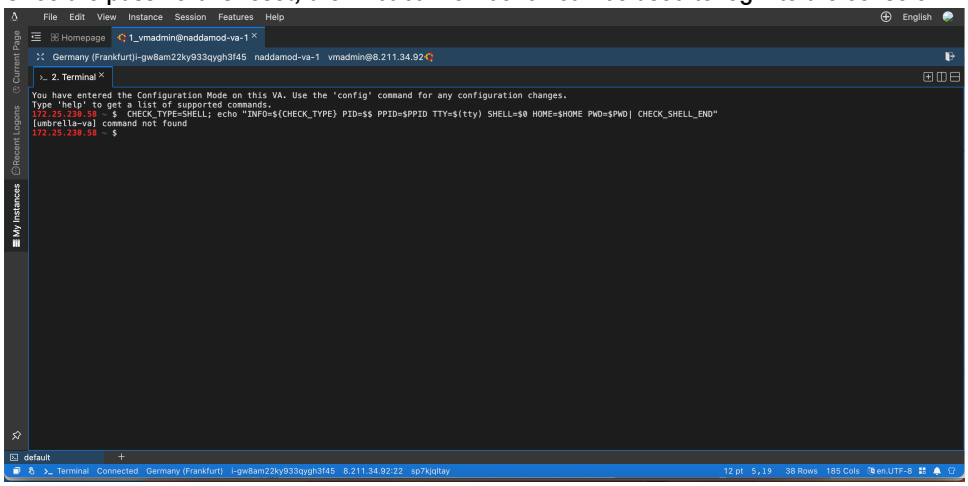
- Go to the newly created instance and edit Security Group rules; see the virtual appliances (VA) network requirements.
- The **vmadmin** password can be reset by doing remote SSH via the public IP as port 3389 is allowed by default.
- If the instance does not have a public IP, a Bastion host has to be created in the same region to access it via Private IP as per Alibaba documentation.



- Please note that connecting to the VA through the Alibaba Cloud workbench will fail due to the change password prompt, so the first time password reset has to happen via SSH.



- Once the password is reset, the Alibaba workbench can be used to login to the console.



- After the password is set, you can SSH to the VA via the ECS Workbench as well.

First-time Login to Secure Access VA

Provides instructions for completing the First-time Login to Secure Access VA workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

There are three ways to do the first-time login to the Secure Access VA:

Procedure

1. If the VA has a public IP associated, use the default **vmadmin/<orgid>** credentials and reset the password.
2. If the VA is inside private network, create another OAM VM (not the Alibaba bastion) inside the same network and SSH through the private IP using the **vmadmin/<orgid>** credentials and reset the password.
3. ECS instances can also be added to a *Bastion host enterprise edition* available on the Alibaba cloud; refer to the following guidelines. When doing so, please note that the password should be reset from the ECS instance UI also before trying to login through the Bastion. Please note that even though the instance password is reset through UI, it won't apply to the instance as we do not have a root account.

Related Topics

Describes Related Topics in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Dual-NIC Support on the VA
- IP Addressing
- Anycast Configuration Support
- DNS Performance on Alibaba ECS Instances
- Extensions on Alibaba ECS Instances

Dual-NIC Support on the VA

Describes Dual-NIC Support on the VA in Cisco Secure Access. In the Alibaba Cloud elastic network interfaces (ENIs) are logical networking components that represent virtual NICs, providing network connectivity and IP addresses for Elastic Compute Service (ECS) instances deployed in virtual private clouds (VPCs).

In the Alibaba Cloud elastic network interfaces (ENIs) are logical networking components that represent virtual NICs, providing network connectivity and IP addresses for Elastic Compute Service (ECS) instances deployed in virtual private clouds (VPCs).

The Secure Access VA supports a dual-NIC configuration. This dual-NIC configuration is intended to enable DMZ deployment of a VA for traffic segregation with one network interface being used for outbound communication and the other network interface used for internal communication.

There is no change to existing behavior if the VA is deployed with a single NIC. Configuring more than two NICs on the VA is not supported.

For more information about Secure Access Dual-NIC support and how to configure Alibaba ENIs, see the following:

- Configure Dual-NIC Support on the VA
- Elastic Network Interfaces

Note: Do not connect more than one ENI the same VSwitch. Network issues will result.

IP Addressing

Describes IP Addressing in Cisco Secure Access and explains General Guidelines and Support for IPv6 Addressing. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

General Guidelines

The Secure Access VA supports both IPv4 and IPv6 addressing (dual stack). However there are some observations on the Alibaba cloud regarding IP addressing:

- While the Alibaba ECS ENI supports multiple private IP address, please note that the Secure Access VA only supports a single IPv4 or Single IPv4 + IPv6 pair per ENI.
- One private IPv4 and one private IPv6 address can be added to the Secure Access VA.

- The Alibaba Cloud is not supporting public IPv6 address to ECS instances.
- An IPv6 gateway can be set up at the VPC level and establish connectivity to Secure Access global IPv6 resolvers. However, it has been observed during testing that IPv6 packets are not getting a response even after setting up the gateway. This has been observed in the Germany Frankfurt Region.

Support for IPv6 Addressing

The following are observations regarding IPv6 addressing on the Alibaba Cloud:

- The IPv6 address range should be enabled on the VSwitch.
- By default, when creating an Elastic Compute Service (ECS) instance, an IPv4 address instead of an IPv6 address is assigned to the instance. To have the instance communicate over IPv6, configure an IPv6 address for the instance.
- IPv6 addressing is not supported on every ECS instance types. It depends on system resources selected during deployment. Refer to ECS instance type family.
- See Configure IPv6 addresses for information on how to configure an IPv6 address for the instance.

Anycast Configuration Support

Describes Anycast Configuration Support in Cisco Secure Access. The Umbrella VA enables the use of Anycast DNS addressing within an enterprise.

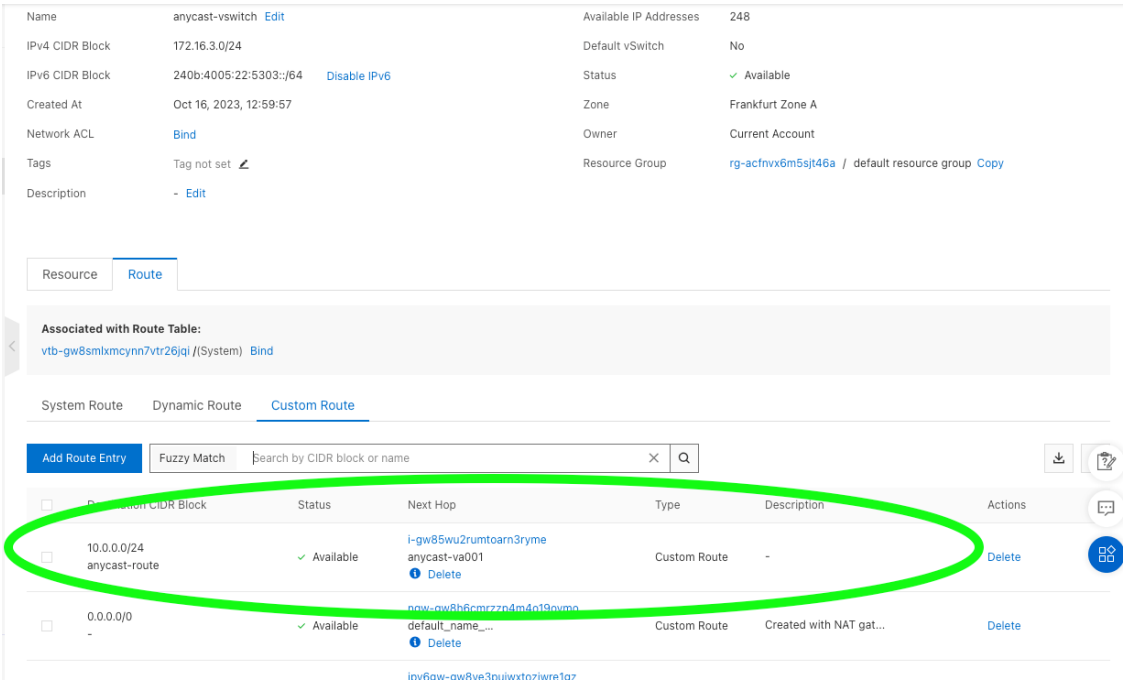
The Umbrella VA enables the use of Anycast DNS addressing within an enterprise.

The VA currently supports enabling Anycast using the BGP protocol. This requires support for BGP on the VA's neighboring router, or any router that is reachable from the VA within 255 hops. See the Configure Anycast topic for information about how to configure Anycast on the VA.

In addition, keep the following in mind when configuring Anycast on the Alibaba cloud:

- Configure an additional route on the VSwitch for the Anycast IP address for packets with the destination IP as Anycast.
- The Anycast IP/network can be routed only per single ECS or ENI per VSwitch, where the next hop is the VA instance on which Anycast is enabled and 10.0.0.5 is the Anycast IP.

> **Note**
>
> VAs participating in anycast DNS should belong to different VSwitches or different networks; the following image shows the route table of a VSwitch configured with an Anycast route.



DNS Performance on Alibaba ECS Instances

Describes DNS Performance on Alibaba ECS Instances in Cisco Secure Access. Different instance types have different CPU, RAM and throughput capacity.

Different instance types have different CPU, RAM and throughput capacity. Latency and throughput testing was performed on the following instances using dnsperf. The results captured after running the test for 1 minute are collected in the following table.

From these statistics, it is recommended to have an instance type having a minimum capability of **ecs.c6.xlarge** for optimal DNS performance. Refer to the Alibaba Cloud Instance family documentation for information on instance configurations.

Instance Type	Maximum DNS Throughput
ecs.c6.large	2000 qps
ecs.c6.xlarge	5000 qps
ecs.c6.2xlarge	10000 qps
ecs.hfc6.large	2200 qps
ecs.g6e.large	3000 qps

Extensions on Alibaba ECS Instances

Describes Extensions on Alibaba ECS Instances in Cisco Secure Access. Alibaba ECS instance supports installing agents/plugins for monitoring purpose, example CloudMonitor argusagent.

Alibaba ECS instance supports installing agents/plugins for monitoring purpose, example CloudMonitor argusagent. It is not recommended to do so as it puts the VA under risk for root partition exhaustion. On a newly deployed VA instance, the memory usage is 66 % due to the aliyun default packages installation.

Configure Virtual Appliances

Describes Configure Virtual Appliances in Cisco Secure Access. Configure your Cisco Secure Access Virtual Appliances (VAs) deployed in VMWare, Hyper-V, KVM, Azure, AWS, Google Cloud Platform, Nutanix, or Alibaba Cloud.

Configure your Cisco Secure Access Virtual Appliances (VAs) deployed in VMWare, Hyper-V, KVM, Azure, AWS, Google Cloud Platform, Nutanix, or Alibaba Cloud.

Prerequisites

- Deploy Virtual Appliances in your environments. For more information, see Deploy Virtual Appliances.

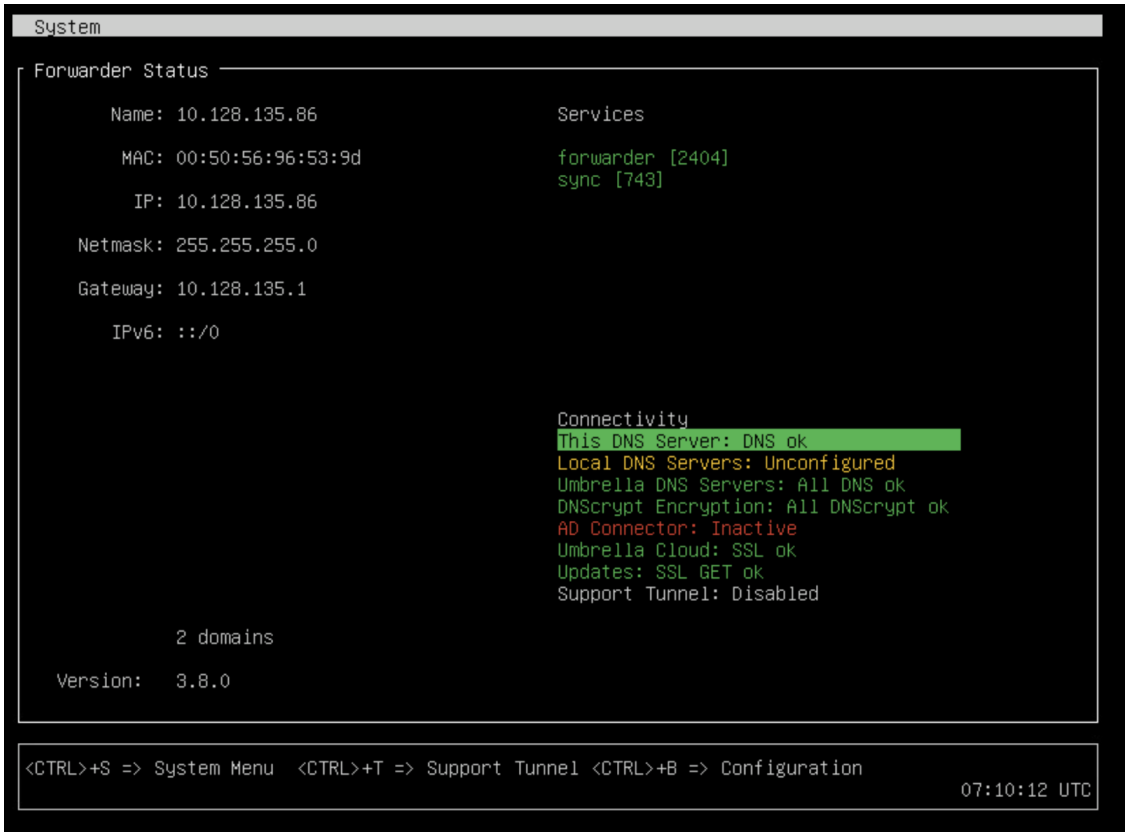
Enter Configuration Mode on a VA Deployed on VMware, Hyper-V, or KVM

Provides instructions for completing the Enter Configuration Mode on a VA Deployed on VMware, Hyper-V, or KVM workflow in Cisco Secure Access. When you open the VA in your preferred hypervisor's console, and you'll see a configuration menu.

When you open the VA in your preferred hypervisor's console, and you'll see a configuration menu. As seen in the lower right corner, the system time is set to UTC by default. This will not affect your DNS, network, or hypervisor.

> **Note**
>
> To access the VA console efficiently, use a native application (such as VMware vSphere Client, VMware Remote Console, or RDP).

If you have deployed the VA in a network that supports DHCP, the VA is automatically assigned a DHCP IP address and registers to Secure Access using this IP. This IP address appears on the configuration and in Secure Access.



Procedure

1. Press **Ctrl+B**. When prompted, provide a password for configuration changes.

   Tip

   Using the numeric lock or the number pad on your keyboard may return incorrect characters. You must change the password when you enter Configuration Mode. Your password must be at least 15 characters long, include at least one lowercase character, one uppercase character, one digit, and one special character. Your password cannot be the same as your last password.

   Note

   `Umbrella<OrgID>` should be set as the default password for the VA. Your Org ID can be retrieved from the dashboard URL in your address bar. For example, if your Org ID is `2406960`, the default password for the VA would be `Umbrella2406960!`. For more information about the Secure Access Org ID, see Find Your Organization ID.

2. Optionally, enable remote configuration of this VA over SSH, enter:

```
config va ssh enable
```

3. If you have enabled SSH, you can now remotely connect to the VA over SSH and enter Configuration Mode after authentication. Enter:

```
ssh vmadmin@<VA's IP address>
```

> **Note**
>
> Configuration mode does not support concurrent access by more than two users.

Enter Configuration Mode on a VA Deployed in Azure, AWS, or Google Cloud Platform

Provides instructions for completing the Enter Configuration Mode on a VA Deployed in Azure, AWS, or Google Cloud Platform workflow in Cisco Secure Access. A VA can be deployed in Azure with either a static IP address or a DHCP IP address.

A VA can be deployed in Azure with either a static IP address or a DHCP IP address. If you do not specify a static IP address at the time of deployment, the VA is automatically assigned a DHCP IP address and registers to Secure Access using this IP address. Secure Access lists this IP address as the name of the VA. For more information, see Manage DNS Forwarders.

In the case of AWS and Google Cloud Platform, the VA is automatically assigned a DHCP IP address and registers to Secure Access using this IPO address. Secure Access lists this IP address as the name of the VA on the dashboard.

Procedure

1. Connect to the VA's static or DHCP IP address over SSH. Enter:

```
ssh vmadmin@<VA's IP address>
```

   SSH access to the VA requires authentication:

2. Enter the default password.

   For information about the VA password, see Reset Password for Virtual Appliance .

   Secure Access prompts you to change the password the first time you log into Configuration Mode. Your password must be at least eight characters long, include at least one lowercase character, one uppercase character, one digit, and one special character. Your password cannot be the same as your last password.

What to do next

> **Note**
>
> Configuration mode does not support concurrent access by more than two users.

Configure the VA Through Configuration Mode

Describes Configure the VA Through Configuration Mode in Cisco Secure Access. Configuring the VA involves configuring the name, IP details, and local DNS servers.

Configuring the VA involves configuring the name, IP details, and local DNS servers. It is mandatory to configure the name and IP, netmask, and gateway (unless already configured). Failing to do this results in the VA not being able to register to Secure Access.

In addition to an IPv4 address, you can also configure the VA with an IPv6 address. Endpoints with an IPv6 address can use the VA for DNS resolution, and Secure Access logs the internal IPv6 address of the endpoint in the reports.

> **Note**
>
> Active Directory integration is currently not supported for IPv6 endpoints.

Field	Description
Name*	The name associated with the VA in Secure Access. This is a descriptive name, similar to a hostname for a computer or server. If you have multiple hypervisor hosts, appending or prepending numbers or letters to indicate the local hypervisor host is advised. **1.** To configure the name, enter `config va name <name>`
IP, Netmask, and Gateway*	Give the VA a local, static IP address on the same network as your endpoints which will utilize the VAs for DNS resolution. **Note** Configuring an IPv4 address is mandatory. Configuring an IPv6 address is optional and does not replace the IPv4 configuration. In addition to static IPv6 configuration, the VA supports dynamic IPv6 addressing through DHCPv6 or Stateless Address Autoconfiguration (SLAAC) when the network provides the required service or router advertisements. **1.** To configure the IP, Netmask, and Gateway for the VA, enter: `config va interface <ipaddress> <netmask> <gateway>` **2.** To configure an IPv6 address on your VA, enter: `config va interface6 <ipv6 address>/<prefix> <ipv6-gateway>` For example: `config va interface6 2011:0db8:85a3:1001:1000:8a2e:1370:7334/128 fe80::2222`

Field	Description
Local DNS 1-6	Configure your local DNS servers that will receive DNS queries for internal domains. These are usually your Windows Servers with the DNS server role installed. You can enter IPv4 and/or IPv6 addresses here. For more information and commands to configure local DNS servers, see Local DNS Forwarding.

*Mandatory parameters for the VA.



If you have entered the Configuration Mode over SSH, to validate status, enter:

```
config va status
```

If tests complete without error, the next step is to verify that the VA syncs with Secure Access.

Configure a Second VA

Describes Configure a Second VA in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Repeat the previous steps to configure a second VA. A second VA is required for continuous operation, high availability, and automatic upgrades.

- Do not clone the first VA. Secure Access does not recognize a cloned VA.
- Ensure that your second VA is set up manually.

> **Note**
>
> Azure AD Domain Services is currently not supported. For identity integration with the VA, the AD Connector and Domain Controllers should be deployed as VMs in Azure. Alternately, these components can be deployed on-premise provided there is an ExpressRoute or MPLS connection over which the AD Connector can communicate with the VA in Azure.

Configure Settings on VAs

Describes Configure Settings on VAs in Cisco Secure Access. Configure other settings on your Cisco Secure Access Virtual Appliances (VAs).

Configure other settings on your Cisco Secure Access Virtual Appliances (VAs).

Prerequisites

- For more information, see Prerequisites for Virtual Appliances.

Configure Rate Limiting

Describes Configure Rate Limiting in Cisco Secure Access. You can set rate limits of DNS queries on a VA for a single IP address.

You can set rate limits of DNS queries on a VA for a single IP address. Use rate limits to prevent any single endpoint from attempting to flood the VA with DNS queries and causing a Denial-of-Service on the VA.

Enable Rate Limits on a VA

Enable rate limits on the Virtual Appliance. Rate-limiting is off by default.

- **pps**–The number of packets accepted for each second from an individual IP. Supported values are 10 to 100,000.
- **burst**–The packet burst rate.

```
config va per-ip-rate-limit enable <pps> <burst>
```

Disable Rate Limiting

Disable rate limits on the Virtual Appliance.

```
config va per-ip-rate-limit disable
```

Check Status and Packet Drops

Check status and packet drops on the Virtual Appliance.

```
config va show
```

Configure NAT64 Prefixes

You can configure NAT64 prefixes on the VA. The prefix must be a valid IPv6 CIDR prefix with host bits set to zero.

```
config va nat64prefixes add 64:ff9b::/96
config va nat64prefixes remove 64:ff9b::/96
config va nat64prefixes show
```

The VA supports up to eight configured NAT64 prefixes

Configure NTP Servers

Describes Configure NTP Servers in Cisco Secure Access. By default, VAs use Ubuntu NTP servers (ntp.ubuntu.com) as their time servers.

By default, VAs use Ubuntu NTP servers (**ntp.ubuntu.com**) as their time servers. You can configure your VAs to use other NTP servers.

You can configure NTP servers by using IPv4 or IPv6 addresses. Use either IPv4 or IPv6, not both.

```
config ntp add 2001:db8::123
config ntp remove 2001:db8::123
config ntp show
```

NTP over TLS also supports IPv6 server addresses:

```
config ntp tls add 2001:db8::123
config ntp tls remove 2001:db8::123
config ntp tls enable config ntp tls disable
config ntp tls ca <certificate>
```

Add NTP Servers to the VA

You can configure NTP servers by using IPv4 or IPv6 addresses. Use either IPv4 or IPv6, not both.

```
config ntp add <serverIP1> <serverIP2>
```

Remove NTP Servers

```
config ntp remove <serverIP1> <serverIP2>
```

View the VA's Current NTP Servers

```
config ntp show
```

Configure Secure Access Resolvers

Describes Configure Secure Access Resolvers and explains Use the IPv4 Secure Access DNS Resolvers, Use the Alternate Secure Access DNS Resolvers, and Use the IPv6 Secure Access DNS Resolvers. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By default, the VA is configured to use the Cisco Secure Access DNS resolvers. For more information, see Secure Access DNS Resolvers .

You can change the Secure Access resolvers used by the VA.

Use the IPv4 Secure Access DNS Resolvers

```
config va resolvers global
```

Use the Alternate Secure Access DNS Resolvers

Use this option if your ISP blocks traffic to the Secure Access DNS resolvers.

```
config va resolvers alternate
```

Use the IPv6 Secure Access DNS Resolvers

```
config va resolvers global-v6
```

Use the US-Only IPv4 Secure Access DNS Resolvers

```
config va resolvers US
```

Use the US-Only IPv6 Secure Access DNS Resolvers

```
config va resolvers US-v6
```

Use the Saudi Arabia-Only IPv4 Secure Access DNS Resolvers

```
config va resolvers 7071
```

Use the Saudi Arabia-Only IPv6 Secure Access DNS Resolvers

```
config va resolvers 7071-v6
```

> **Note**
>
> If you configure the IPv6 Secure Access DNS resolvers, then the VA only sends DNS queries over IPv6. HTTPS traffic to other endpoints is sent over IPv4.

Configure DNSSEC Support

Describes Configure DNSSEC Support in Cisco Secure Access. Secure Access supports DNSSEC by performing validation on queries sent from Secure Access DNS resolvers to upstream authorities.

Secure Access supports DNSSEC by performing validation on queries sent from Secure Access DNS resolvers to upstream authorities.

If your endpoints are making DNS queries with the **DNSSEC OK (DO)** bit to the VA, the default behavior of the VA is to turn off this bit before forwarding the query to Secure Access or the local DNS server.

Configure VA to Preserve the DO Bit

Configure the VA to preserve the DO bit when forwarding the DNS query to Secure Access or the local DNS server.

> **Note**
>
> The VA preserves any DNSSEC Security Resource Records in the DNS response to the endpoint.

```
config va dnssec enable
```

Turn Off the DO Bit

```
config va dnssec disable
```

Command	Description	Notes
config va dnssec enable	Configure the VA to preserve the DO bit when forwarding the DNS query to Secure Access and/or the local DNS server.	Preserves any DNSSEC Security Resource Records in the DNS response to the endpoint.
config va dnssec disable	Disable the above configuration.	

Configure Logging to Remote Syslog Server

Describes Configure Logging to Remote Syslog Server in Cisco Secure Access. Virtual Appliances can forward logs to a remote syslog server.

Virtual Appliances can forward logs to a remote syslog server. If configured, Secure Access forwards logs related to internal DNS queries, logs on upgrades and reboots of the VA, and admin audit.

Configure the Destination of the Remote Syslog Server

Describes Configure the Destination of the Remote Syslog Server in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

```
config logexport destination <server-ip-address:port> <protocol>
```

Supported Values for `<protocol>`:

- TCP, UDP, or TLS.
- If no value is specified, TCP is the default.
- If the protocol value is TCP or UDP and a port is not specified, 514 is assigned as the default port.
- If the protocol value is TLS and a port is not specified, 6514 is taken as the default port.
- IPv6 addresses are not supported as destination IPs for this command.

  For example: `config logexport destination <10.26.02.82:514> udp`

When you configure an IPv6 log export destination, enclose the IPv6 address in square brackets before specifying the port.

```
config logexport destination [2001:db8::50]:514 udp
config logexport destination [2001:db8::50]:514 tcp
config logexport destination [2001:db8::50]:6514 tls
```

To forward the logs over a TLS-encrypted session, first create the certificates for the client (VA) and server (remote syslog server). The certificates can be self-signed or signed by a Root certificate authority (CA).

Add the key and certificate to the VA using the following commands:

```
config logexport key <copy the contents from keyForClientCert.pem file>
config logexport cert <copy the contents from ClientCert.pem file>
config logexport ca \<copy the contents from selfsignedCA.pem|chainCertCA.pem
 file>
```

Note

The CA configured in the last command should be the CA used to sign the server certificate.

Configure Log Export Internal DNS

Describes Configure Log Export Internal DNS in Cisco Secure Access. All internal DNS queries sent to the internal DNS server are logged at the syslog server.

All internal DNS queries sent to the internal DNS server are logged at the syslog server. Logs include the date and time, the internal domain being queried and the private IP, hostname and username of the source endpoint that made the query.

Note

If AD integration is not configured for the VA, the hostname and username of the source endpoint are not available.

```
config logexport enable internaldns
```

Format for internal DNS queries:

- Date
- Time
- Hostname (forwarder)
- VA Label:
  - InternalDNS
- Internal IP of source
- User AD identity of source (if a user identity is mapped to this IP else "NULL")
- Host AD identity of source (if a host identity is mapped to this IP else "NULL")
- Internal Domain being queried

Configure Log Export Enable Health

Describes Configure Log Export Enable Health in Cisco Secure Access. Reboots and upgrades of the VA are logged at the syslog server.

Reboots and upgrades of the VA are logged at the syslog server.

```
config logexport enable health
```

Format for VA boot:

- Date
- Time
- Hostname ("forwarder")
- VA Label:
  - Health
  - VA started

Format for VA upgrade:

- Date
- Time
- Hostname (forwarder)
- VA Label: Health
- VA downloaded version <x.y.z> or VA upgraded to version <x.y.z>

Configure Log Export Enable Admin

Describes Configure Log Export Enable Admin in Cisco Secure Access. Admin audit log (logins by admin users and config commands run on the VA) are logged at the syslog server.

Admin audit log (logins by admin users and config commands run on the VA) are logged at the syslog server.

```
config logexport enable admin
```

Format for User Login to VA:

- Date
- Time
- Hostname (forwarder)
- VA Label: Audit-Auth

- SSH login from as <vmadmin/vmuser> succeeded/failed or "Console login as <vmadmin/vmuser> succeeded/failed

Format for Configuration change:

- Date
- Time
- Hostname (forwarder)
- VA Label: `AuditLog-Config command executed`

Configure Log Export Enable All

Describes Configure Log Export Enable All in Cisco Secure Access. Enables logging of internal DNS, health, and admin logs at the syslog server.

Enables logging of internal DNS, health, and admin logs at the syslog server.

```
config logexport enable all
```

Configure Log Export Status

Describes Configure Log Export Status in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Run this command to check the status of the log forwarding:

```
config logexport status
```

Turn Off Logging

Describes Turn Off Logging in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Run this command to turn off logging:

```
config logexport disable <feature>
```

> **Note**
>
> You can set the `feature` option to `internaldns`, `health`, `audit` or `all`.

Example:

```
config logexport disable all
```

Configure Dual-NIC Support on the VA

Describes Configure Dual-NIC Support on the VA in Cisco Secure Access. Throughout this section, the terms NIC, network interface, and network adapter are used interchangeably.

> **Tip**
>
> **NIC Terminology**
>
> Throughout this section, the terms NIC, network interface, and network adapter are used interchangeably.

Virtual Appliances support a dual-NIC configuration. This dual-NIC configuration is intended to enable the DMZ deployment of a VA for traffic segregation with one network interface. The network interface is used for outbound communication and the other network interface is used for internal communication.

Dual-NIC support has only been qualified on VAs running on Hyper-V and VMware. There is no change to existing behavior if the VA is deployed with a single NIC. Configuring more than two NICs on the VA is not supported.

> **Note**
>
> When using the dual-NIC configuration, Secure Access does not support the configure of IPv6 addresses for network adapters.

For DMZ deployment, configure two interfaces on the VA before you enable DMZ mode.

To enable DMZ mode, enter

```
config va dmz
        enable
```

.

To disable DMZ mode, enter

```
config va dmz
        disable
```

.

To check the current DMZ mode, enter

```
config va
                show
```

.

Configure an Existing VA to Support Dual-NIC

Provides instructions for completing the Configure an Existing VA to Support Dual-NIC workflow in Cisco Secure Access. Open your existing VA in your preferred hypervisor's console or SSH to the VA.

Procedure

1. Open your existing VA in your preferred hypervisor's console or SSH to the VA.
2. Run the command to show the configuration of the VA.

   Ensure that the IP configured here is the IP that will be used for internal communication. This is the IP that your endpoints will use for DNS resolution.

> **Note**
>
> Before adding a secondary network adapter, save the MAC address of the existing network adapter before adding a secondary network adapter.

```
config va show
```

3. Shut down the VA and add a second network adapter using your hypervisor console.

   This is the network adapter you will be using for your outbound communication. This should be of the same driver type as your primary network adapter.

   > **Note**
   >
   > Some platforms may not permit the addition of a second network adapter after the VA has been created.

4. Turn the VA on, enter the Configuration mode from the console or through SSH, and run the command `config va show`. This command returns the name of the second adapter.

   > **Note**
   >
   > Adding a second adapter when the VA is powered on may result in the adapter not being detected or the corruption of the existing configuration. The VA needs to be compulsorily shut down before adding the second adapter.

5. For the secondary adapter, assign the IP, netmask, and gateway parameters to be used for outbound (Internet) communication. Enter: `config va interface <*interface name*> <*ip address*> <*netmask*> <*gateway*>`.

   Verify against the MAC address of the respective adapters to ensure that the IP addresses are not misconfigured.

   > **Note**
   >
   > You cannot direct DNS requests to the IP configured on the secondary adapter because incoming DNS traffic will be blocked on this IP.

6. Once you have saved changes, enable traffic segregation.

   Static routes are configured for the IP on the secondary adapter to all Secure Access destinations required for the proper functioning of the VA. Configuring additional static routes is currently not supported.

   Enter:

```
config va dmz enable
```

Deploy a New VA to Support Dual-NIC DMZ Mode

Provides instructions for completing the Deploy a New VA to Support Dual-NIC DMZ Mode workflow in Cisco Secure Access. You can deploy a new VA with dual-NIC support.

You can deploy a new VA with dual-NIC support. The configuration steps are similar to configuring an upgraded VA. You can add the secondary adapter to the VM using the hypervisor console, before powering on the VM. Both adapters should be of the same driver type.

Procedure

1. Enter configuration mode on the VA and retrieve the name of both adapters.

   Run:

   ```
   config va show
   ```

2. Configure the primary adapter and then the secondary adapter.

   Ensure that the primary adapter is configured with the IP that you wish to use for internal communication and that the secondary adapter is configured with the IP to be used for internet-bound communication.

   Run:

   ```
   config va interface <interface name> <ip address> <netmask> <gateway>
   ```

3. Once both adapters are configured, enable traffic segregation.

   Run:

   ```
   config va dmz enable
   ```

Configure Anycast

Describes Configure Anycast in Cisco Secure Access. Secure Access Virtual Appliances enable the use of Anycast DNS addressing within an enterprise.

Secure Access Virtual Appliances enable the use of Anycast DNS addressing within an enterprise.

The advantage of using Anycast is that all your endpoints can use the same DNS IP address irrespective of the Site where they belong. Configuring an Anycast IP address on the VA adds resiliency for DNS resolution.

The VA currently supports enabling Anycast using the BGP protocol. This requires support for BGP on the VA's neighboring router, or any router that is reachable from the VA within 255 hops.

You can configure up to 4 routers running BGP as BGP peers for the VA.

Two VAs in different branches can also be configured with the same Anycast IP address, ensuring resiliency across branches. However, if AD integration is required, these VAs must be in the same Secure Access Site, since the AD Connector propagates IP-AD user mappings only to VAs in its Secure Access site.

Secure Access supports the configuration of IPv4 addresses as an Anycast address on the VA.

Secure Access Virtual Appliances use Anycast for load balancing. Secure Access has verified the use of Anycast for load balancing on the VA in on-premises deployments: VMware and Hyper-V. However, for VAs that are deployed in the cloud, the use of Anycast depends on the egress networking support provided by the cloud environment's virtual switches (vSwitches).

> **Note**
>
> Anycast for VAs is not supported on Google Cloud Platform (GCP) due to limited support on the GCP infrastructure.

Configure Anycast over BGP on the VA

Provides instructions for completing the Configure Anycast over BGP on the VA workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Enter the Configuration Mode on the VA.
2. Enable Anycast support on the VA. Enter **config anycast bgp <*options*>**

   Command returns an ASN for the VA.

   Options are:

   - **enable** <***anycast_ip***> <***bgp_info***>–Enable the anycast mode
     - <***anycast_ip***>–Anycast IP address
     - <***bgp_info***>–ASN:IPAddress:Hop count of the BGP router to publish. If a hop count is not specified, a default value of 255 is assumed, therefore, the router can be up to 255 hops away.
   - **add <ASN:Router IP:Hop count>**–Use this command to specify an additional router as a BGP peer for the VA. A maximum of 4 peers can be configured.
   - **delete <Router IP>–Use this command to remove a BGP peer for the VA.**
   - **stats**–Show statistics around the Anycast configuration
   - **summary**–Show summarized list of all BGP peers for this VA
   - **disable**–Disable anycast mode
   - **status**–Show status of anycast
   - **test**–test Anycast connectivity
   - **help**–Display this usage information
3. Validate status. Enter **config anycast bgp status**
4. On the router, add the VA's ASN from step 2 as the neighbor of the router.

What to do next

Example:

In the following configuration, the VA needs to be configured with Anycast IP 192.168.1.22, the BGP router's ASN is 7105, and IP address is 10.1.0.1.

Configure Load Balancing

Describes Configure Load Balancing in Cisco Secure Access and explains Add a Load Balancer and Remove a Load Balancer. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can configure your Virtual Appliances behind a load balancer that meets the following requirements:

- The load balancer is able to inject the source IP address of the client making the query in the EDNS Client Subnet (ECS) field of the DNS request sent to the VA.

- The DNS response from the Virtual Appliance routes through the load balancer. Thus, the response to the client comes from the address of the load balancer.

This feature has specifically been qualified with the F5 BIGIP-LTM 16.1.1 version, where the F5 can inject the endpoint source IP in DNS requests that it forwards to VAs in the load balancing pool. Refer to F5 documentation on ECS injection in DNS requests when forwarding these requests to a DNS server pool.

By default, the VA does not accept DNS requests with the ECS option from any endpoint. To allow the VA to accept DNS requests with the ECS option from load balancers, the load balancer IP has to be added to the VA configuration using the following commands:

Add a Load Balancer

```
config loadbalancer add <server-ip/prefix>
```

Remove a Load Balancer

```
config loadbalancer remove <server-ip/prefix>
```

> **Note**
>
> You can add a maximum of 8 load balancers to a VA. Also, add or remove a single load balancer at a time.

Configure Identity Association Timeouts

Describes Configure Identity Association Timeouts in Cisco Secure Access. Use the config admap command to configure association timeouts for a given IP address.

Use the `config admap` command to configure association timeouts for a given IP address. You can also view or clear the AD mapping. You can only clear the mappings of an individual IP address.

Example commands:

```
config admap view <ip address>
```

```
config admap clear <ip address>
```

```
config admap set-user-timeout 28800
# This command sets the host timeout for 8 hours
```

```
config admap set-host-timeout 28800
# This command sets the host timeout for 8 hours
```

```
config admap show-timeout
```

Configure API Key Credentials for Authentication

Describes Configure API Key Credentials for Authentication in Cisco Secure Access. Once you delete the Secure Access API key credentials that you created for authentication of your Virtual Appliances, the VAs have 90 days to use the existing API client key and secret.

Once you delete the Secure Access API key credentials that you created for authentication of your Virtual Appliances, the VAs have 90 days to use the existing API client key and secret. After 90 days, your VAs can not sync with Secure Access.

> **Note**
>
> Unless you have unusual circumstances, we do not recommend that you delete your Secure Access API key credentials.

Configure the Client ID and Client Secret

Provides instructions for completing the Configure the Client ID and Client Secret workflow in Cisco Secure Access. Create a new set of API client credentials in Secure Access.

Procedure

1. Create a new set of API client credentials in Secure Access. For more information, see Configure Authentication for Virtual Appliances.
2. With your generated Secure Access API client key and secret, run the `config authcred set` command:

```
config authcred set "<client_id>:<client_secret>"
```

Local DNS Forwarding

Describes Local DNS Forwarding in Cisco Secure Access. Cisco Secure Access Virtual Appliances (VAs) are conditional DNS forwarders in your network, forwarding public DNS queries to Secure Access, and local DNS queries to your existing local DNS servers and forwarders, respectively.

Cisco Secure Access Virtual Appliances (VAs) are conditional DNS forwarders in your network, forwarding public DNS queries to Secure Access, and local DNS queries to your existing local DNS servers and forwarders, respectively.

When the VAs receive queries which match domains or subdomains of a local DNS zone (local domain), the VA forwards those queries to your local DNS server for resolution instead of the Secure Access public DNS resolvers. This is accomplished by defining your local domain names in Secure Access.

Important

Do not set your local DNS forwarders to point to the VAs. It is possible to create loops in DNS in this configuration and it's not recommended or supported.

Manage Domains in the VA

Describes Manage Domains in the VA in Cisco Secure Access. Any DNS queries received by the VAs which match a domain on the Internal Domains list, will be forwarded to the local DNS server as described in Configure Virtual Appliances.

Any DNS queries received by the VAs which match a domain on the Internal Domains list, will be forwarded to the local DNS server as described in Configure Virtual Appliances.

The following domains/zones are **pre-populated** and do *not* need to be added:

- ***RFC1918*** –non-publicly routable address spaces used only for reverse DNS on internal networks. All local IP address space for reverse lookups (PTR records) is covered with this entry. Adding **in-addr.arpa** reverse lookup zones are not needed.
- ***.local*** –Any domain name with a TLD of .local.

You have a choice of what type of identities are set to respect these internal domains:

- All Sites–Covers all requests that are made through a VA.
- Sites listed under All Sites–Covers requests only made through VAs deployed in the selected sites.
- All Devices–Covers all requests that are made through a roaming device.

Which domains should be added?

Describes Which domains should be added in Cisco Secure Access. Any domain name which has a forward lookup zone on your local DNS servers must be added, along with any domains that are configured with conditional forwarders.

Any domain name which has a **forward lookup zone** on your local DNS servers must be added, along with any domains that are configured with conditional forwarders. If you already know which domains to add, skip the Add A & PTR Records for the VAs section.

On Windows Server, this information is located in the DNS Manager tool.

1. Open the DNS Manager (**Start** > **Run** and type "`dnsmgmt.msc`").
2. Expand the **Server name** and **Forward Lookup Zones** sections.

   Any domains listed here are treated as local by your local DNS forwarders. Add these domains to your internal domains list in Secure Access. This is a critical part of the setup process.

3. If any public IPs are in use as local IPs, also add the **Reverse Lookup Zone** of any public IPs which have local DNS records attached. RFC-1918 reverse lookup zones are included by default. These are entered in the in-addr.arpa format.

   > **Note**
   >
   > Be aware that it can take up to 10 minutes for the virtual appliance to synchronize with changes you make to the Internal Domains list.

(Optional) Add A and PTR Records for the VAs

Describes (Optional) Add A and PTR Records for the VAs in Cisco Secure Access. Adding A and PTR records for the VAs makes them easy to identify within your network topology, including firewall and security appliance logs.

Adding A and PTR records for the VAs makes them easy to identify within your network topology, including firewall and security appliance logs.

If you're unfamiliar with adding A and PTR records, see the Microsoft articles:

- Add a PTR record
- Add a host (A) record

After adding A and/or PTR records, verify the records:

Verify PTR record

From a command prompt, enter:

```
nslookup <VA IP ADDRESS>
```

You should see the record in the last line of the result.

```
nslookup 192.168.1.10

    Server:192.168.1.1
```

```
    Address:192.168.1.1#53
    Non-authoritative answer:
    9.168.192.in-addr.arpaname = \[va01.corp.domain.com\]
```

Verify A record

From a command prompt, enter:

```
nslookup <VA HOSTNAME>
```

You should see the record in the last line of the result.

```
nslookup va01.corp.domain.com

   Server: 192.168.1.1
    Address: 192.168.1.1#53
    Non-authoritative answer:
    Name: va01.corp.domain.com
    Address: 192.168.1.9
```

Configure Local DNS Servers on the VA

Describes Configure Local DNS Servers on the VA in Cisco Secure Access. You can configure the VA to send queries for local domains to any local DNS server.

You can configure the VA to send queries for local domains to any local DNS server. You can also selectively forward DNS queries for specific local domains to specific local DNS servers.

Use the following commands to configure the VA to send queries for local domains to local DNS servers:

Task	Command	Note
Configure up to 6 local DNS servers	**config localdns add <ip>** Example: `config localdns add 2001:db8:300::53 corp.example.com`	The command must be entered individually for each local DNS server. The command does not take multiple IP inputs. You can configure IPv4 or IPv6 local DNS servers. The VA must have an IPv6 address configured before you add an IPv6 local DNS target.
Remove a configured local DNS server	**config localdns remove <ip>**	
Add a local DNS server and assign specific internal domains to this server	**config localdns add <ip of local DNS server><domain1>||<domain2_domainN>**	Add Internal domains to Secure Access. Requests for other internal domains will not be forwarded to these local DNS servers.
Show the list of internal DNS servers and any domain mappings against these servers	**config localdns show**	

> **Note**
>
> If you are assigning specific domains to specific local DNS servers, be sure to add at least one local DNS server with no domain assignment so that it can support queries for all other internal domains.

Examples

Describes Examples in Cisco Secure Access. You can also combine the above features to have some local domains redirected to specific local DNS servers and other domains redirected to the remaining local DNS servers.

You can also combine the above features to have some local domains redirected to specific local DNS servers and other domains redirected to the remaining local DNS servers.

Command	Outcome
config localdns add 209.165.200.229 internaldomain1.com	DNS queries for internaldomain1.com will now be forwarded to 209.165.200.229 and 209.165.200.229.
config localdns add 209.165.200.229 internaldomain1.com internaldomain2.com	DNS queries for internaldomain2.com will now be forwarded to 209.165.200.229
config localdns add 209.165.200.229	DNS queries for all other internal domains will be forwarded to 209.165.200.229

Test Virtual Appliance Deployments

Describes Test Virtual Appliance Deployments in Cisco Secure Access. After you deploy the Cisco Secure Access Virtual Appliances (VAs) in your environment and set up internal domains in Secure Access, we recommend that you test your Virtual Appliances.

After you deploy the Cisco Secure Access Virtual Appliances (VAs) in your environment and set up internal domains in Secure Access, we recommend that you test your Virtual Appliances.

To begin enforcing your DNS-layer security settings, DNS traffic from the endpoints on your network must exclusively use the VAs as a DNS forwarder.

Prerequisites

- A minimum user role of Read-only. For more information, see Manage Accounts.

Resolve Public and Local DNS Queries

Describes Resolve Public and Local DNS Queries in Cisco Secure Access. Before configuring endpoints to utilize the VAs for DNS traffic, ensure that the VAs are capable of resolving public and local DNS queries.

Before configuring endpoints to utilize the VAs for DNS traffic, ensure that the VAs are capable of resolving public and local DNS queries. The simplest test is to open a command prompt from a local endpoint and run the `nslookup` command:

nslookup opendns.com <VA IP Address>

```
nslookup opendns.com. 192.168.10.1

    Server:   192.168.10.1
    Address: 192.168.10.1#53
```

```
    Non-authoritative answer:
    Name: opendns.com
    Address: 67.215.92.218
```

- If the lookup times out, confirm that you have met firewall requirements. For more information, see Prerequisites for Virtual Appliances.
- If the test succeeds, perform the same test again, but this time with a local resource, such as a domain controller or mail server.

nslookup dc01.localdomain.corp. <VA IP Address>

```
nslookup dc01.localdomain.corp.

    Server:  192.168.10.1
    Address: 192.168.10.1#53

    Non-authoritative answer:
    Name: dc01.localdomain.corp
    Address: 192.168.10.47
```

If the result is something other than expected, ensure the domain was added as an internal domain in Secure Access.

When deploying the VA, we recommend the following for DNS configuration on any internal DNS servers:

- On the DNS server adapter settings, use the loopback address (127.0.0.1) so that the server will use itself for DNS resolution. The second entry should be another internal DNS server.
- On the forwarder settings of the DNS server, we recommend using the Secure Access Anycast IPs (208.67.222.222/208.67.220.220) rather than the virtual appliance IPs. This limits the ability to see the source IP when viewing reports but avoids any problems with DNS loops if there is a misconfiguration on either the VA or internal DNS server.
- If the server also acts as a mail server, the best option is to point to your ISP's DNS servers or other recursive resolvers such as those provided by your ISP.

Test with Endpoints

Describes Test with Endpoints in Cisco Secure Access. Before sending most or all of your network's DNS traffic to the VAs, testing with several endpoints is highly recommended.

Before sending most or all of your network's DNS traffic to the VAs, testing with several endpoints is highly recommended. First, change an endpoint's DNS settings to the IPs of the VAs, and then verify the following:

- **Local and Remote DNS is functioning**–Ensure that local resources, internet resources, and applications are working as expected; this includes cloud-based applications, local websites, and commonly-used resources on the internet in general.
- **Verify in the Secure Access Reports**–Within a few minutes of changing DNS on an endpoint, you should start seeing traffic containing the Internal IP address in the Secure Access reports.

Example.com	Allowed	Software/Technology	Vancouver	192.0.2.1	192.0.2.254
Example.org	Allowed	Software/Technology,...	forwarder04....	198.51.100.1	198.51.100.254
Example.net	Allowed	Software/Technology	Townsend	198.51.100.1	198.51.100.254
Example2.net	Allowed	Software/Technology,...	Townsend	198.51.100.1	198.51.100.254

Secure Access recommends testing for between two and five days with several computers, preferably from different areas of your organization, before switching all production traffic to the VAs.

If DNS fails to resolve after modifying your DNS settings, confirm that you have met the network requirements. For more information, see Prerequisites for Virtual Appliances.

Transition Production Traffic

Describes Transition Production Traffic in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

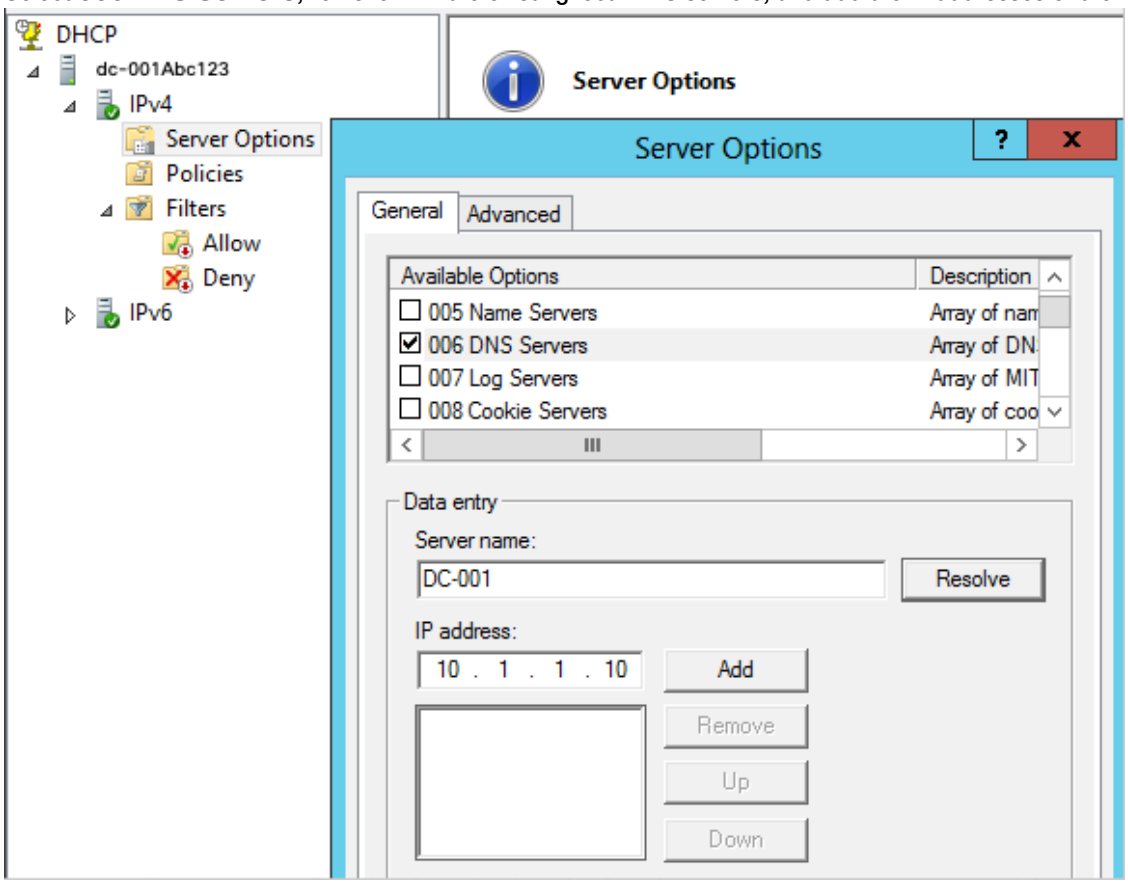
After successful testing, begin utilizing the VAs for production DNS traffic.

Important

The Secure Access VAs must be the **only** servers listed as DNS servers. Using a mixture of the VAs and other types of DNS servers is not supported.

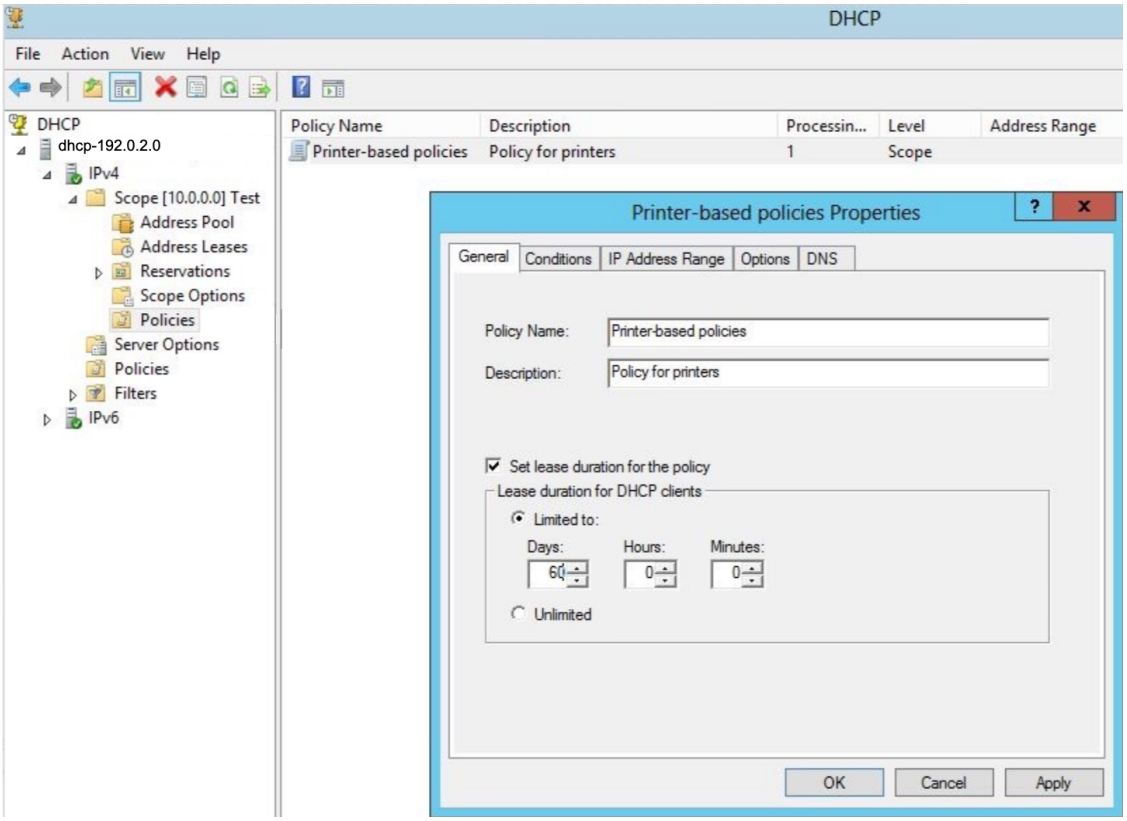
In most network environments using Windows Server, local IP addressing is handled through the **DHCP Manager**. To update your endpoints' DNS settings to point to the VAs, change the DNS Servers in your DHCP scope options.

1. Open **DHCP Manager** and navigate to **Start** > **Administrative Tools** > **DHCP**.
2. Select IPv4 or specific scope, if applicable.
3. Right-click Server Options or Scope Options.
4. Select **006 DNS Servers**, *remove***ALL** the existing local DNS servers, and *add* the IP addresses of the VAs.



The VAs must be the **only** DNS servers in this list. It is not possible to use a mixture of VAs and other DNS servers.

After updating the DNS Servers in the DHCP options, wait for the DHCP leases on the endpoints to expire and see the new changes. In most cases, DHCP lease durations are seven days or less, but sometimes may be set to higher values. We recommend verifying the DHCP lease duration in the **DHCP Manager**.



Unfortunately, there is no easy way to force an immediate DHCP lease renewal. One method is to use a **Group Policy Object** to deploy and execute a *batch* file with the `ipconfig /renew` command in it; this would cause the endpoints to recognize the VAs as their DNS servers.

SNMP Monitoring for Virtual Appliances

Describes SNMP Monitoring for Virtual Appliances in Cisco Secure Access. The Cisco Secure Access Virtual appliances (VAs) support the Simple Network Management Protocol (SNMP), including versions SNMPv2c and SNMPv3.

The Cisco Secure Access Virtual appliances (VAs) support the Simple Network Management Protocol (SNMP), including versions SNMPv2c and SNMPv3. You can configure and enable SNMP in a VA to monitor the health of the VA and provide connectivity statistics. SNMP monitoring on a VA is disabled by default.

About SNMP Monitoring

The Secure Access VA listens on port 161 for SNMP queries. The VA supports SNMP monitoring of:

- Health statistics—CPU, load, memory, disk space, and status.
- Connectivity statistics—Connectivity to Secure Access resolvers, connectivity to the local DNS servers, connectivity to the Active Directory (AD) connector, and connectivity to the Secure Access API.

Enable SNMP Monitoring

Describes Enable SNMP Monitoring in Cisco Secure Access. In the Secure Access VA, the SNMP configuration supports the SHA-1, DES-128, and AES-128 algorithms.

In the Secure Access VA, the SNMP configuration supports the SHA-1, DES-128, and AES-128 algorithms.

SNMPv2.x

Configure SNMPv2 with the `config snmp` command, for example:

```
config snmp configure -v2 <options> <args>
```

If your VA uses SNMP version 2.3 or earlier, configure SNMP with the `support snmp` command, for example:

```
support snmp <options> <args>
```

SNMPv3

When you configure SNMPv3 in your VA, provide a `username` and `password`. All other parameters are optional.

Configure SNMPv3 with the `config snmp` command, for example:

```
config snmp configure -v3 <options> <args>
```

Privacy Password

The SNMP privacy password is a string that can include 8-255 alphanumeric characters.

> **Note**
>
> The SNMP privacy password can not include special characters.

Configure SNMP in Secure Access Virtual Appliance

Provides instructions for completing the Configure SNMP in Secure Access Virtual Appliance workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Enter the Configuration Mode on the VA. Use the `configure` option with the SNMP command. See the SNMP Command Syntax for the list of command-line arguments.
2. Enable SNMP monitoring.

   ```
   config snmp enable
   ```

3. Enter **exit** to return to the VA console.

SNMP Command Syntax

Describes SNMP Command Syntax in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

```
Usage: config snmp <options> <args>

       The options parameter must be one of the following: configure | enable
| disable | status

        configure      -v2 [ -c '<community string>' ]
                           Enables SNMP v2.
```

```
                              * c - Community string; The default Community
string is 'public'.
                         -v3 -u '<username>' -p '<password>' [-a [MD5|SHA] -x
[AES|DES] -X [password]\]
                              Enables SNMP v3 with username and password.
                             * u - Username can include at most 32 alphanumeric
 characters.
                              * p - Password can include 8-12 alphanumeric
characters.
                              * a - Optional password hash algorithm; Default
SHA.
                              * x - Optional encryption algorithm; Default AES.

                              * X - Privacy password is used with the AES
algorithm.
                                    The privacy password can include 8-255
alphanumeric characters.
                                    Special characters are not supported.

         enable          Enable SNMP.
         disable         Disable SNMP.
         status          Show the SNMP service status and Version information.

         -h, -\-help      Display this usage information.
```

Standard OIDs Supported by the Virtual Appliance

Describes Standard OIDs Supported by the Virtual Appliance in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Note**
>
> AWS does not support monitoring the VA's disk usage with OIDs.

Information	OID	Notes
Load	UCD-SNMP-MIB::laTable Load-1 (1 minute load): .1.3.6.1.4.1.2021.10.1.3.1 Load-5 (5 minute load): .1.3.6.1.4.1.2021.10.1.3.2 Load-15 (15 minutes load): .1.3.6.1.4.1.2021.10.1.3.3	If the five minute load is consistently greater than .75 of the number of processor cores, the VA is running short of processing power.
CPU	UCD-SNMP-MIB:systemStats Percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0 Percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0 Percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0	
Memory Utilization	UCD-SNMP-MIB::memory Available swap: .1.3.6.1.4.1.2021.4.4.0 Total swap: .1.3.6.1.4.1.2021.4.3.0	If the ratio of Available swap to Total swap is consistently lower than 0.5, the VA is running low on memory.

Information	OID	Notes
Disk Usage	Percentage of space used on data portion of disk: .1.3.6.1.4.1.8072.1.3.2.4.1.2.9.100.105.115.107.117.115.97.103.101.1	If this value is consistently greater than 0.8, the VA may be running out of disk space.

Note

Virtual Appliances support querying of the system OIDs **1.3.6.1.2.1.1.1** to **1.3.6.1.2.1.1.7**.

Extended OIDs Supported by the Virtual Appliance

Describes Extended OIDs Supported by the Virtual Appliance in Cisco Secure Access. The asterisk (*) denotes an OID which returns the throughput of the VA–the number of queries handled per second.

Information	OID
VA status (dns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.7.116.104.105.115.100.110.115.1
Connectivity to Secure Access resolvers (dns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.3.100.110.115.1
Connectivity to local DNS servers (localdns)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.8.108.111.99.97.108.100.110.115.1
Connectivity to Secure Access (cloud)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.5.99.108.111.117.100.1
Connectivity to AD connectors (ad)	.1.3.6.1.4.1.8072.1.3.2.4.1.2.2.97.100.1
Queries per second over last 5 minutes*	.1.3.6.1.4.1.8072.1.3.2.4.1.2.4.113.112.115.53
Queries per second over last 15 minutes*	.1.3.6.1.4.1.8072.1.3.2.4.1.2.5.113.112.115.49.53

The asterisk (*) denotes an OID which returns the throughput of the VA–the number of queries handled per second.

For the first 5 OIDs in the table above, search for the following sub-strings in the output:

- **green**–Indicates a status of Okay.
- **red**–Indicates a status of Not Okay.
- **yellow**–indicates a status of Partially Okay.
- **white**–indicates a status of Not Configured.

Note

If an SNMP probe against any of these OIDs results in a timeout, we recommend that you increase the timeout value when issuing the probe.

Troubleshoot Virtual Appliances

Describes Troubleshoot Virtual Appliances in Cisco Secure Access. Log in to your Cisco Secure Access Virtual Appliance (VA) to diagnose error conditions on the Virtual Appliance.

Log in to your Cisco Secure Access Virtual Appliance (VA) to diagnose error conditions on the Virtual Appliance.

Prerequisites

- A username and password to sign in to your Virtual Appliance.

Reset a Virtual Appliance's Password

You can reset the password for a Virtual Appliance in Secure Access. For more information, see Manage DNS Forwarders: Reset Password.

Use Configuration Mode to Troubleshoot

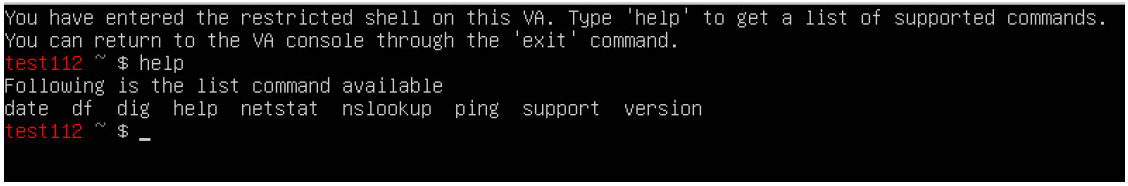
Provides instructions for completing the Use Configuration Mode to Troubleshoot workflow in Cisco Secure Access. The VA allows basic troubleshooting commands to be executed using the Configuration Mode.

The VA allows basic troubleshooting commands to be executed using the Configuration Mode.

Procedure

1. To enter the Configuration Mode, on the VA console, press **Ctrl+B**.

   You can also enter the Configuration Mode by initiating an SSH connection to the VA.

2. To view a list of supported commands in the restricted shell, enter **help**.
3. To return to the VA console, type **exit**.

   If the VA console crashes, the VA automatically enters the restricted shell.

Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed on Azure

Describes Troubleshoot Intermittent DNS Resolution Failures on a VA Deployed on Azure in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

If you have deployed the VA on Azure as a stand-alone virtual machine (VM) without a public IP address, you might experience intermittent DNS resolution issues when heavy DNS traffic is directed at the VA. This is due to SNAT port exhaustion on virtual machines deployed to Azure (such as the VA) because Azure only pre-allocates 1024 UDP ports for standalone VMs without a public IP address. To address this issue, you may either need to assign a public IP to each VA or deploy VAs behind a public Standard Load Balancer in Azure.

> **Note**
>
> If you are assigning a public IP to a VA, make sure that there are no inbound port rules for this VA that allow inbound access from the internet.

Troubleshoot DNS Resolution in Configuration Mode

Describes Troubleshoot DNS Resolution in Configuration Mode in Cisco Secure Access. The nslookup command can be used to test DNS queries on the VA.

The `nslookup` command can be used to test DNS queries on the VA. This test reflects how a users' DNS lookups will be answered and is subject to internal domains routing and other processing on the VA.

You can specify a server IP address as a parameter for `nslookup`. This is useful for testing a Local DNS server or the Secure Access cloud directly. These tests bypass the VA software.

Troubleshoot DNS Resolution Failures Behind a Firewall

Describes Troubleshoot DNS Resolution Failures Behind a Firewall in Cisco Secure Access. The VA offers DNSCrypt functionality that protects the content of your DNS queries.

The VA offers DNSCrypt functionality that protects the content of your DNS queries. This functionality may be blocked by your firewall.

If you are using the Cisco ASA firewall, you can see an indication of this in the ASA log.

For example:

```
Dropped UDP DNS request from inside:192.168.1.1/53904 to
outside-fiber:208.67.220.220/53;
    label length 71 bytes exceeds protocol limit of 63 bytes
```

DNS resolution is not affected by this blocking, but your DNS queries are not fully protected.

To address this, ensure that your firewall allows outbound queries on port 443 and 5353 for both TCP and UDP to the Secure Access resolver IP addresses as mentioned in the Pre-requisites section.

40 File Inspection and Analysis

Topics:

- Manage File Inspection and File Analysis
- Enable File Inspection
- Enable File Analysis by Cisco Secure Malware Analytics
- Test File Inspection for Internet Access
- Monitor File Inspection and Analysis Activity
- Troubleshoot File Inspection and Analysis

Provides an overview of File Inspection and Analysis in Cisco Secure Access, including Manage File Inspection and File Analysis, Enable File Inspection, and Enable File Analysis by Cisco Secure Malware Analytics. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage File Inspection and File Analysis

Describes Manage File Inspection and File Analysis in Cisco Secure Access. Protect your network from malicious files using file inspection and file analysis.

Protect your network from malicious files using file inspection and file analysis. You can enable these features for traffic to internet destinations and to private resources.

Malicious files can be encountered through an explicit download, such as when a user clicks a link in an email, or through a behind-the-scenes 'drive-by' download scenario.

Secure Access offers two options for evaluating files for malicious content:

- File Inspection
- File analysis (sandboxing) using Cisco Secure Malware Analytics

Once inspected and analyzed, Secure Access allows "good" files through and blocks the downloading of malicious files. When a malicious file is deleted in internet traffic, Secure Access shows the end user a block page.

Overview of Configuring File Inspection and Analysis

Describes Overview of Configuring File Inspection and Analysis in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To maximize protection, enable both options. If File Inspection does not detect that a file is malicious, and Secure Malware Analytics is not enabled, the file can be downloaded when requested.

To configure these features:

- Enable file inspection and analysis in security profiles for internet and private access and configure the features.
- In security profiles for internet access, also do the following:
  - Ensure that decryption is enabled.
  - Configure block notification pages and choose the applicable page
- Associate the security profile with an access rule.
- Enable and configure decryption in the configured private resources for destinations in the access rule.

File Inspection Details

Describes File Inspection Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

When File Inspection is enabled, Secure Access scans files using two features:

- Cisco Advanced Malware Protection (AMP) and
- a proprietary antivirus scanner

Cisco Advanced Malware Protection (AMP)

Describes Cisco Advanced Malware Protection (AMP) in Cisco Secure Access. When File Inspection is enabled, Secure Access uses AMP to scan for malicious files.

When File Inspection is enabled, Secure Access uses AMP to scan for malicious files.

AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the Talos Security Intelligence and Research Group, and Secure Malware Analytics intelligence feeds. The Cisco AMP engine does not do real-time sandboxing, instead, the Cisco AMP integration blocks files with a known bad reputation based on the checksum or hash of the file. The AMP checksum database is comprised of lookup and data from all AMP customers and is a dynamic global community resource shared between customers utilizing the technology.

For more information about AMP, see Advanced Malware Protection (AMP).

AMP File limitations

AMP can compute the hash of an archive file but cannot compute the hashes of files contained by archive files.

Antivirus Scanner

Describes Antivirus Scanner in Cisco Secure Access. When File Inspection is enabled, an antivirus scanner attempts to scan all files.

When File Inspection is enabled, an antivirus scanner attempts to scan all files.

Secure Access utilizes multiple Anti-Virus engines to scan files for malware. These engines check for updates multiple times per hour, applying and synchronizing updates across all Secure Access data center locations whenever updates are available from the associated anti-virus vendor.

The system begins streaming large files from the proxy to the user after scanning up to 50 MB to ensure that the user starts receiving the download while scanning continues in the background. If a file is identified as malicious, the connection is immediately terminated. For larger files, the user may initially experience a brief lag, but should still receive the entire file as quickly as normal—unless it's malicious.

Secure Access blocks downloads if there is a scanning error or the file is found to be corrupt. Once virus scanning is complete, the file is either delivered or the connection is terminated.

Antivirus scanner file limitations

Secure Access antivirus scanner:

- Scans only the first 50 MB of a file and does not scan any content of files greater than 50 MB in size.
- Decompresses and scans archives (such as .zip or .rar files) to a maximum of 16 levels of recursion, and blocks files compressed above 16 levels of recursion.
- Cannot decompress and scan a password-protected archive as the file cannot be decompressed without a password. Secure Access can block a password-protected archive under the scanner's Protected Archive category.

Cisco Secure Malware Analytics (formerly Threat Grid) Details

Describes Cisco Secure Malware Analytics (formerly Threat Grid) Details in Cisco Secure Access. Secure Malware Analytics is Cisco's malware analysis and threat intelligence platform.

Secure Malware Analytics is Cisco's malware analysis and threat intelligence platform. Secure Malware Analytics generates and gathers malware intelligence through static and dynamic runtime sample analysis, as well as from other Cisco integrations.

When you enable Secure Malware Analytics, files are first evaluated by the File Inspection engines. If files are neither known to the AMP file reputation service nor blocked by the anti-virus (AV) scanner, Secure Access can send them to Secure Malware Analytics for analysis, if this option is enabled.

When a file is submitted to Secure Malware Analytics for further examination, Secure Malware Analytics may sandbox the file so that it can be analyzed in safety to determine whether or not it is malicious.

If Secure Malware Analytics determines that a file is malicious, Secure Malware Analytics sends this information to AMP so that the File Inspection feature blocks any future attempts to download the file. (Secure Malware Analytics does not protect against the first download of a new or unknown malicious file.)

For more information about Secure Malware Analytics, see Cisco Secure Malware Analytics (formerly Threat Grid).

For essential information about enabling Secure Malware Analytics, see Enable File Analysis by Secure Malware Analytics.

Supported Files and File Limitations

Describes Supported Files and File Limitations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Secure Malware Analytics:

- Accepts the following file types:
  - bat, bz2, chm, dll, doc, docx, exe, gz, hta, hwp, hwt, hwpx, iso, jar, jtd, jtt, jtdc, jttc, lnk, msg, msi, mhtml, rar v5, rtf, xls, xlsx, ppt, pptx, pdf, ps1, sep, slk, swf, tar, vbe, vbn, vbs, wsf, xml, xps, xz, zip, 7-zip
  - Note that this list of accepted file types includes MS Office documents, PDFs and executables.
- Does not accept the MIME file type text/html.
- Does not accept files greater than 50 MB in size.

For more information about supported file types, see the online help in Secure Malware Analytics, under _Sample File Types.

Note

Secure Malware Analytics Quota

Your licensing package may not support sending unlimited files to Secure Malware Analytics. To determine your current package, navigate to Admin > Licensing. For more information, see Determine Your Current Package. See also Cisco Secure Access Packages.

If your package is limited, Secure Access can send only 500 files for analysis per rolling 24 hour period. To monitor this file count, see Monitor File Inspection and Analysis Activity.

Secure Malware Analytics Sandbox

Describes Secure Malware Analytics Sandbox in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The sandbox is a protected environment within which Secure Malware Analytics detonates unknown files to determine whether or not they are harmful.

Important

You cannot change the selected sandbox region

The first time you enable Secure Malware Analytics in any security profile, you must select a sandbox region: North America, Europe, or India.

Once selected, this location cannot be changed.

Not all files submitted to Secure Malware Analytics are sandboxed.

When you enable Secure Malware Analytics for the first time in any security profile, you must choose a sandbox location. Once this location is set, you are sent an email from Secure Malware Analytics with credential information including your username and a link to reset your password, which you must do within 36 hours.

Enable File Inspection

Describes Enable File Inspection in Cisco Secure Access. To inspect files for threats, enable the file inspection features in security profiles for internet and private access, then assign the security profiles to internet and private access rules.

To inspect files for threats, enable the file inspection features in security profiles for internet and private access, then assign the security profiles to internet and private access rules.

File Inspection uses multiple features to evaluate for malicious files. For details, see Manage File Inspection and Analysis.

Once inspections are complete, a file is either delivered to the end user or the connection is terminated and the user is shown a block page.

Once you have enabled File Inspection, to monitor and review Umbrella's inspection activities, use the Security Activity and Activity Search reports.

Prerequisites for Enable File Inspection

Describes Prerequisites for Enable File Inspection in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Full Admin user role. For more information, see Manage Accounts.
- Determine which options you want to enable. For details, see Manage File Inspection.

  If you will enable file analysis: Before you enable that feature, see important caveats in Enable File Analysis by Secure Malware Analytics.

  By default, File Inspection is enabled and file analysis is not.

  You must first enable File Inspection before you can enable file analysis.

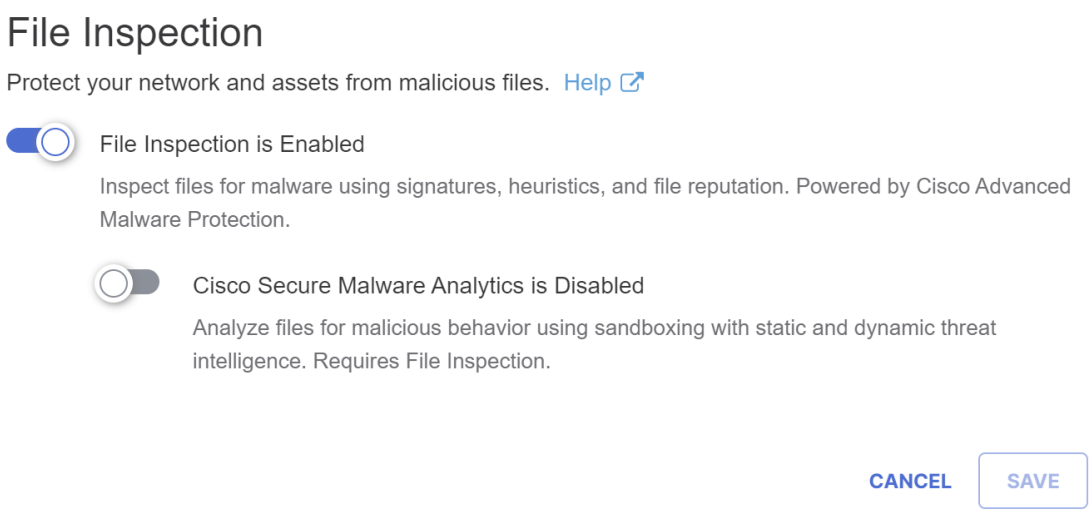
- Decryption must be enabled. See Manage Traffic Decryption.
- Certificates are required to decrypt traffic and detect files, and to display block notifications for files blocked in internet traffic.
  - For internet traffic, see Certificates for Internet Decryption.
  - For traffic to private resources, configure certificates in each private resource or see Manage Certificates for Private Resource Decryption.

Procedure for Enable File Inspection

Provides instructions for completing the Procedure for Enable File Inspection workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Click **+Add Profile** or expand an existing profile.
3. In the **Security and Acceptable Use Controls** section, for **File Inspection**, click **Edit**.
4. Enable **File Inspection** if it is not already enabled:



5. Click **Save**.
6. If you will enable file analysis using Cisco Secure Malware Analytics, see important information and follow the procedure in Enable File Analysis by Cisco Secure Malware Analytics.
7. For security profiles for internet access: In the same profile, ensure that Decryption is enabled.
8. For security profiles for private access: Ensure that destinations configured in the rule are configured as Private Resources with decryption enabled.
9. Choose a security profile that has file inspection enabled when you configure access rules.

Enable File Analysis by Cisco Secure Malware Analytics

Describes Enable File Analysis by Cisco Secure Malware Analytics in Cisco Secure Access. For maximum protection, files that are unknown to the File Inspection service (AMP) that are not blocked by the anti-virus feature can be sent to Secure Malware Analytics for further analysis.

For maximum protection, files that are unknown to the File Inspection service (AMP) that are not blocked by the anti-virus feature can be sent to Secure Malware Analytics for further analysis.

For file processing details, see Manage File Inspection and Analysis.

When you enable this option, you will create a Secure Malware Analytics account.

Prerequisites for Enable File Analysis by Cisco Secure Malware Analytics

Describes Prerequisites for Enable File Analysis by Cisco Secure Malware Analytics in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Full Admin user role. For more information, see Manage Accounts.
- If you are enabling file analysis for the first time:
  - Read this entire procedure before doing anything.
  - You must choose a sandbox region (North America, Europe, or India) that cannot be changed later. The sandbox holds files captured from both internet and private traffic.
  - Ensure that you can perform the following time-sensitive actions:

Important

Time-sensitive action required

Before you start this procedure, be sure that:

- you will be able to receive and access the email message that Secure Malware Analytics will send when you save the changes described in this procedure.
- you are able to take the required actions as described at the end of the procedure below.

You must sign in to Secure Malware Analytics within 36 hours after you click Save after enabling Secure Malware Analytics.

Procedure for Enable File Analysis by Cisco Secure Malware Analytics

Provides instructions for completing the Procedure for Enable File Analysis by Cisco Secure Malware Analytics workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

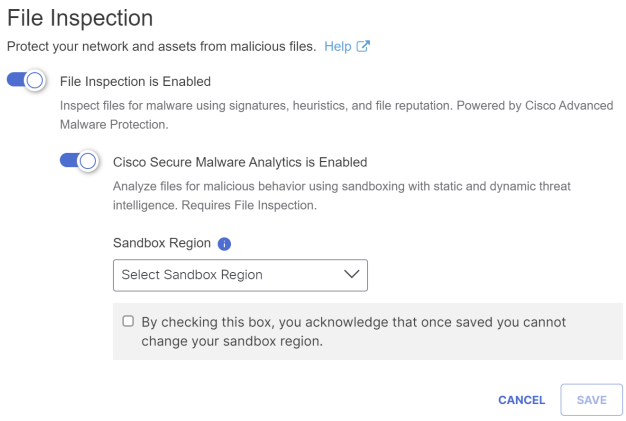
Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Expand an existing profile or click **+Add Profile** to add a new profile (for either internet or private access.)
3. In the **Security and Acceptable Use Controls** section, for **File Inspection**, click **Edit**.
4. Enable **File Inspection** if it is not already enabled.

   You cannot enable file analysis unless File Inspection is enabled.

5. Enable **Cisco Secure Malware Analytics**

   If this is the first time you are enabling this option, you will see this:



6. If you are enabling Secure Malware Analytics for the first time:

   Important

   Read the rest of this procedure before completing the procedure.

   a. There is a time limit for performing additional tasks after saving this configuration.

   b. Select a **Sandbox Region** (**North America**, **Europe**, or **India**) based on your data sovereignty preferences, then acknowledge that you understand that this location cannot be changed. The sandbox holds files captured from both internet and private traffic.

c. As soon as you click Save in the next step in this procedure, your organization's sandbox region is set and cannot be changed.

d. Be prepared to access and take action on the email message you will receive after you click Save in the next step. The email will be sent to the address associated with your Secure Access administrator account.

7. Click **Save**.

Important

You must log into Secure Malware Analytics within 36 hours of setting your sandbox region.

8. **Important:**

a. Take action using the email message you will receive from Secure Malware Analytics. You will sign into Secure Malware Analytics using the unique link provided in the email message. If you chose the Europe sandbox, the link goes to panacea.threatgrid.eu. If you chose the North America sandbox, it goes to panacea.threatgrid.com. If you chose the India sandbox, it goes to panacea.threatgrid.in. You will accept the End User License Agreement and set up your password. Your Secure Malware Analytics username will be the same email address as your Secure Access account.

b. Store your Secure Malware Analytics password securely so that you can use it later; you will need to sign in to Secure Malware Analytics to review information about files sent for analysis.

Test File Inspection for Internet Access

Provides instructions for completing the Test File Inspection for Internet Access workflow in Cisco Secure Access. A source device that is known to have access controlled by Secure Access.

After setting up file inspection, we recommend that you check your configured security profile and internet access rules. You can evaluate File Inspection by pointing your browser to one of our test files.

Before you begin

- A source device that is known to have access controlled by Secure Access.
- An internet access rule near the top of the rule order that has a security profile with File Inspection enabled.

  To ensure that the traffic is not blocked by other security features, test the security profile in a rule that has all other security and acceptable use features disabled. Ensure that no other rule in the access policy hits the traffic first.

Procedure

1. Browse to one of Cisco's EICAR test files.

Test File	Description
http://proxy.opendnstest.com/download/eicar.com	Clear text test file.
https://ssl-proxy.opendnstest.com/download/eicar.com	Encrypted test file.
http://proxy.opendnstest.com/download/AMP_TEST_FILE.txt	Cisco AMP clear text test file.
https://ssl-proxy.opendnstest.com/download/AMP_TEST_FILE.txt	Cisco AMP encrypted test file.

2. After loading a File Inspection test file, you should see a block page. Diagnostic information includes details about which server the file went through. If you do not see a block page, see Troubleshoot File Inspection.

Block Page Diagnostic Information

Provides instructions for completing the Block Page Diagnostic Information workflow in Cisco Secure Access. Block page diagnostic information identifies the hostname of the reputation authority.

Block page diagnostic information identifies the hostname of the reputation authority. When proxying a domain or URL, Secure Access evaluates the destination in two phases.

Procedure

1. Secure Access receives a request and checks the reputation of the domain or URL. If the destination is known to be malicious, Secure Access blocks the request and displays a block page. The block page diagnostic information lists the `Server` as `nginx`.
2. Next, Secure Access checks if a destination matches a security category or is blocked by an internet access rule. If a destination is not blocked, then Secure Access retrieves any requested content from the URL, then scans the requested files by file inspection (antivirus and AMP). If a file is malware, Secure Access returns a block page. The block page diagnostic information lists the `Server` as `mps`.

Monitor File Inspection and Analysis Activity

Describes Monitor File Inspection and Analysis Activity in Cisco Secure Access. There are several places to monitor file inspection and Secure Malware Analytics activity.

There are several places to monitor file inspection and Secure Malware Analytics activity.

Monitor and Review File Inspection and Analytics

To review inspection activity at any time, use the Security Activity and Activity Search reports.

Monitor and Review Secure Malware Analytics

Describes Monitor and Review Secure Malware Analytics in Cisco Secure Access. Your Secure Access licensing package includes access to a version of the dashboard in Secure Malware Analytics.

Your Secure Access licensing package includes access to a version of the dashboard in Secure Malware Analytics.

To review submitted files and Secure Malware Analytics activity, sign into Secure Malware Analytics.

The URL that you sign into depends on the sandbox region you chose the first time you enabled the Secure Malware Analytics feature in Secure access:

- If you chose Europe, use https://panacea.threatgrid.eu/login.
- If you chose North America, use https://panacea.threatgrid.com/login.
- If you chose India, use https://panacea.threatgrid.in/login.

The first time you enable Secure Malware Analytics in a security profile for either internet or private access, you set up credentials to access Secure Malware Analytics. You cannot use your Secure Access credentials to sign into Secure Malware Analytics.

For information about how to use Secure Malware Analytics, see the online help in Secure Malware Analytics.

Depending on your licensing package, you may not have access to all features in the Secure Malware Analytics dashboard. If you are a Secure Malware Analytics Cloud customer and have access to the full functionality of Secure Malware Analytics, you can link your Secure Access account to your Secure Malware Analytics Cloud portal. For more information, contact your account manager or Secure Malware Analytics support.

Monitor File Submission Limits

Describes Monitor File Submission Limits in Cisco Secure Access. If your licensing package limits the number of files that Secure Access can submit to Secure Malware Analytics, you should monitor file submission rates to ensure that potentially harmful files are analyzed.

If your licensing package limits the number of files that Secure Access can submit to Secure Malware Analytics, you should monitor file submission rates to ensure that potentially harmful files are analyzed.

To do this, sign into Secure Malware Analytics using the credentials you set up the first time you enabled Secure Malware Analytics in Secure Access.

The file limit applies to each rolling 24 hour period. At the end of the rolling 24 hour time period, the file quota is cleared and submissions start again–if the file limit is reached; otherwise, submissions continue unabated. To remove the limit, contact your account manager.

To determine your current licensing package, navigate to Admin > Licensing. For more information, see Determine Your Current Package. See also Cisco Secure Access Packages.

For more information about how to use Secure Malware Analytics, see the online Help in the Secure Malware Analytics dashboard.

Troubleshoot File Inspection and Analysis

Describes Troubleshoot File Inspection and Analysis in Cisco Secure Access and explains General Troubleshooting. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

General Troubleshooting

For internet destinations: When File Inspection is enabled, and Secure Access does not present a block page when expected:

- Check to be sure that the rule that matched the traffic has a security profile that has file inspection and analysis enabled.
- Ensure that the rule that needs to match the traffic is above other rules in the policy that the traffic might also match.
- Confirm that a required certificate is installed. For more information, see Certificates for Internet Decryption.

For traffic to private resources:

- Make sure Decryption is enabled in Global Settings.

Wait at least five minutes before testing again after any policy changes to ensure enough time has passed for the changes to be replicated throughout the Secure Access infrastructure. If problems persist, try clearing the local browser cache on your machine, or even your machine's DNS cache (a reboot will accomplish this).

41 File Type Controls

Topics:

- Manage File Type Controls
- Enable File Type Controls

Provides an overview of File Type Controls in Cisco Secure Access, including Manage File Type Controls and Enable File Type Controls. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage File Type Controls

Describes Manage File Type Controls in Cisco Secure Access. Cisco Secure Access provides file type controls in the Security profiles.

Cisco Secure Access provides file type controls in the Security profiles. File type controls manage access to certain types of files in traffic to internet destinations and private resources. When enabled, a source that attempts to download a selected file type is presented with a Block page and the requested file cannot be downloaded.

Secure Access checks a file based on the file's file extension and also evaluates each file to determine its type. For example, if a .gif file extension is changed to .xyz, Secure Access is still able to detect that the file is a .gif file. Thus, if you set your policy rule to block .gif files but allow .xyz files, Secure Access blocks any .gif file that has had its extension changed to .xyz.

File Types to Block

Describes File Types to Block in Cisco Secure Access. As an administrator, you can block certain file types in a security profile.

As an administrator, you can block certain file types in a security profile.

To request that Secure Access add a new file type, contact Cisco Support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Audio	Compressed	Data and Database	Disc and Media	Documents	Executable	Image	System-related	Video
aif cda m4a mid mp3 mpa ram snd wav wma wpl	7z arj deb gz pak pkg rar rar rpm tar.gz tbz z zip	csv dat db log mdb nzb sav sql tar torrent	dmg iso toast vcd	doc docm docx dotm pdf pop potm pptx rtf tex xls xlsm xlsx	apk bat bin cgi com dll exe hta jar js moo msi pif pl prg py sh swf vb vbs vm wsf	ai bmp gif ico jpeg jpg png ps psd rm svg tif tiff	bak cab cpl cur drv emu icns ini ps1 scr sys tmp	avi flv gat h264 m4v mkv mov mp4 mpeg qtm rm rv ssm vob wmv

Enable File Type Controls

Describes Enable File Type Controls in Cisco Secure Access. In Cisco Secure Access, you can manage the file type controls for either internet or private access in the Security profile.

In Cisco Secure Access, you can manage the file type controls for either internet or private access in the Security profile. The file type control settings determine whether an end user can access certain types of files on internet or private destinations.

Important

For internet destinations and internet access rules in the Access policy, Secure Access supports the option to manage the upload, download, or upload and download of file types selected in the Security profile. Secure Access released this option beginning on June 1, 2025 and completing the rollout of the feature on July 31, 2025.

About File Type Controls for Internet Access

In a Security profile, configure the file type controls for files on internet destinations. You can choose whether to control the **upload**, **download**, or **upload and download** of certain types of files. Then, add the Security Profile for internet access to the internet access rules in the Access policy.

If **File Type Blocking** is enabled and a user device attempts to download or upload a selected file type from an internet destination, Secure Access presents a Block page instead of the requested resource.

> **Note**
>
> Blocking some file types may cause a website not to display correctly.

About File Type Controls for Private Access

In a Security profile, configure the file type controls for files on private destinations. You can choose whether to **download** certain types of files. Then, add the Security Profile for private access to the private access rules in the Access policy.

Enable File Type Blocking for Internet Access

Provides instructions for completing the Enable File Type Blocking for Internet Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

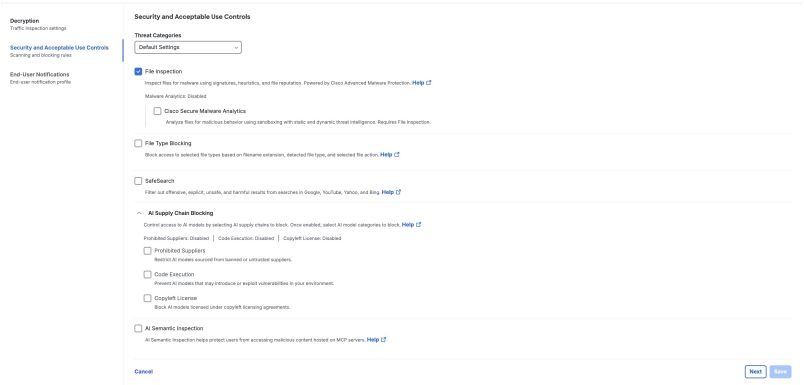
Enable File Type Blocking on internet access rules in the Access policy.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Enable decryption in the same Security profile for internet access where you configure the file type controls.

Procedure

1. Navigate to **Secure** > **Security Profiles**.
2. Click **Add Profile** and then choose **Internet Access**, or expand an existing Security profile.
3. Navigate to **Security and Acceptable Use Controls**, navigate to **File Type Blocking**.

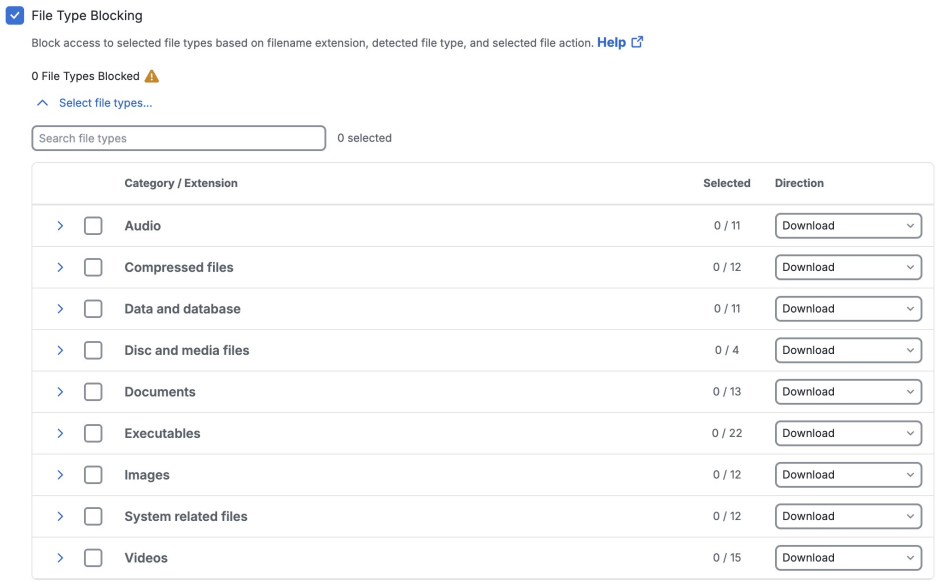


4. For **File Type Blocking**, search for specific file types or choose the file types to block.
   a) Check the categories of the file types to choose all file types in the group, or expand a file type category to choose specific file types.

      For more information about available file types, see File Types to Block.

> **Note**
>
> When an entire file type group is selected, all future file types added to that group are also blocked.

b) Choose either **Upload**, **Download**, or **Both**.



5. Click **Save**.

   Use the Security profile in an internet access rule to apply the file type blocking security controls to the configured destinations.

Enable File Type Blocking for Private Access

Provides instructions for completing the Enable File Type Blocking for Private Access workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Enable File Type Blocking on private access rules in the Access policy.

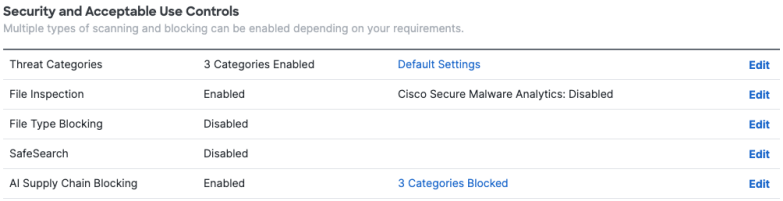
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- In private access rules, configure decryption for private resources as rule destinations.

Procedure

---

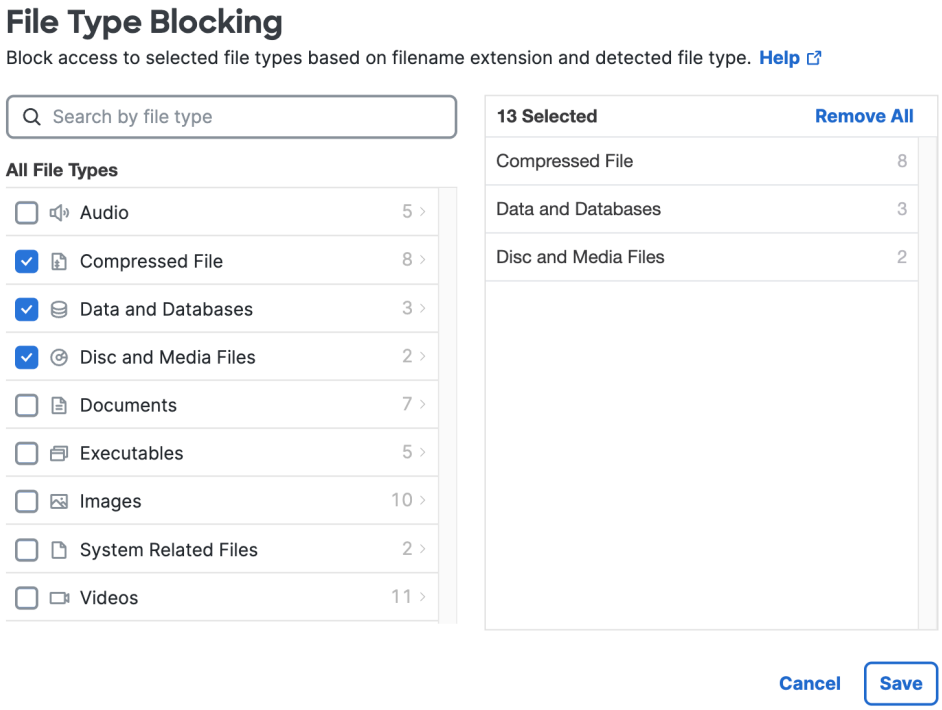
1. Navigate to **Secure** > **Security Profiles**.
2. Click **Add Profile** and then choose **Private Access**, or expand an existing Security profile.
3. Navigate to **Security and Acceptable Use Controls**, navigate to **File Type Blocking**, and then click **Edit**.



4. For **File Type Blocking**, search for specific file types or choose the file types to block.
   a) Check the categories of the file types to choose all file types in the group, or expand a file type category to choose specific file types.

   For more information about available file types, see File Types to Block.

> **Note**
>
> When an entire file type group is selected, all future file types added to that group are also blocked.



5. Click **Save**.

   Use the Security profile in a private access rule to apply the file type blocking security controls to the configured destinations.

Review File Type Controls Through Reports

Provides instructions for completing the Review File Type Controls Through Reports workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

File types enabled through security profiles are listed in the Activity Search Report.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

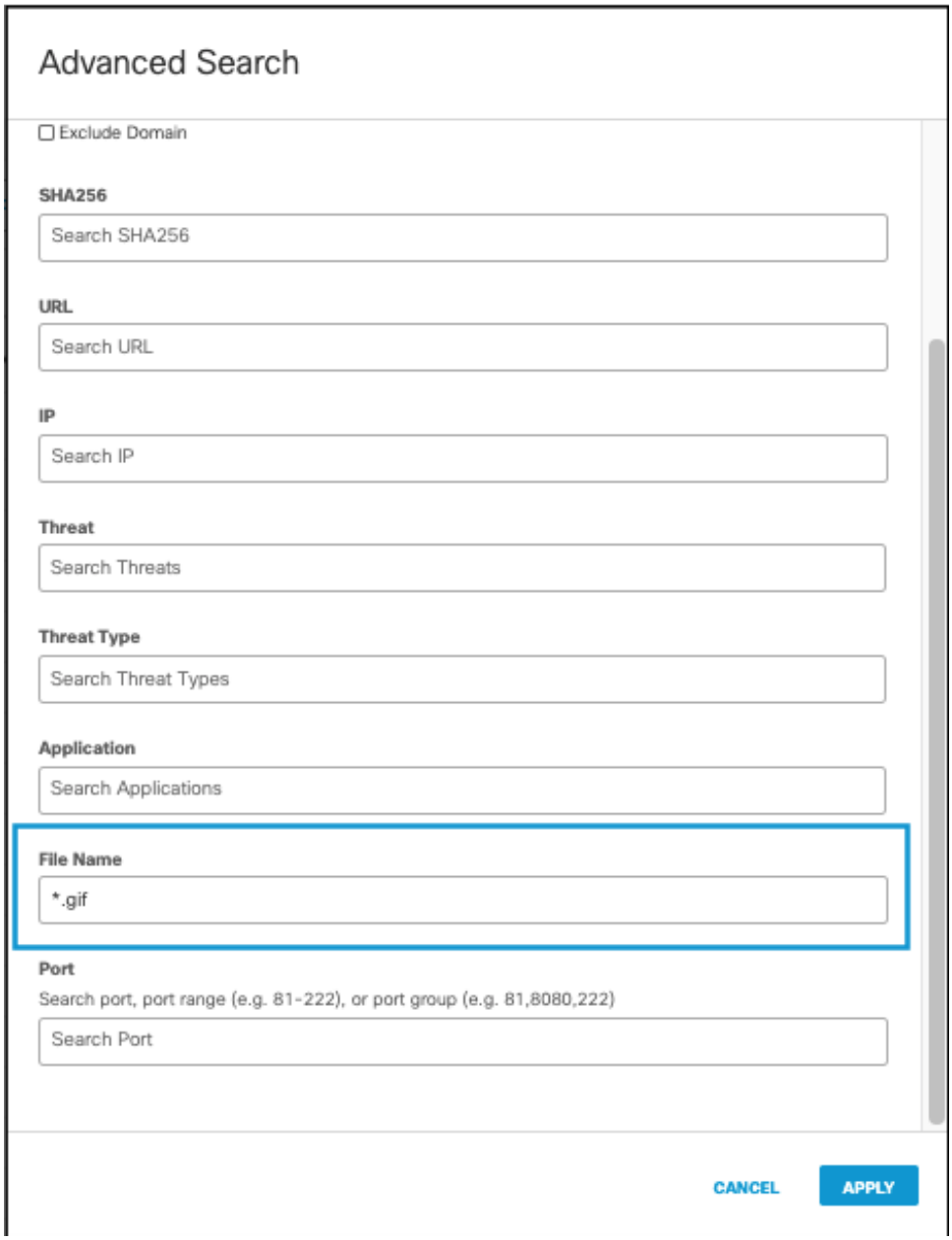
Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. Under the **Response** filter, choose **Blocked**.

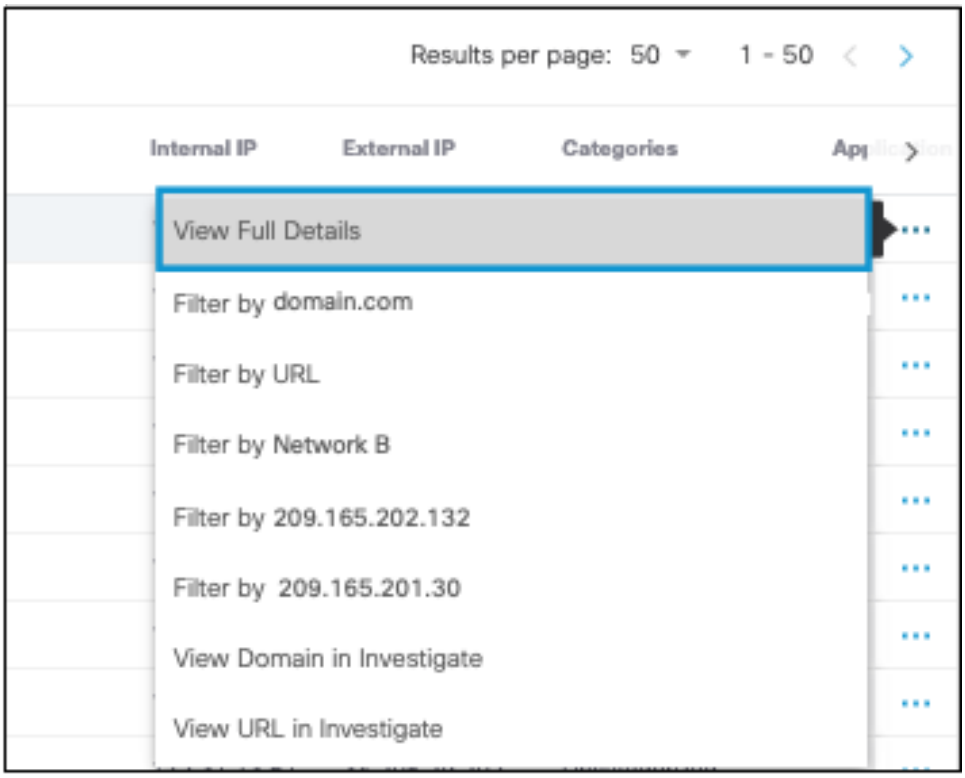


3. Click **Advanced** in the search bar to bring up the Advanced search.
4. Under **File Name**, enter the asterisk wildcard symbol and a file type to search by and then click **Apply**.

   The results will filter by events where files of that type were blocked.



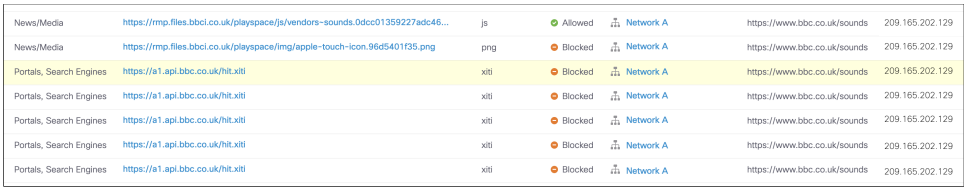
5. Click the action menu and select **View Full Details.**



- View further details of the blocked file, such as the action taken, the name of the file, and the file extension.

  In cases where the file extension is displayed in the file extension column but does not match the extension shown against the file type block control action, the file type control block action should be trusted because it is more accurate and based on the detection engine.

  For example, the file extension listed here is shown as a *.xiti*.



News/Media	https://rmp.files.bbci.co.uk/playspace/js/vendors~sounds.0dcc01359227adc46...	js	Allowed	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
News/Media	https://rmp.files.bbci.co.uk/playspace/img/apple-touch-icon.96d5401f35.png	png	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129
Portals, Search Engines	https://a1.api.bbc.co.uk/hit.xiti	xiti	Blocked	Network A	https://www.bbc.co.uk/sounds	209.165.202.129

When you examine the details, however, you discover that the file type is actually a *.gif*, which was successfully detected and blocked by the File Type Control engine.

42 Notification Pages

Topics:

- Manage Notification Pages

Provides an overview of Notification Pages in Cisco Secure Access, including Manage Notification Pages. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Notification Pages

Describes Manage Notification Pages in Cisco Secure Access. You can configure Cisco Secure Access to display a notification page to users that request internet destinations.

You can configure Cisco Secure Access to display a notification page to users that request internet destinations. Secure Access shows a notification page when:

- A destination is blocked by an internet access rule that has certain configurations in a Security profile. In this case, Secure Access displays a Block page.
- A destination matches an internet access rule that is configured with the **Warn** action. In this case, Secure Access displays a Warn page.

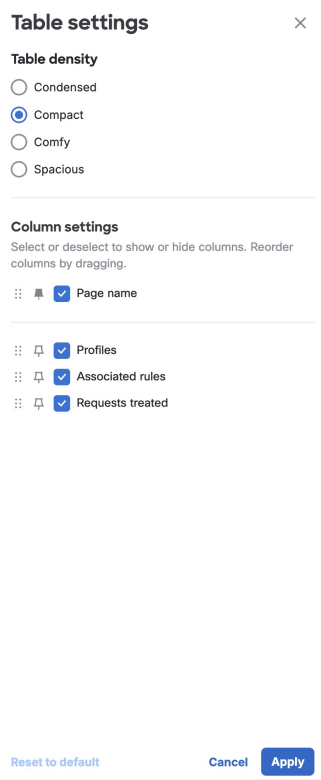
Configure Secure Access to display the default notification page or a custom notification page. You can create one or more custom notification pages to display in different situations. Each Security profile for internet access is associated with the configuration of a single notification page that includes both Block and Warn pages.

Note

The notification pages described in this section do not apply to private access rules in the Access policy. For information about private access rules, see Get Started With Private Access Rules.

Note

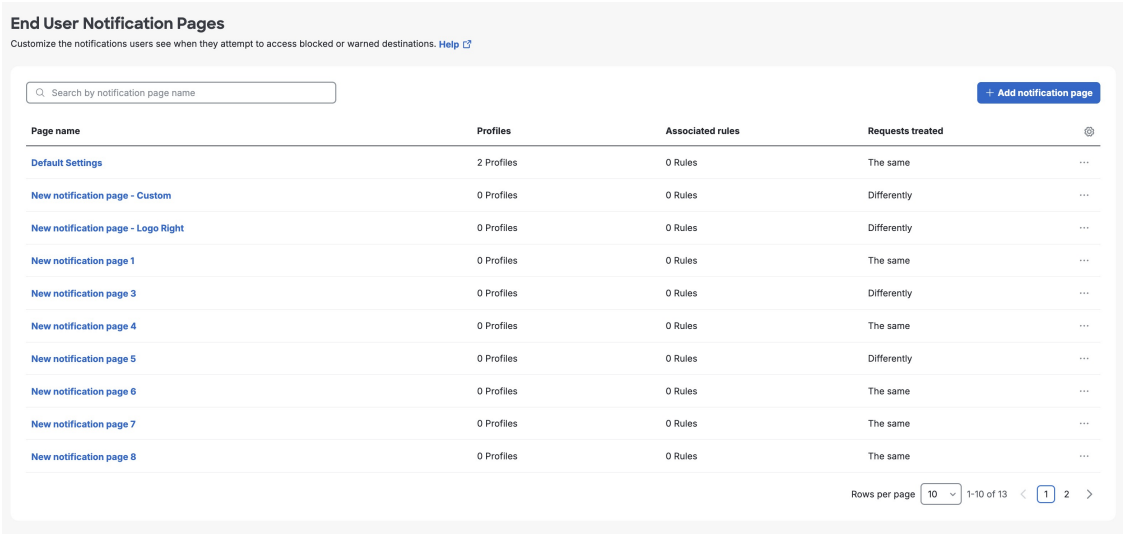
You can pin a specific column or re-arrange columns in your desired layout by clicking on the **Settings** gear icon.



View Notification Pages Displayed to End Users

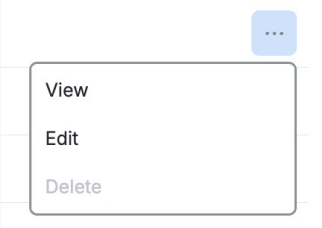
Describes View Notification Pages Displayed to End Users in Cisco Secure Access. In Secure Access you can view the default notification page and any custom notification pages.

In Secure Access you can view the default notification page and any custom notification pages. For more information, see Preview Notification Pages.



Note

You can **View** or **Edit** the Default Settings End User Notification Page, but you cannot **Delete** it.



Display Custom Notification Pages to End Users

- Create custom notification pages for blocked destinations and destinations in internet access rules configured with the Warn action. For more information, see Create Custom Block and Warn Pages.
- Configure one or more Security profiles for internet access to use custom notification pages. For more information, see Add a Security Profile for Internet Access.
- In the default Security profile for internet access, choose to display the block and warn pages when traffic matches internet access rules that use the default profile. For more information about choosing a default Security profile for internet access, see Edit Rule Defaults and Global Settings.
- Configure internet access rules to use the Security profiles, which you have configured to display your custom notification pages. To display a Warn page, choose the **Warn** action in the rule.
- Deploy required certificates. For more information, see Certificates for Internet Decryption.

  If user devices do not have the necessary certificate, users will see the standard browser error when they try to access a blocked destination.

About Warn Pages for Internet Access Traffic

Describes About Warn Pages for Internet Access Traffic in Cisco Secure Access. Secure Access displays a Warn page for destinations where the organization has configured internet access rules with the Warn action.

Secure Access displays a Warn page for destinations where the organization has configured internet access rules with the **Warn** action. The **Display user input field in warning messages** global setting on the Access policy determines whether a user clicks a link on the Warn notification or enters a key word before accessing the destination. For more information about the **Display user input field in warning messages** global settings, see Global Settings for Access Rules.

- The Warn page includes either a link that the user must click to continue to the destination, or if configured a user input field.
- When a user gets access to a destination, the destination is available for one hour. After one hour, Secure Access displays the Warn page again and the user must click on the link or enter **Continue** to access the requested destination.

Warn Page: Click Link and Continue to Destination

If an administrator has not enabled the **Display user input field in warning messages** global setting on the Access policy, Secure Access requires that the user click a link in the Warn notification page, and then access the requested destination.

Warn Page: Enter Key Word and Continue to Destination

Describes Warn Page: Enter Key Word and Continue to Destination in Cisco Secure Access. If an administrator has enabled the Display user input field in warning messages global setting on the Access policy, the user input field appears on the Warn notification page.

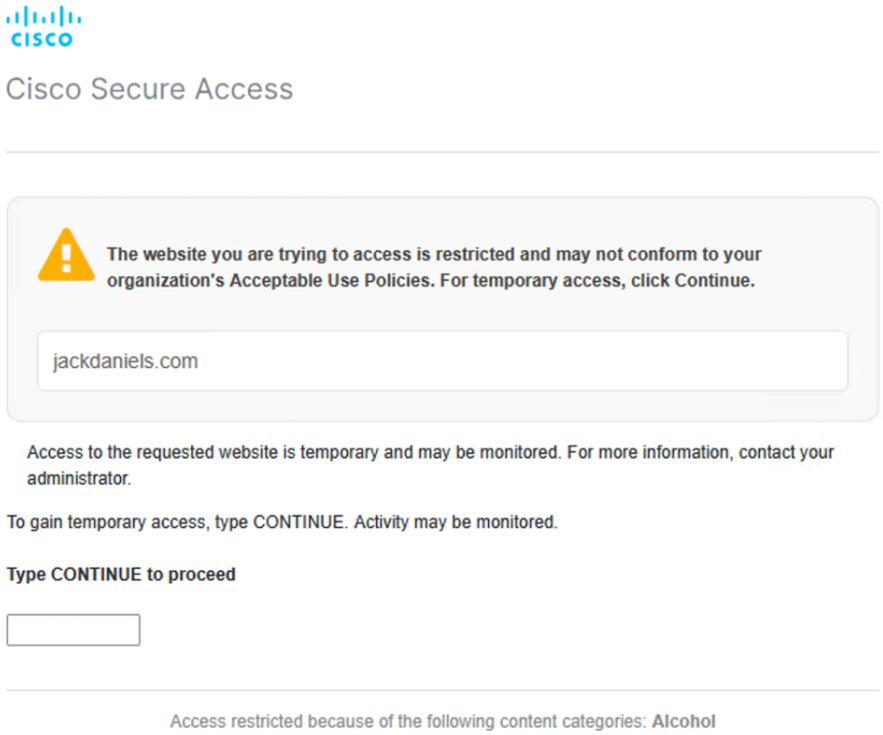
If an administrator has enabled the **Display user input field in warning messages** global setting on the Access policy, the user input field appears on the Warn notification page.

When Secure Access displays the Warn notification page, the user must enter the key word **Continue** to activate the **Continue** button.

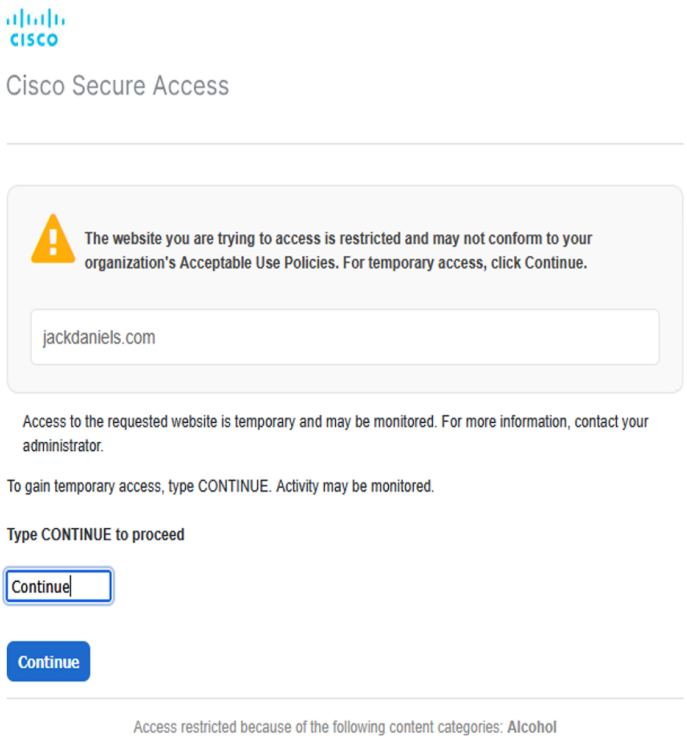
1. Enter **Continue**.

Note

The value of the user input field is a case-insensitive string.



2. Click the **Continue** button to reach the internet destination.



Preview Notification Pages

Preview the system-provided (default) and custom notification pages that Cisco Secure Access displays to users when an internet access rule blocks or warns about a connection. Previewing lets you verify the appearance and content of each page before you apply a security profile.

Cisco Secure Access displays notification pages to users when an internet access rule blocks or warns about a connection. You can preview these pages from two locations:

- A security profile for internet access.
- The **Secure** > **Settings** > **Notification Pages** page.

This procedure describes how to preview notification pages from a security profile for internet access.

> **Note**
>
> The system-provided notification page that a user actually sees depends on the rule configuration and the user's connection method. In most cases, users see the Secure Web Gateway (SWG) proxy block page, but some rule configurations cause the firewall block page to appear instead. For details, refer to System-Provided Notification Pages for Firewall and Secure Web Gateway.

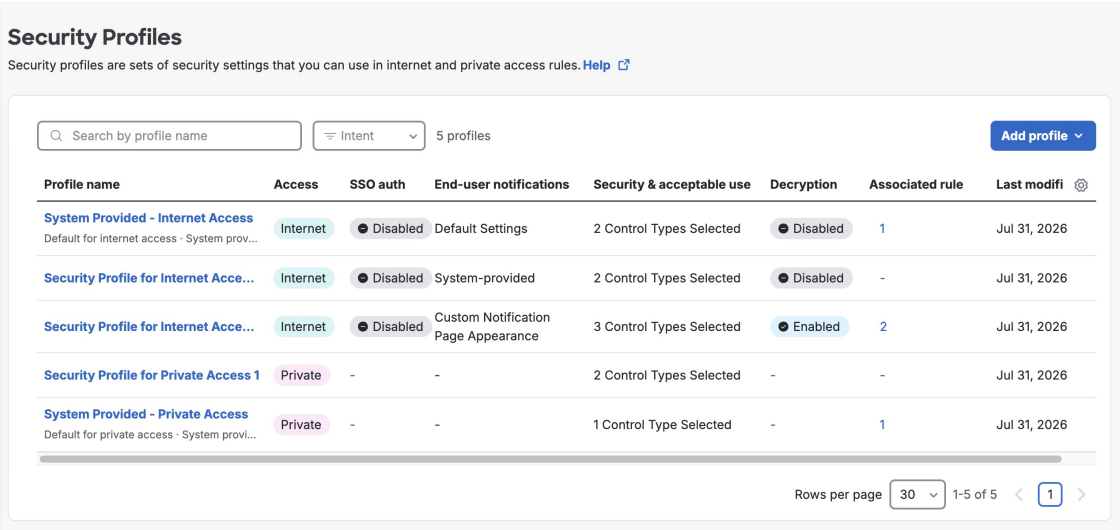
Before you begin

Before you begin, verify the following:

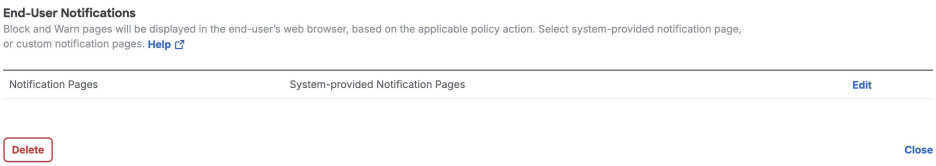
- You have the Full Admin user role. For more information, see Manage Accounts.
- Your organization's DNS resolves to the Secure Access DNS servers.

Procedure

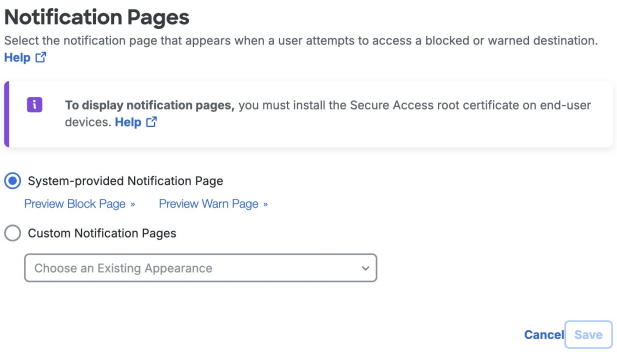
1. In the Secure Access dashboard, navigate to **Secure** > **Security Profiles**.



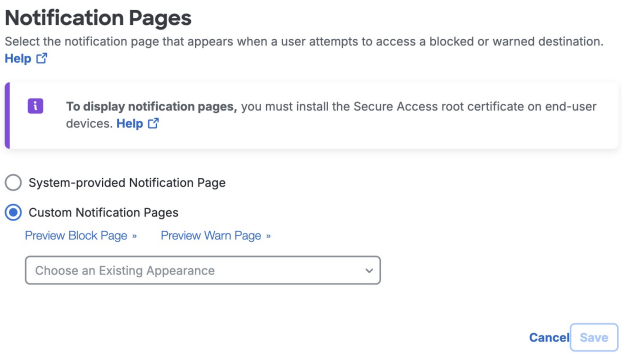
2. Open a security profile for internet access.
   - To preview pages in an existing profile, click the profile name.
   - To preview pages in a new profile, click **Add Profile** > **Internet Access**.
3. Scroll to **End-User Notifications** and click **Edit**.



4. Preview a system-provided notification page.
   a) Select **System-provided Notification Pages**.
   b) Click the **Preview** link next to the Block page or the Warn page.



   c) Review the page that opens in a new browser tab.
5. Preview a custom notification page.
   a) Select **Custom Notification Pages**.
   b) Click **Choose an existing appearance** and select the notification page design that you want to preview.
   c) Click the **Preview** link next to the Block page or the Warn page.



d) Review the page that opens in a new browser tab.

You have previewed the selected notification pages. If the page content or appearance needs to change, edit the custom notification page design or contact your administrator to update the system-provided page text.

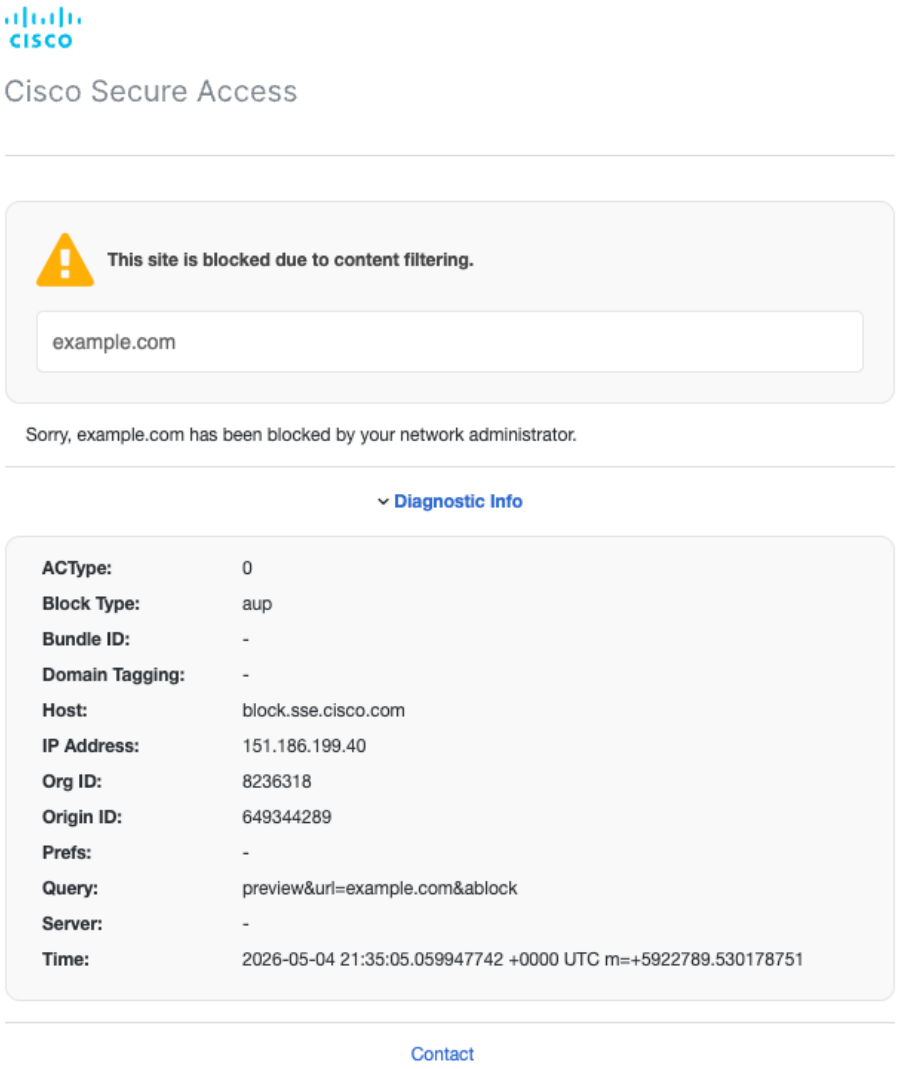
System-Provided Notification Pages for Firewall and Secure Web Gateway

When an internet access rule blocks a user's connection, Secure Access displays either the Secure Web Gateway (SWG) proxy block page or the firewall block page. The SWG proxy block page appears in most cases; the firewall block page appears only when a rule uses a specific combination of destination and network or service criteria.

Default behavior

By default, Secure Access displays the SWG proxy block page when an internet access rule blocks a user's connection. This is the notification page that users see in most scenarios.

Figure 3: SWG proxy block page (default)



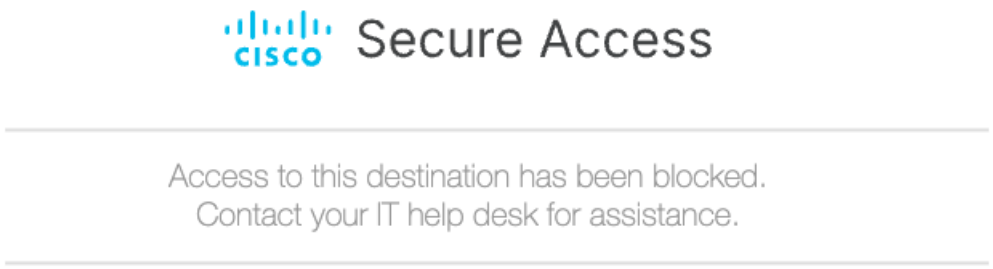
Exception: When the firewall block page appears

Secure Access displays the firewall block page instead of the SWG proxy block page when *all* of the following conditions are true:

- An internet access rule uses a combined destination that includes both of the following:
  - An application list, Destination list, Content category list, internet application, or application category.
  - A network object or group, or a service object or group.
- The rule action is set to **Block**.
- The user connects to Secure Access through one of the following methods:
  - A network tunnel group IPsec tunnel.
  - A remote access VPN tunnel.
  - Client-based zero trust access.
  - A trusted network.

Under these conditions, the user sees the generic firewall block page hosted at accessdenied.sse.cisco.com rather than the SWG proxy block page.

Figure 4: Firewall block page



> **Note**
>
> This behavior results from the combined-destination rule logic introduced for internet access rules. For details about how combined destinations are evaluated, see Combining Multiple Destinations in a Rule (Boolean Logic).

Notification pages at a glance

Table 22: Notification page shown by rule configuration and connection method

Rule Configuration	Connection Method	Notification Page Displayed
Any blocking rule that does *not* combine destination Lists, Application Lists or Content Category Lists with a network or service object.	Any supported connection method, including devices managed by Cisco Secure Client with the Umbrella Roaming Security module or configured with a PAC file.	SWG proxy block page (default).
Blocking rule that combines an application list, Destination list, Content category list, internet application, or application category *with* a network or service object or group.	Network tunnel group IPsec tunnel, remote access VPN tunnel, client-based zero trust access, or a trusted network.	Firewall block page.

Related information

- Combining Multiple Destinations in a Rule (Boolean Logic)
- Manage Network Tunnel Groups
- Manage Virtual Private Networks
- Manage Client-Based Zero Trust Access in Secure Access

- Trusted Networks for Zero Trust Access Connections
- Umbrella Roaming Security Module Requirements
- Manage PAC Files

Create Custom Block and Warn Pages

Describes Create Custom Block and Warn Pages in Cisco Secure Access. Instead of showing end users the default block or warn message with the Secure Access logo, you can display your own logo, custom Block and Warn messages, and an option to contact an administrator.

Instead of showing end users the default block or warn message with the Secure Access logo, you can display your own logo, custom Block and Warn messages, and an option to contact an administrator. You can also display different pages depending on the reason for the block.

You can create a custom Block page and a custom Warn page as a set, and then choose them in security profiles for internet access.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Gather your logo, help desk email address, and any other information you want to provide.
- If you use a custom logo, Secure Access notification pages support PNG and JPEG. Images larger than 125x70 pixels will be cropped and resized.

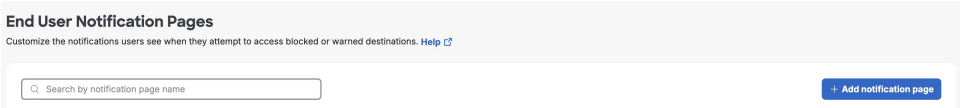
Create Custom Block and Warn Pages

Provides instructions for completing the Create Custom Block and Warn Pages workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Settings** > **Notification Pages**.
2. Click **+ Add notification page**, or expand the setting you want to edit.

   The settings on the page are optional.



3. If this is a new configuration, name this set of notification pages using a maximum of 128 characters.



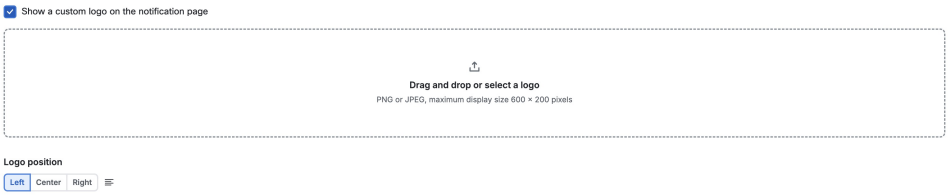
4. Enable **Show diagnostic information that Cisco TAC may need for troubleshooting, such as organization ID, origin ID, query string, and server name. Disabling diagnostic fields may limit support effectiveness.**.

   If you want to allow end users to contact an administrator from a block message, provide the email address that will be used to forward user messages.

   For more information, see Allow Users to Contact an Administrator.

5. Click **Show a custom logo on the block page**.

   Secure Access notification pages support PNG and JPEG. Images larger than 600 x 200 pixels will be cropped and resized. You can select your desired logo position.



6. Expand **Block Page Appearance**.

   a. If you want to display a unique message based on the reason for the block, click **Differently** and click a **Block** reason.

   b. Click **Show a block page with a custom message**.

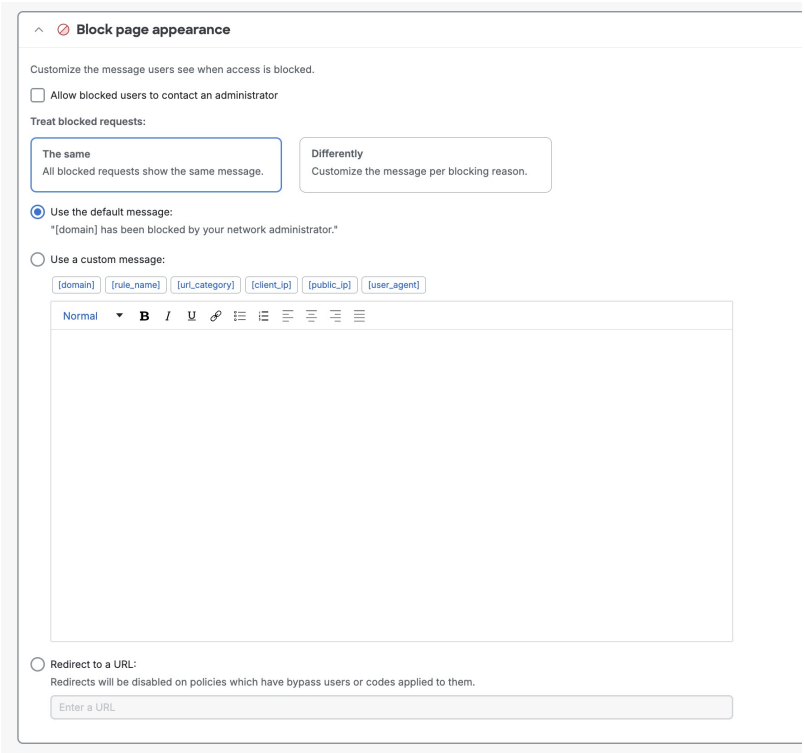
   c. Enter your custom message.

      You can change the size and formatting of your text. Add bold, italic, underline, and strikethrough styles. You can also include hyperlinks, numbered lists, and bulleted lists.

      You can include the following variables within your message.

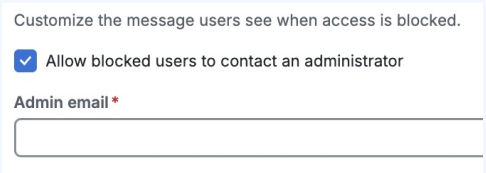
      - **[domain]**–Displays the domain that triggered the block and warn page.
      - **[rule_name]**–Displays the name of the rule that triggered the block or warn page.
      - **[url_category]**–Displays the URL category associated with the blocked or warned destination.
      - **[client_ip]**–Displays the client IP address associated with the request.
      - **[public_ip]**–Displays the public source IP address of the client.
      - **[user_agent]**–Displays information about the browser or client that made the request.

   d. You can redirect users to the URL of your choice by clicking on the radio button and entering the URL.



Note

You can allow users to directly contact their administrators by enabling **Allow blocked users to contact an administrator**.

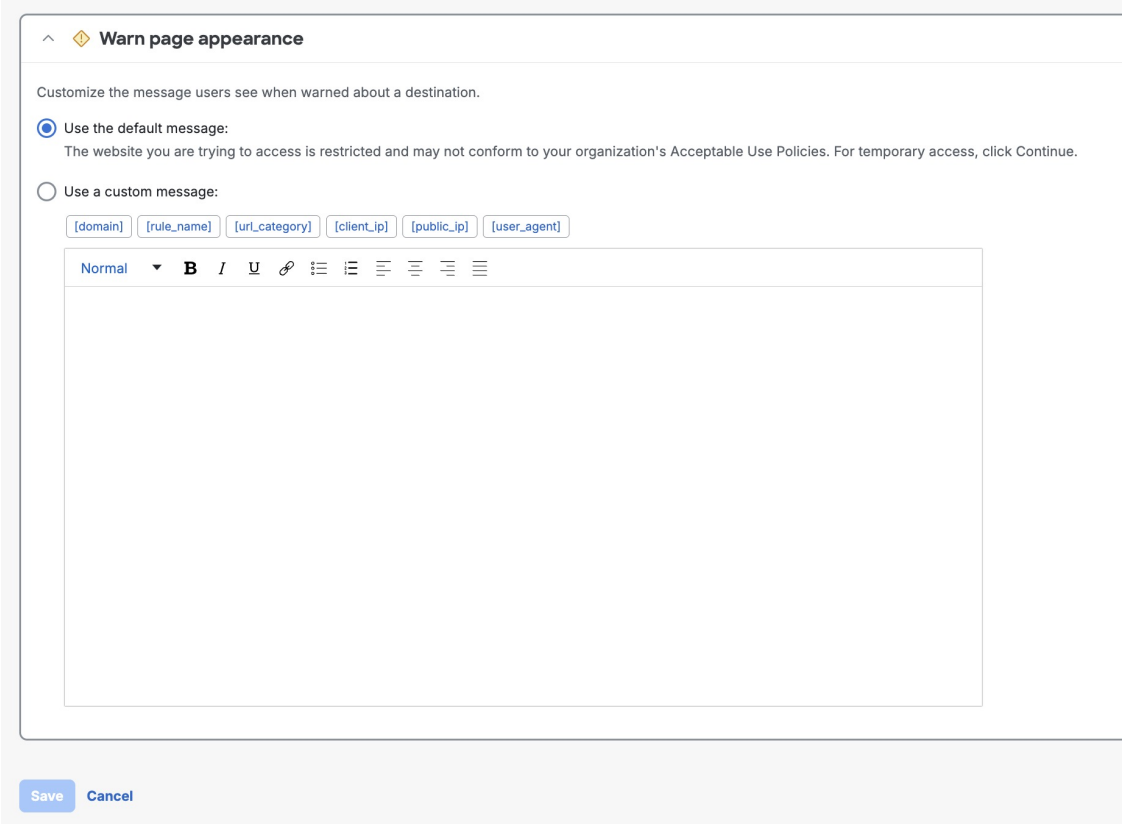


7. Expand **Warn Page Appearance**.
   a. Click **Show a warn page with a custom message**.
   b. Enter your custom message, using the same guidelines as for a custom block message.

      You can change the size and formatting of your text. Add bold, italic, underline, and strikethrough styles. You can also include hyperlinks, numbered lists, and bulleted lists.

      You can include the following variables within your message.

      - **[domain]**–Displays the domain that triggered the block and warn page.
      - **[rule_name]**–Displays the name of the rule that triggered the block or warn page.
      - **[url_category]**–Displays the URL category associated with the blocked or warned destination.
      - **[client_ip]**–Displays the client IP address associated with the request.
      - **[public_ip]**–Displays the public source IP address of the client.
      - **[user_agent]**–Displays information about the browser or client that made the request.



8. Preview your notification pages:
   a. Scroll to the top of your configuration.
   b. Click the **Preview Block Page** or **Preview Warn Page** links.



9. Click **Save**.

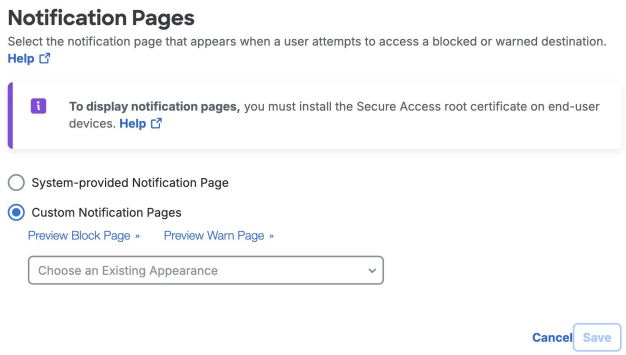
Link a Custom Notification Page Appearance to a Security Profile

Provides instructions for completing the Link a Custom Notification Page Appearance to a Security Profile workflow in Cisco Secure Access. Navigate to Secure Security Profiles and expand the profile you'd like to link.

Procedure

---

1. Navigate to **Secure** > **Security Profiles** and expand the profile you'd like to link.
2. Under **End-User Notifications** click **Edit** for **Notification Pages**.



3. Choose **Custom Notification Pages**, and then choose the notification page appearance to get the set of block and warn pages.
4. Click **Save**.

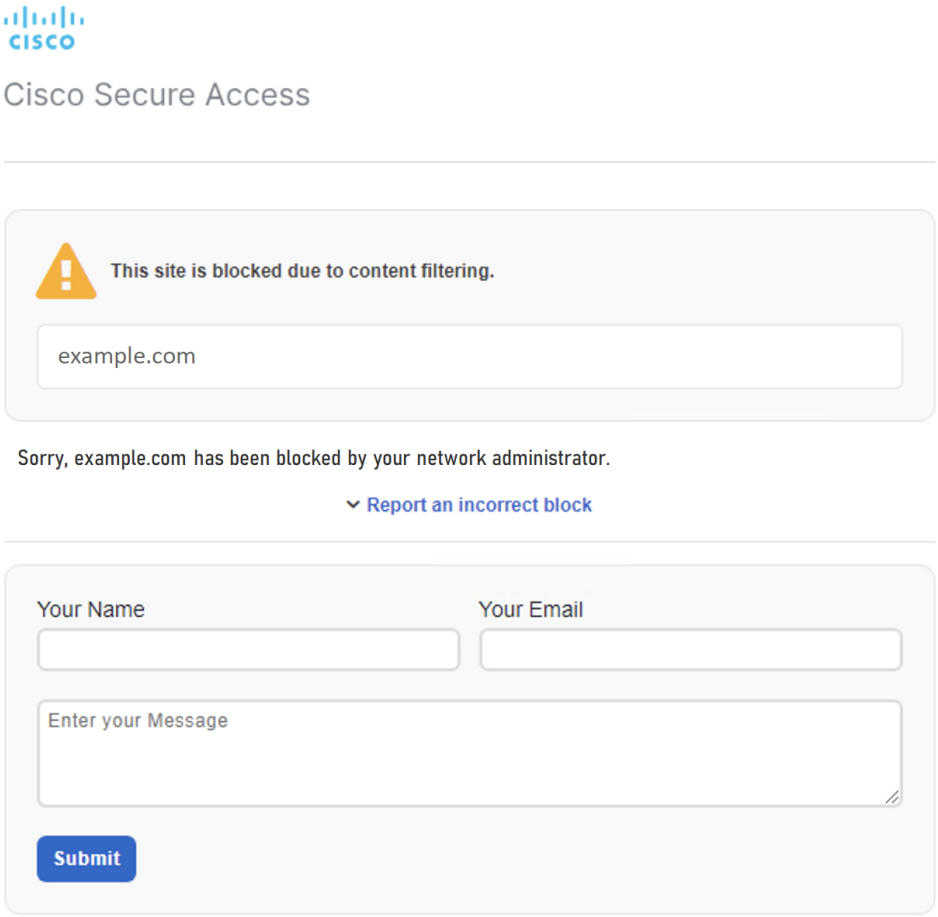
What to do next

Complete the remaining requirements described in Manage Notification Pages.

Allow Users to Contact an Administrator

Describes Allow Users to Contact an Administrator in Cisco Secure Access. If you configure Secure Access to allow end users to contact an administrator from the block page, users can notify you if they feel a website should not be blocked.

If you configure Secure Access to allow end users to contact an administrator from the block page, users can notify you if they feel a website should not be blocked. When end users attempt to access blocked sites, Secure Access includes a contact form at the bottom of block notifications:



After the end user submits the form, Secure Access sends an email message to the administrator address you provided, including the user's message and diagnostic information that helps you determine whether to allow access to the site.

Tip

Assistance With Allowing Websites

If you are unsure if a website should be allowed or have questions about a domain classification, contact Support.

Procedure for Allowing Users to Contact an Administrator

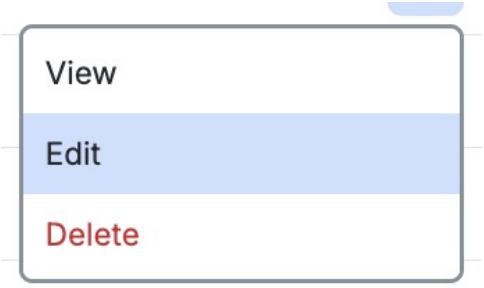
Provides instructions for completing the Procedure for Allowing Users to Contact an Administrator workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

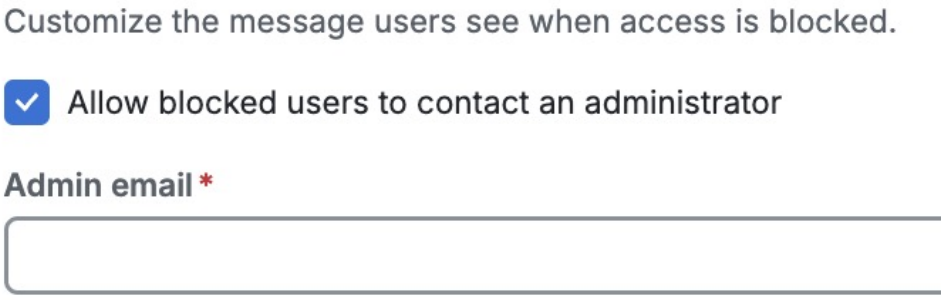
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Notification Pages**.
2. Navigate to a notification page and click **Edit**.



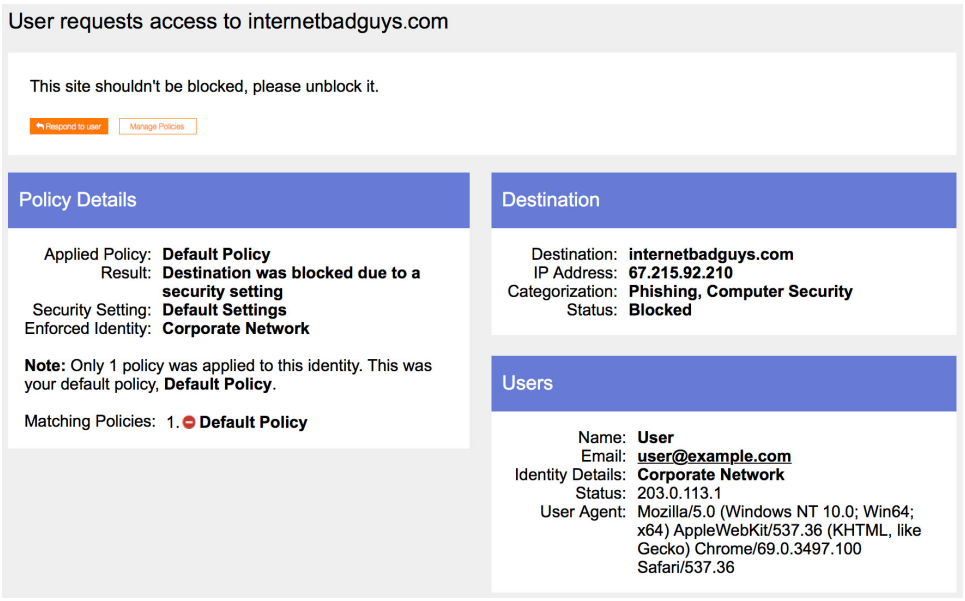
3. Select **Allow blocked users to contact an admin from the block page** to allow end-users to contact an administrator from your organization. You can only add one email.



4. Click **Save**.

What to do next

The following is an example of an email sent to an administrator when a user sent a message from a block page:



Block Page IP Addresses

Describes Block Page IP Addresses in Cisco Secure Access. When Secure Access blocks a domain or URL, the Secure Access DNS servers display a block page instead of the requested page.

When Secure Access blocks a domain or URL, the Secure Access DNS servers display a block page instead of the requested page. Secure Access provides different types of block pages depending on the security event.

IP Addresses for Secure Access Block Pages

The following table describes the types of block pages, DNS record types, and Anycast IP addresses for the Secure Access servers.

Block Page Type	Record Type	IP Address
Domain List	A	146.112.61.113
Domain List	AAAA	2620:119:18::115
Command and Control Callback	A	146.112.61.114
Command and Control Callback	AAAA	2620:119:18::114
Content Category or Application	A	146.112.61.115
Content Category or Application	AAAA	2620:119:18::115
Malware	A	146.112.61.116
Malware	AAAA	2620:119:18::116
Phishing	A	146.112.61.117
Phishing	AAAA	2620:119:18::117
Security Integrations, Newly Seen Domains, DNS Tunneling VPN, Potentially Harmful, and Dynamic DNS	A	146.112.61.119
Security Integrations, Newly Seen Domains, DNS Tunneling VPN, Potentially Harmful, and Dynamic DNS	AAAA	2620:119:18::119

Domains for Secure Access Block Pages

Secure Access displays block pages on these domains:

- **block.sse.cisco.com**
- **phishing.block.sse.cisco.com**
- **malware.block.sse.cisco.com**

43 Data Loss Prevention

Topics:

- Manage the Data Loss Prevention Policy
- Add a Real Time Rule to the Data Loss Prevention Policy
- Add a SaaS API Rule to the Data Loss Prevention Policy
- Add an AI Guardrails Rule to the Data Loss Prevention Policy
- Integrate Email Threat Defense with Secure Access DLP
- Add an Email Rule to the Data Loss Prevention Policy
- Discovery Scan
- Edit a Data Loss Prevention Rule
- Delete a Data Loss Prevention Rule
- Enable or Disable a Data Loss Prevention Rule
- Manage Global Settings

Provides an overview of Data Loss Prevention in Cisco Secure Access, including Manage the Data Loss Prevention Policy and Add a Real Time Rule to the Data Loss Prevention Policy. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage the Data Loss Prevention Policy

Describes Manage the Data Loss Prevention Policy in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Tip**
>
> **Secure Access Packages and Feature Availability**
>
> Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Current Package. If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. For more information, click Cisco Secure Access Packages.

The Data Loss Prevention (DLP) policy helps protect sensitive data uploaded to the web or transferred to external devices like a USB storage device, a Bluetooth device, a network share, or when a file is printed to a local or a network printer. It discovers and protects sensitive data stored and shared in your cloud-sanctioned applications.

You can configure the DLP policy with multiple DLP rules. **Real Time** DLP rules inspect web traffic passing through the proxy or files transferred to external devices like a USB storage device, a Bluetooth device, a network share, or when a file is printed to a local or a network printer. **SaaS API-based** rules ensure data protection of data in the cloud. **AI Guardrails** rules ensure data protection in prompts and responses exchanged with AI applications. Furthermore, DLP Administrators can initiate on-demand Discovery Scans to learn about all the files in the applicable cloud applications that contain matches with the selected Data Classifications. **Email DLP** rules provide DLP functionality to enhance protection provided to outgoing emails by Cisco's Secure Email Threat Defense.

- Real Time Rules: are added to the policy to define which web proxy traffic or files to monitor (identities and destinations), the content or document properties to search for, and whether to monitor or block the specified content. For example, an office may want to monitor its network for file uploads that include credit card numbers, as the uploads are a breach of the company's privacy and security policies. A Real Time DLP rule designed to monitor the network and uploads to domains can block these files.
- SaaS API Rules: operate by leveraging the APIs of the applicable cloud tenants to scan and look for data violations in the cloud-stored files. As files in the selected tenant change in content or context (with whom we share), Secure Access near-time assesses the changed file against this rule's criteria. If a match is made, this rule's action is immediately enforced.
- AI Guardrails Rules indicate which generative AI applications to monitor for specific types of data: sensitive data, inappropriate content, or content that presents a safety or security risk. Prompts, responses, and files embedded within prompts exchanged with selected AI applications can be monitored and potentially blocked, depending on rule settings.
- Email DLP Rules coordinate with Cisco's Secure Email Threat Defense, analyzing the content of outgoing cloud-native email and enhancing the protection Email Threat Defense provides by adding Data Loss Prevention. DLP scans email and monitors or blocks emails that match rule criteria that define violations. To use this feature, you must generate DLP API keys within Secure Access, and use those keys to enable DLP in Email Threat Defense. More more details, see Integrate Email Threat Defense with Secure Access DLP.

Data violations detected through DLP rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Discovery Scans operate similarly to the SaaS API rules; they exercise the necessary cloud APIs to determine the files in the applicable cloud tenant that contain data matching any of the configured Data Classifications at the time the scan runs. Files containing matching data are considered to be in violation of the Discovery Scan.

The Discovery tab in the Data Loss Prevention Report lists the files in violation of the most recently initiated Discovery Scan. Additionally, DLP Administrators can quickly retrieve the reported offending files from any of the last 10 generated Discovery Scans.

Realtime DLP rules support scanning traffic isolated by the RBI (Remote Browser Isolation) in the outbound direction, in addition to scanning non-isolated HTTPs traffic. When the system detects a DLP violation in RBI traffic, a pop-up dialog appears in the user's browser indicating the content has been blocked due to a potential data security violation.

Real Time rules, SaaS API rules, AI Guardrails rules, Email rules, and Discovery Scans all support scanning embedded files.

Limitations

1. The rate limit is dependent on vendor SLA, which is usually up to 10 RPS for Microsoft 365 and up to 20 RPS for Google Drive.
    - The Discovery Scan can scan up to 36,000 files per hour and 864,000 files per day with an average file size of 1MB.
    - The incremental scan and Discovery Scan share the same rate limits, therefore, file changes (i.e. incremental) during the Discovery Scan are counted and have an effect on the Discovery Scan throughput.
    - An org that triggers more than 864k events per day will be at risk of not having all their events scanned.
2. Triggering a Discovery Scan should take place around 24 hours after the tenant authorization, as the system needs time to evaluate and enumerate the users in the organization. Any triggering beforehand might not include all users and hence, the system is unable to scan all files.
3. The DLP scans the plain text of files up to 50 MB.
4. DLP scans archives as well as files containing embedded files. For these, DLP can extract and scan content for up to 100 files nested up to 10 levels deep.
5. Revoke share for internal or external works only for organizations with one domain in Google Drive due to Google API limitation.

Best Practices for the Data Loss Protection Policy

Describes Best Practices for the Data Loss Protection Policy in Cisco Secure Access. Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection.

Some of the Data Loss Prevention policy's built-in identifiers have the potential to produce false positives if not customized to narrow the scope of the inspection. The following are recommended to reduce the number of false positives in these classifications. For more information on customizing an identifier, see Copy and Customize a Data Identifier.

Threshold

The default threshold for built-in identifiers without tolerance is 1. This means that the policy will search for content where the identifier is met only once within a file. Increasing the threshold will scan content for instances where the identifier is met more than once, creating fewer false positives for each individual instance of the identifier. A threshold of 10, for example, only monitors or blocks a file if 10 instances of the identifier are found in the file.

Proximity Terms

Proximity keywords reduce false positives by requiring identifiers to match within 10 terms of specified words.

For example, a Canadian bank account identifier will search for a pattern matching Canadian bank account numbers and transit numbers. A document containing several random numbers matching that pattern could produce false positives, however, if proximity terms such as "Canada" and "bank" are added to the customized identifier, the scope of the inspection is reduced.

Supported File and Form Types

Details the behavior of DLP rules configured with File Control using custom file size thresholds and no Data Classification, explaining that the Monitor action excludes logging uploads for specific common MIME types to prevent report flooding, while the Block action logs all uploads regardless of MIME type.

The Data Loss Prevention policy can monitor or block the data being uploaded to the web. The policy discovers and protects sensitive data contained in your cloud-sanctioned applications. The DLP scans the plain text of files up to 50 MB. DLP also scans archives and files containing embedded files. For these, DLP can extract and scan up to 100 files, nested up to 10 levels deep. Secure Access scans all files uploaded through the Secure Access SWG proxy that match the criteria for Real Time rules and scans files stored in Secure Access authorized cloud tenants. It performs a deeper analysis for these mime types:

MIME Type	File Type	Supported for Internet Traffic	Suppor for Private Traffic
application/catia	CATIA_CAD	Yes	
application/coreldraw	COREL_DRAW	Yes	
application/dca-fft	IBM DCA/FFT	Yes	
application/dca-rft	IBM DCA/RFT	Yes	
application/dicom	DICM	Yes	Yes
application/gzip	GZ	Yes	Yes
application/illustrator	ADOBE_ILLUSTRATOR	Yes	
application/java-archive	JAVA_ARCHIVE	Yes	Yes
application/msword	Word .doc, .docx	Yes	Yes
application/pdf	PDF	Yes	Yes
application/postscript	Postscript .ps	Yes	
application/pro-e	PRO_ENGINEER	Yes	
application/rtf	RTF	Yes	Yes
application/sldworks	SOLIDWORKS	Yes	
application/x-tar	POSIX_TAR	Yes	Yes
application/vnd.apple.keynote	Apple iWork Keynote .key	Yes	
application/vnd.apple.keynote.13	APPLE_KEYNOTE	Yes	
application/vnd.apple.numbers	Apple iWork Numbers .numbers	Yes	
application/vnd.apple.pages	Apple iWork Pages .pages	Yes	
application/vnd.framework3	FRAMEWORK_SPREADSHEET	Yes	
application/vnd.hancell	HANCOM_OFFICE_HANCELL	Yes	
application/vnd.hp-pcl	Printer Command Language	Yes	
application/vnd.lotus-1-2-3	LOTUS_1_2_3	Yes	
application/vnd.ms-cab-compressed	MICROSOFT_CABINET_ARCHIVE	Yes	
application/vnd.ms-excel	Excel .xlsx	Yes	Yes
application/vnd.ms-excel.addin.macroenabled.12	Excel Add-In with Macro .xlam	Yes	

MIME Type	File Type	Supported for Internet Traffic	Suppor for Private Traffic
application/vnd.ms-excel.sheet.binary.macroenabled.12	Excel Binary with Macro .xlsb	Yes	
application/vnd.ms-excel.sheet.macroenabled.12	Excel with Macro .xlsm	Yes	
application/vnd.ms-excel.template.macroenabled.12	Excel Template with Macro .xltm	Yes	
application/vnd.ms-resourcefile	Windows Resource File	Yes	
application/vnd.openxmlformats-officedocument.spreadsheetml.template	Excel Template .xltx	Yes	
application/vnd.openxmlformats-officedocument.wordprocessingml.template	Word Template .dotx	Yes	
application/vnd.ms-outlook	Microsoft Outlook .msg	Yes	
application/vnd.ms-outlook-olk15-msgsource	Microsoft Outlook for Mac Message Source	Yes	
application/vnd.ms-paint	IMAGE_MS_PAINT	Yes	
application/vnd.ms-powerpoint	PowerPoint .ppt	Yes	Yes
application/vnd.ms-visio.drawing	MICROSOFT_VISIO_DRAWING	Yes	
application/vnd.ms-word.document.macroenabled.12	Word with Macro .docm	Yes	Yes
application/vnd.ms-works	MICROSOFT_WORKS	Yes	
application/vnd.ms-xpsdocument	MICROSOFT_XPS	Yes	Yes
application/vnd.oasis.opendocument.presentation	OpenDocument Presentation .odp	Yes	
application/vnd.oasis.opendocument.spreadsheet	OpenDocument Sheet .ods	Yes	
application/vnd.oasis.opendocument.text	OpenDocument Word .oth	Yes	
application/vnd.openxmlformats-officedocument.presentationml.presentation	PowerPoint .pptx	Yes	Yes
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Excel .xlsx	Yes	
application/vnd.paradox	PARADOX_DATABASE	Yes	
application/vnd.prowrite	Professional Write	Yes	
application/vnd.rar	RAR archive format .rar	Yes	Yes
application/vnd.tcpdump.pcapng	PCAP	Yes	Yes
application/vnd.visio	MICROSOFT_VISIO	Yes	
application/vnd.wordperfect; version=4.2	WordPerfect 4.2	Yes	Yes
application/vnd.wordperfect; version=5.0	WordPerfect 5.0	Yes	Yes

MIME Type	File Type	Supported for Internet Traffic	Suppor for Private Traffic
application/vnd.wordperfect; version=5.1	WordPerfect 5.1	Yes	Yes
application/vnd.wordperfect; version=6.x	WordPerfect 6	Yes	Yes
application/vnd.wordstar; version=5	WordStar 5	Yes	
application/vnd.wordstar; version=2000	WordStart 2000	Yes	
application/vnd.xy-write	XyWrite	Yes	
application/x-dbf	DBASE_DATABASE	Yes	
application/x-hwp	Hangul	Yes	Yes
application/x-isys-index	ISYS_INDEX_FILE_ISYS_IX	Yes	
application/x-mathcad	MATHCAD	Yes	
application/x-msaccess	MICROSOFT_ACCESS_DATABASE_MDB	Yes	Yes
application/x-mswrite	Windows Write	Yes	
application/x-step	STEP_3D_CAD	Yes	
application/x-adobe-indesign	ADOBE_INDESIGN	Yes	
application/x-ace-compressed	ACE_ARCHIVE	Yes	
application/x-alz-compressed	ALZ_ARCHIVE	Yes	Yes
application/x-archive	UNIX_AR_ARCHIVE	Yes	
application/x-arj	ARJ_ARCHIVE	Yes	Yes
application/x-bzip	bz	Yes	
application/x-bzip2	bz2	Yes	
application/x-compress	COMPRESS_ARCHIVE_Z	Yes	
application/x-corelpresentations	COREL_PRESENTATION	Yes	
application/x-cpio	CPIO_UNIX_ARCHIVE	Yes	
application/x-dosexec+rar	RAR_ARCHIVE_SFX	Yes	
application/x-dosexec+zip	ZIP_ARCHIVE_SFX	Yes	
application/x-dosexec+7z	SEVEN_ZIP_ARCHIVE_SFX	Yes	
application/x-egg-compressed	EGG_ARCHIVE_EGG	Yes	Yes
application/x-iso9660-image	ISO_DISK_IMAGE	Yes	
application/x-jt	JT_CAD	Yes	
application/x-lha	LHA_ARCHIVE	Yes	
application/x-lzh	LZH_ARCHIVE	Yes	
application/x-msbinder	MICROSOFT_BINDER	Yes	
application/x-ms-object	Microsoft Outlook MSO object	Yes	
application/msonenote	ONE	Yes	Yes
application/x-ms-outlookexpress	Microsoft Outlook Express	Yes	

MIME Type	File Type	Supported for Internet Traffic	Suppor for Private Traffic
application/x-quattro-pro	QUATTRO_PRO_SPREADSHEET	Yes	
application/x-rpm	RPM_PACKAGE	Yes	
application/x-stuffitsea	STUFFIT_SELF_EXTRACTING_ARCHIVE	Yes	
application/x-stuffit	STUFFIT_ARCHIVE	Yes	Yes
application/x-stuffitx	STUFFIT_X	Yes	
application/x-tar	Tape archive .tar	Yes	
application/x-xz	XZ_ARCHIVE	Yes	
application/x-7z-compressed	7 Zip Format .7z	Yes	Yes
application/zip	Zip archive .zip	Yes	Yes
audio/mpeg	AUDIO_MPEG	Yes	
image/bmp	BMP	Yes	Yes
image/brk	IMAGE_BROOKTROUT_FAX	Yes	
image/cgm	CGM	Yes	
image/emf *	EMF	Yes	
image/iff	IMAGE_IFF	Yes	
image/jpeg	JPEG	Yes	Yes
image/jpeg	JPG	Yes	Yes
image/gif	GIF	Yes	Yes
image/png	PNG	Yes	Yes
image/sgi	SGI_IMAGE_FILE	Yes	
image/starview-metafile	STARVIEW_METAFILE_SVM	Yes	
image/svg+xml	SCALABLE_VECTOR_GRAPHIC	Yes	
image/tiff	TIFF	Yes	Yes
image/vnd.adobe.photoshop	PSD	Yes	Yes
image/vnd.dgn	INTERGRAPH_MICROSTATION_CAD_DGN	Yes	
image/vnd.dwg	AUTODESK_AUTOCAD	Yes	Yes
image/vnd.dxf	AUTOCAD_DXF	Yes	
image/vnd.imnet-c4	IMNET_MEDICAL	Yes	
image/vnd.microsoft.icon	ICO	Yes	Yes
image/vnd.ms-modi	IMAGE_MDI	Yes	
image/vnd.wap.wbmp	WBMP	Yes	
image/webp	WEBP	Yes	
image/wmf *	WMF	Yes	

MIME Type	File Type	Supported for Internet Traffic	Suppor for Private Traffic
image/wmf	WINDOWS_METAFILE_WMF	Yes	Yes
image/x-bitmap	XBM	Yes	
image/x-cals	CALS	Yes	
image/x-macpaint	IMAGE_MAC_PAINT	Yes	
image/ncr	IMAGE_NCR	Yes	
image/x-paintshoppro	IMAGE_PAINTSHOP_PRO	Yes	
image/x-pcx	PCX	Yes	
image/x-pict	PICT	Yes	
image/x-portable-bitmap	PBM	Yes	
image/x-tga	TGA	Yes	
image/x-xpixmap	XPM	Yes	
image/x-xwindowdump	IMAGE_X_WINDOW_SYSTEM_SCREEN_DUMP	Yes	
message/rfc822	E-mail	Yes	Yes
model/iges	IGS_CAD	Yes	
model/prt	PRO_ENGINEER_MODEL	Yes	
model/vnd.dwf	AUTODESK_WHIP	Yes	
model/vnd.parasolid.transmit.binary	PARASOLID_MODEL_PART	Yes	
model/x.stl-ascii	STEREOLITHOGRAPHY_CAD_TEXT	Yes	
model/x.stl-binary	STEREOLITHOGRAPHY_CAD_BINARY	Yes	
multipart/related	Microsoft Web Archive	Yes	
text/csv	CSV	Yes	Yes
text/html	HTML/XML	Yes	
text/obj-cad	OBJ_3D_IMAGE	Yes	
text/plain**	Plain text .txt	Yes	
text/plain**	UNIX_SCRIPT	Yes	Yes
text/rtf	RTF	Yes	
text/tab-separated-values	TSV	Yes	
text/url	URL	Yes	

** Plain text files, such as plain text .txt and UNIX_SCRIPT, as well as JSON files, are not supported when the file type is used as the only matching criterion. They are supported only when combined with other matching criteria.

* EMF and WMF are wrapper file types. In DLP reports, these files display as the types of the files they contain: PNG or JPG.

Real Time DLP rules can scan the content of all applicable web requests of these form types:

- JSON
- XML
- URL-encoded
- Multipart form

Note

The DLP engine decompresses and scans 10 levels of sub-folders in the zipped and archive types for both Real time and SaaS API DLP.

Note

Optical Character Recognition (OCR) supports scanning and extracting text from supported image file types, including BMP, BRK, CGM, DCX, EMF, GEM, GIF, IFF, IMNET, JEDICS, JPEG, JPG, JPK, JXR, MACPAINT, MDI, MSPAINT, NCR, PBM, PCX, PICT, PNG, PSP, SVM, TGA, TIFF, WBMP, WEBP, WMF, and XWD. OCR also scans from scanned PDFs and images embedded in files such as Excel spreadsheets, PowerPoint presentations, Word documents, PDFs, and ZIP files.

Secure Access supports scanning images with a minimum resolution of 300 dpi and a minimum font size of 10 points. Once text is extracted, it is scanned against all configured DLP rule types for violations. OCR supports multiple languages. For more information on configuring OCR scanning, see Manage Global Settings.

Monitoring DLP Rules That Use Only File Size Without Data Classification

When a DLP rule is configured using **File Control** with a custom **File Size** threshold and no **Data Classification**, and the action is set to **Monitor**, uploads for certain MIME types are not logged intentionally. This exclusion applies to these MIME types:

- text/plain
- application/octet-stream
- application/json
- application/x-ndjson
- application/reports+json
- application/dns-message
- application/protobuf
- application/x-protobuf
- message/ohttp-req
- application/csp-report

Important

The **Block** action logs all uploads regardless of MIME type.

This behavior is intended and applies only to file-size-only rules, without Data Classification.

Understand Exclusions in a Real Time Rule

Describes Understand Exclusions in a Real Time Rule in Cisco Secure Access. The Data Loss Prevention policy evaluates all active Real Time rules against the web requests in your environment.

The Data Loss Prevention policy evaluates all active Real Time rules against the web requests in your environment. Upon determining that a web request matches the identity and destination criteria of a Real Time rule, Secure Access then inspects the web request for matches with the rule's configured data classifications and file labels. Exclusions enable you to narrow your data criteria monitoring to specific applications and destinations. For example, if you have the rule to monitor data classifications for an application, but want to exclude some domains or URLs from being scanned, you can exclude a destination list with those domains. Traffic through that application will be scanned with the exception of the destination list excluded.

Within the context of a Real Time rule, exclusions will always override inclusions. For example, if a rule states that a domain on one list is excluded but the same domain is included on another destination list, the domain will automatically be excluded from the rule.

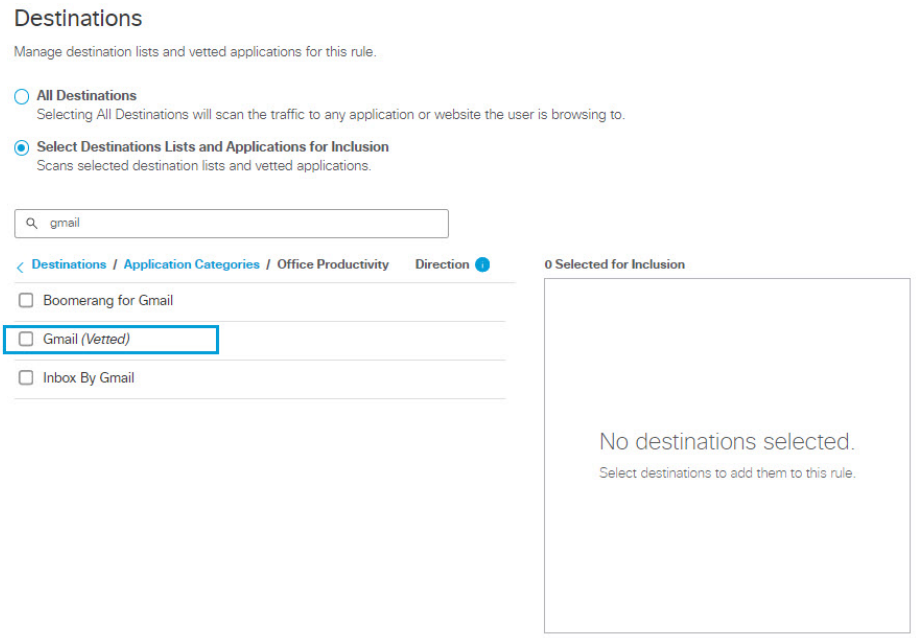
Supported Applications

Describes Supported Applications in Cisco Secure Access. The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy.

The Real Time DLP rules inspect the content of all Secure Access proxied web requests matching the resources and destinations selected in the Real Time rules of the Data Loss Prevention (DLP) policy. When a Real Time DLP rule is configured with **Select Destination Lists and Applications for Inclusion**, Secure Access scans for data violations every web request matching the rule's applicable resources and targeting a destination matching the rule-configured destinations. A web request can be a web form or a file upload. File uploads can be scanned for matches with the selected data classifications in the file content, file name, or either. Moreover, a file upload can be scanned for the presence of document properties matching the rule's File Labels settings. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.

Verified applications also support other workflows besides file uploads. For example, if the rule is configured to **Select Destination Lists and Applications for Inclusion** and Yahoo Mail is chosen as an application to scan for content, the policy can scan for file uploads, emails sent, and draft emails saved. Violations within these workflows are then blocked or monitored, depending on the action selected in the rule. However, some applications have limitations when scanning for file names of file uploads. For example, the DLP policy can scan Dropbox for file uploads, but the file name can not be scanned.

The DLP Real Time rules support thousands of applications, divided into categories for ease of reference. Before January of 2024, DLP supported a more limited set of applications; the table below lists those applications and the limitations on their support. These applications appear in the GUI with the notation *(Vetted)*, as shown in the example below:



The list of apps marked *Vetted* in the GUI, and their workflow limitations, is listed below:

Application	Supported Workflows	File Name Limitations
Box Cloud Storage	File upload	
ChatGPT	Create conversation	
OpenAI ChatGPT API	Request and Response of Chat and Completions	
Concur Invoice	Receipt upload	
Confluence	File upload; edit a file **Note** To scan file uploads, you must select Atlassian and Confluence as destinations for the DLP rule.	
DLPTest.com	Submit test message; File upload	

Application	Supported Workflows	File Name Limitations
Dropbox	File upload; File upload add comment; File upload update comment. **Note** Dropbox Paper is not supported using Real Time DLP, but may be supported using SaaS API DLP.	File names of file uploads are not scanned. **Note** Depending on the mechanism used to upload large files, such as chunked uploads by platforms like Dropbox, the DLP engine may not be able to fully scan the document for policy violations.
Facebook Messenger	Upload a file to chat	
Gmail	Send email; attach a file; save a draft; send an email (classic); save a draft (classic)	
Jira	Create a ticket (epic/story/task/subtask/bug/customer issue/customer request) description; upload an attachment to a newly created ticket (Atlassian must also be selected); add a comment to a ticket; edit a comment in a ticket; edit description. **Note** To scan file uploads, you must select Atlassian and Jira as destinations for the DLP rule.	
LinkedIn SlideShare	File upload; publish content after a file upload; edit a published slide; edit privacy settings of a post; report content as inappropriate; upload thoughts and ideas on a slideshare; like a thought or slide; upload files from a Cloud app (Dropbox, GDrive, Box, Gmail, OneDrive); share content using linkedIn, Facebook, or Twitter	

Application	Supported Workflows	File Name Limitations
Monday	Create workspace; create board; add item-update with file upload; add an item-update reply with file upload; add a message to Text column; add text to Long Text column; add an update with a file upload to a sub-item; reply to a sub-item update with a file upload; add a local file to File column; add an email address or text to Email column; upload a file to a shared form; add text to the dashboard text widget;	
PasteBin	Post a message	
SalesForce	File upload; upload file via chatter; write a post in chatter; write a note;	
ServiceNow	Service management post incident; service automation post incident	
ShareFile	Create note; create request list; upload a file to a task; create a task; add task comment; send an invite to a new user; share a file; file upload; submit a form; remote upload a form; create a file drop; share a file via email; send an email	File names of files uploaded to ShareFile storage are not scanned.
Slack	File upload; post a message in a channel	
SmartSheet	File upload; upload attachment to a form; add comment to a form	
WeTransfer	File upload; upload a file to a message	File names of files uploaded to WeTransfer are not scanned.
WorkDay HCM	Add an address; edit an address; add text to a field; upload a file	
Yahoo Mail	Upload file; send an email; save a draft	

Add a Real Time Rule to the Data Loss Prevention Policy

Provides instructions for completing the Add a Real Time Rule to the Data Loss Prevention Policy workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

There is only one data loss prevention policy. Rules are added to the policy to define what traffic to monitor (resources and destinations), the data classifications that require monitoring, and whether content should be blocked or only monitored.

A Real Time rule must have at least one of the following four criteria defined:

- Data Classifications – Include files that match data classification of your own making or a built-in data classification provided by Secure Access.
- File Labels – Include files that have specific file label names configured in the value of the files' document properties, or include files that have no file labels configured. (You cannot select both of these criteria in a single rule.) Secure

Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

- File Size – Include files that meet custom size criteria.
- File Type – Include files that have a specific file type.

> **Note**
>
> DLP for private resources does not support scanning of CSV and TXT file types.

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- You must have a Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

1. Create the Real Time rule and establish general settings.
2. Select **Data Classifications** to apply to the rule.
3. Make **Files Control** selections for the rule.
4. Select **Identities** to apply to the rule.
5. Select **Destinations** to include for the rule.
6. Select **Destinations** to exclude from the rule.
7. Select an **Action** to be performed when data matches the rule.
8. If you have established a connection with an ICAP server, you can optionally disable payload transmission for DLP violations triggered by this rule.
9. For Endpoint DLP only, you can select to display pop-up notifications on the endpoint when a violation occurs.

> **Note**
>
> To use this feature you must have at least one real time rule defined with at least one endpoint channel selected under Destinations.

10. For any destination you can enable and configure an email notification to be sent to users when a violation occurs.

Create a DLP Real Time Rule Step 1 — Establish General Settings

Provides instructions for completing the Create a DLP Real Time Rule Step 1 – Establish General Settings workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

This is the first step in the process to add a real time rule to a DLP policy, in which you create the rule and establish its basic characteristics.

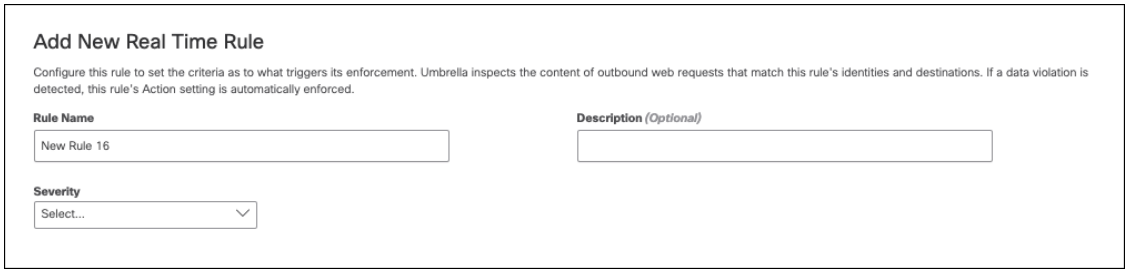
- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the next step in the process, see Create a DLP Real Time Rule Step 2 – Select Data Classifications

Before you begin

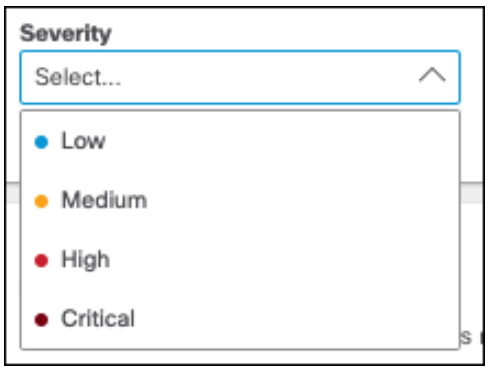
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, click **Add Rule**, and choose **Real Time Rule**.
2. Under **Add New Real Time Rule**, give your rule a meaningful name and description.



3. Choose a severity for your rule based on the risk involved or importance within the ruleset.



Create a DLP Real Time Rule Step 2 — Select Data Classifications

Provides instructions for completing the Create a DLP Real Time Rule Step 2 – Select Data Classifications workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

This is the second step in the process to add a real time rule to a DLP policy, in which you select the data classifications to apply to the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 1 – Establish General Settings
- For the next step in the process, see Create a DLP Real Time Rule Step 3 – Select Files Controls

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

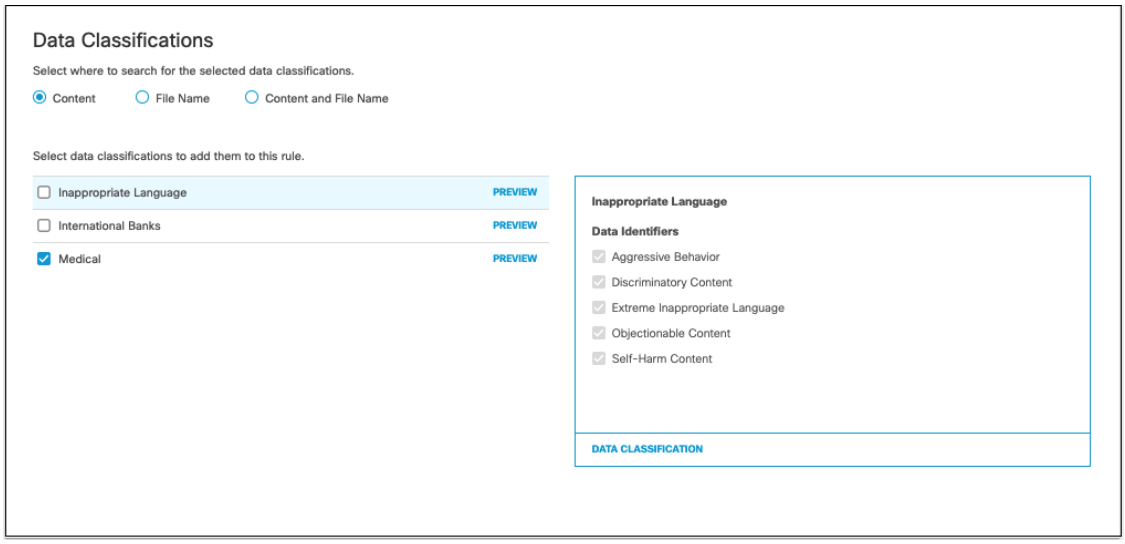
Procedure

1. In the **Data Classifications** area, choose where you would like this rule to search for data classifications.
   - **Content**–(Default) Searches only the content of files for the selected data classifications. Use this option when you want the rule to evaluate text extracted from images by OCR scanning.
   - **File Name**–Searches only file names for the selected data classifications.

- **Content and File Name**–Searches content and file names for the selected data classifications. Both content and file name do not need to match for the rule to apply, only one or the other. Use this option if you want the rule to match either OCR-extracted content or the file name.

> **Note**
>
> Choosing **Content**, **File Name**, or **Content and File Name** refers to scanning file uploads for the selected data classifications and configured file labels.

2. Select classifications to apply this rule. For more information, see Manage Data Classifications. For OCR-based detection, select the classifications that include the custom identifiers created for the required languages or terms.



Create a DLP Real Time Rule Step 3 — Select Files Controls

Configure file controls in a Real Time DLP rule using file labels, file size, and file type filters to enhance data protection.

This is the third step in the process to add a real time rule to a DLP policy, in which you select the files controls to apply to the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 2 – Select Data Classifications.
- For the next step in the process, see Create a DLP Real Time Rule Step 4 – Select Identities.

In the **Files Control** area, choose the file filters to apply to this rule. You can apply filters for:

- File Labels, or files that have no file labels associated with them. (You cannot select both of these criteria in a single rule.)
- File Size
- File Type

> **Note**
>
> Files encrypted with Digital Rights Management (DRM) or Microsoft Sensitivity Labels cannot be decrypted for deep content inspection or text extraction. Because content cannot be extracted from encrypted files, DLP content and pattern-matching rules cannot be evaluated against the file body. As a result, these files are allowed by default unless explicitly governed by supported metadata or transport-level policies.

Before you begin

- You must enable HTTPS Inspection on the default access policy, or at least one access policy rule configured with the same identity as in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

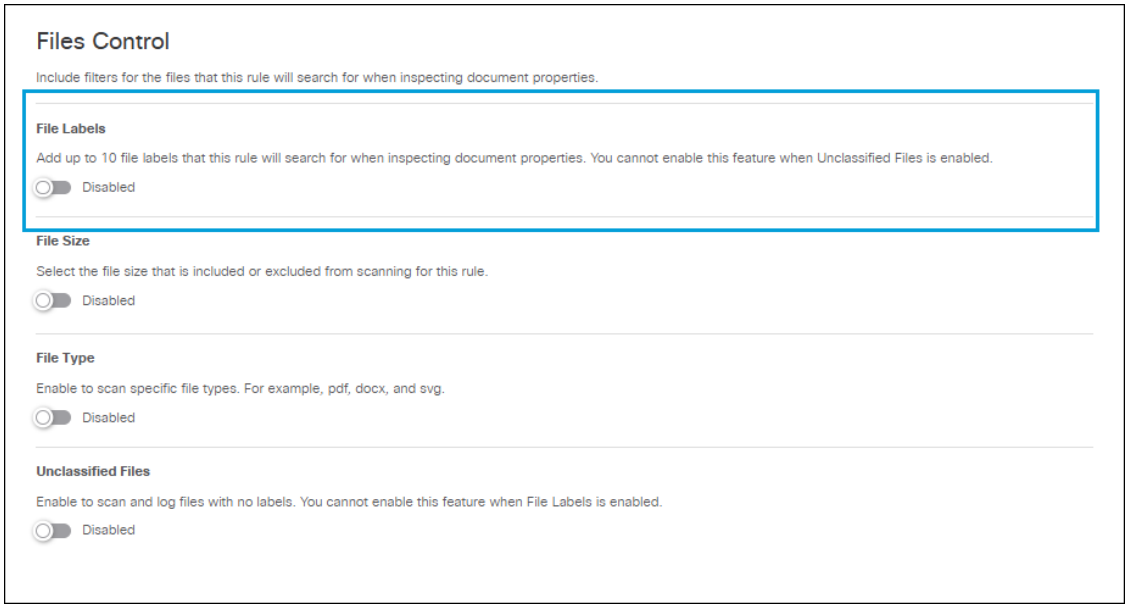
Procedure

1. Choose **File Labels**.

   Add up to 10 case-sensitive file label names to apply to this rule. The rule searches for configured file label names in the files' document properties. This includes Microsoft Office Sensitivity Labels and Adobe PDF Document Properties. For Microsoft Office Document Properties , this includes only the Label Value field in the custom document properties. File uploads to Confluence and Jira are not scanned for file labels.

   Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

> **Note**
>
> You can configure a DLP rule with data classifications, file labels, or both. When a DLP rule is configured with both, then a DLP event is raised when any of the selected data classifications and when any of the configured file labels are detected in the inspected file.



> **Note**
>
> Secure Access currently supports detection of Microsoft sensitivity labels in the file properties' values of the inspected file for Microsoft Word, Excel, PowerPoint, and PDF files. Ensure you configure the rule with the name of the sensitivity labels, not the Display Names.

> **Note**
>
> For documents protected with Microsoft Information Protection (MIP) sensitivity labels, Endpoint DLP policy enforcement is not applied to the Print channel. Policy enforcement for all other supported channels remains unaffected.

2. Choose **File Size** criteria for the rule.

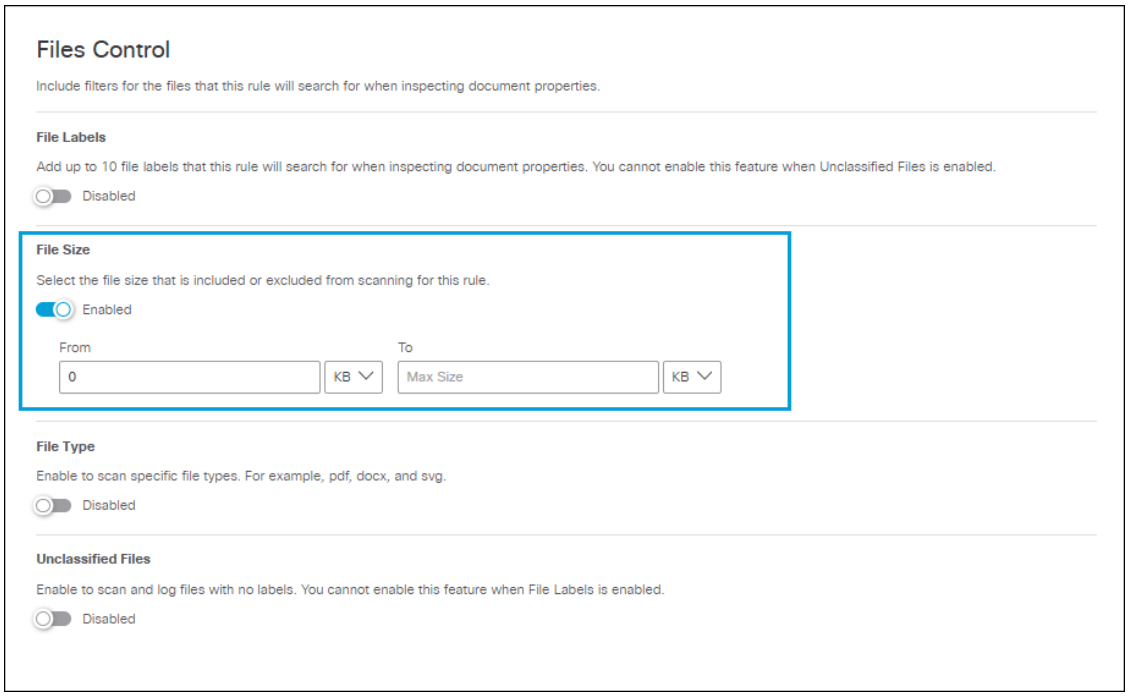
   The **File Size** area has two use cases:

   - In a rule with only custom file size criteria, DLP applies the rule action to files that match the file size criteria, regardless of content. (This may be useful in situations where you want to exclude certain low-risk files below a certain size from inspection, so as not to waste processing time on insignificant events.)
   - In a rule that specifies a custom file size along with other criteria such as Data Classification, the DLP applies the rule action to files that match the other criteria within the file size specified up to the first 50 MB of plain text. (Secure Access does not scan file content beyond the first 50 MB regardless of the file size specified here.)

In the **File Size** area choose from two options:

- To scan up to the first 50 MB of plain text of all files that meet other criteria defined by this rule, enable the **File Size** toggle and do not select custom sizes. (A rule that uses this option must also specify Data Classifications.)
- To specify the minimum and maximum size limits the system will scan for files that meet other inclusion criteria defined by this rule, if there are any, enable the **File Size** toggle and select custom size values. If the file size exceeds the first 50 MB of the file, Secure Access scans only up to the first 50 MB of plain text in the file. (I.e., if you specify a minimum file size greater than 50 MB, Secure Access will not scan for other criteria specified in the rule.)

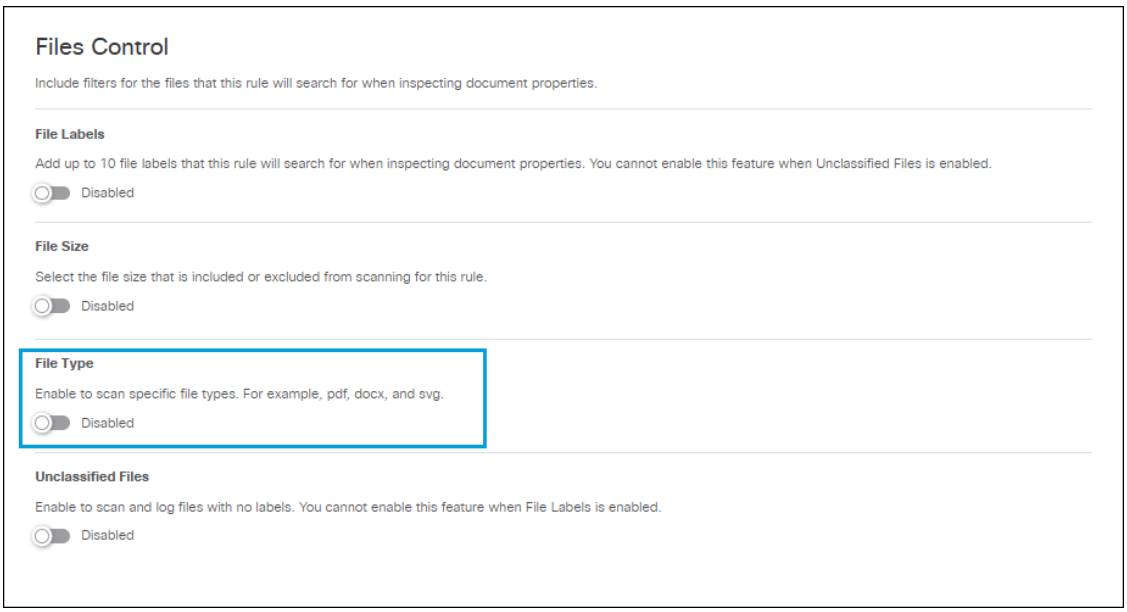
  You can choose to apply the rule action only to files that are greater than a minimum size you specify, or to files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB.



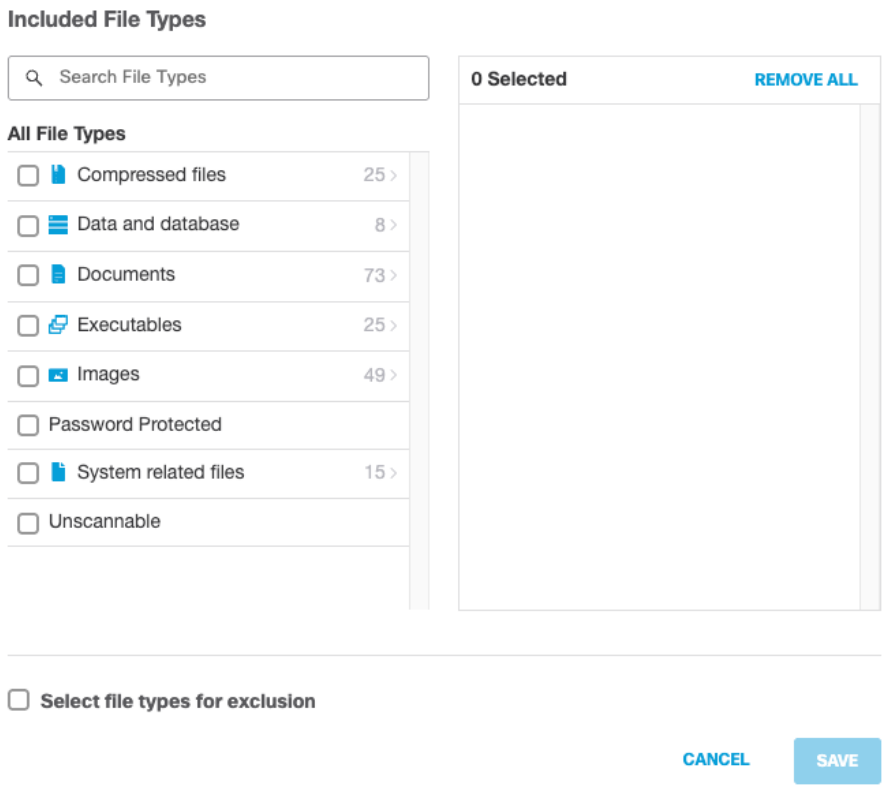
Note

For Endpoint Channels → Printer, custom file size–based exfiltration detection may not apply consistently.

3. In the **File Type** area, configure the rule to include specific file types or to exclude unrecognized file types.
   a) Click the toggle to enable file type filtering.



b) To include file types, use the search box to search for file types or browse within the lists for file types. Check the boxes for the file types to include individually or by group. Selected file types appear on the right.



You can now select the Executables file type group to identify and control files that may pose security risks.

- Detection Mechanisms: The system uses MIME type matching for reliably identifiable types and extension-based pre-checks for types with generic or overlapping MIME types.
- Limitations: Renaming file extensions may bypass extension-based checks for certain types.
- CGI Exclusion: .cgi files are explicitly excluded from this feature due to the high risk of false positives

When a DLP rule combines the **Executables** file type group with a Data Classification (e.g., PCI), both conditions must be satisfied for a block action to trigger.

- **Binary-based Executables (.exe, .jar, .apk, .swf, .elf):** These files are not extractable by the system. If a rule requires both an executable file type and a data classification, the rule will not trigger because the system cannot extract content from these files to match against the classification.
- **Script-based Executables (.sh, .pl):** These files are text-based and extractable. The rule will trigger and block the file if the specified classification content is present.

You can select the **Password Protected** category to detect and enforce policies on files that are password-protected.

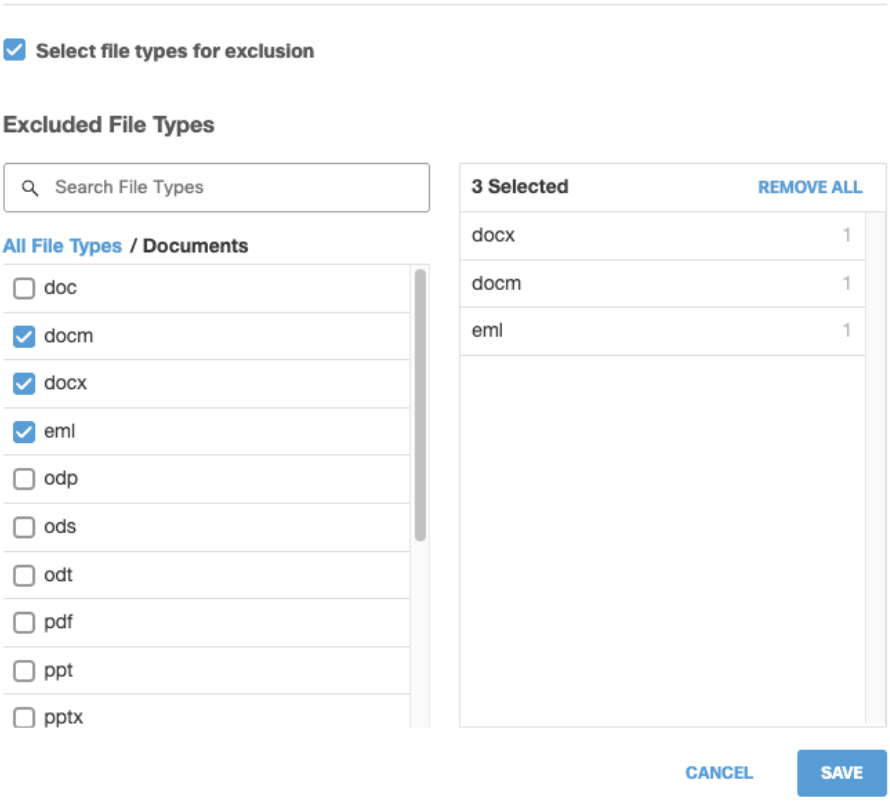
- **Policy Usage:** This category can be used in both inclusion and exclusion lists within your DLP policy rules.
- **Migration Note:** If you previously used the Unscannable category to detect password-protected files, you must update your existing DLP rules to use the new Password Protected category to ensure continued enforcement.

> **Note**
>
> Content classifiers cannot be combined with the **Password Protected** file type category. Because the contents of a password-protected file cannot be extracted or inspected, classification-based rules will not trigger for these files.

> **Note**
>
> Filename-based matching remains supported for password-protected files, as the filename is accessible without requiring file decryption.

c) To exclude file types, check **Select the file type for exclusion** check box.

In **Excluded File Types** section, use the search box to search for file types or browse within the lists for file types. Check the boxes for file types to exclude individually or by group. Selected file types appear on the right.

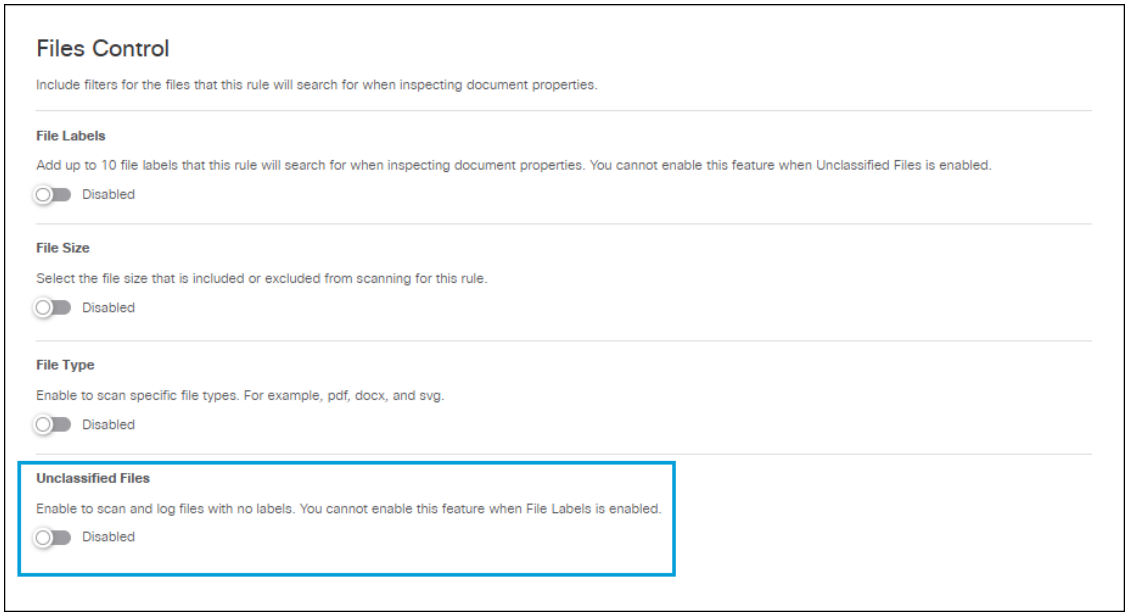


4. In the **Unclassified Files** area, click the toggle to include files that have no labels associated with them.

   This includes Microsoft Office Sensitivity Labels and Adobe PDF Document Properties. For Microsoft Office Document Properties (or Titus labels) , this includes only the Label Value field in the custom document properties.

   Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

> **Note**
>
> You can configure a Real Time rule with data classifications, absence of file labels, or both. When a rule is configured with both, then a DLP event is raised when any of the selected data classifications are detected in an inspected file that has no file labels.



Create a DLP Real Time Rule Step 4 — Select Identities

Provides instructions for completing the Create a DLP Real Time Rule Step 4 – Select Identities workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

This is the fourth step in the process to add a real time rule to a DLP policy, in which you select the identities to apply to the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 3 – Select Files Controls.
- For the next step in the process, see Create a DLP Real Time Rule Step 5 – Select Destinations for Inclusion.

Before you begin

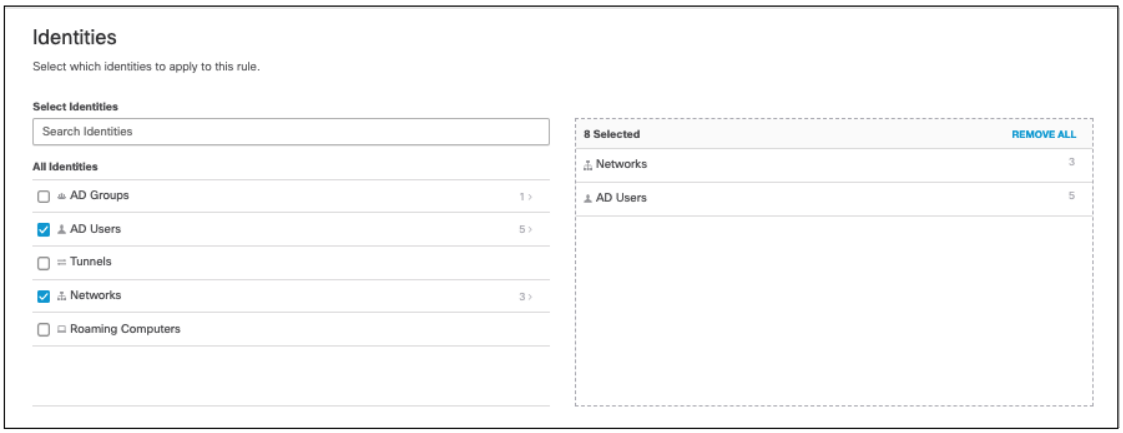
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.

- Enable global decryption.

- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

In the **Identities** area, select identities to apply to this rule.



Note

For Endpoint DLP, only **AD Users**, and **AD Groups** are applicable.

Create a DLP Real Time Rule Step 5 — Select Destinations for Inclusion

Learn how to select destinations for inclusion when creating a Data Loss Prevention (DLP) real-time rule. This procedure explains how to configure the applications, private resources, resource groups, destination lists, and endpoint channels that the rule monitors and protects.

This is the fifth step in the process to add a real time rule to a DLP policy, in which you select the identities to apply to the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 4 – Select Identities.
- For the next step in the process, see Create a DLP Real Time Rule Step 6 – Select Destinations for Exclusion.

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.

- Enable global decryption.

- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

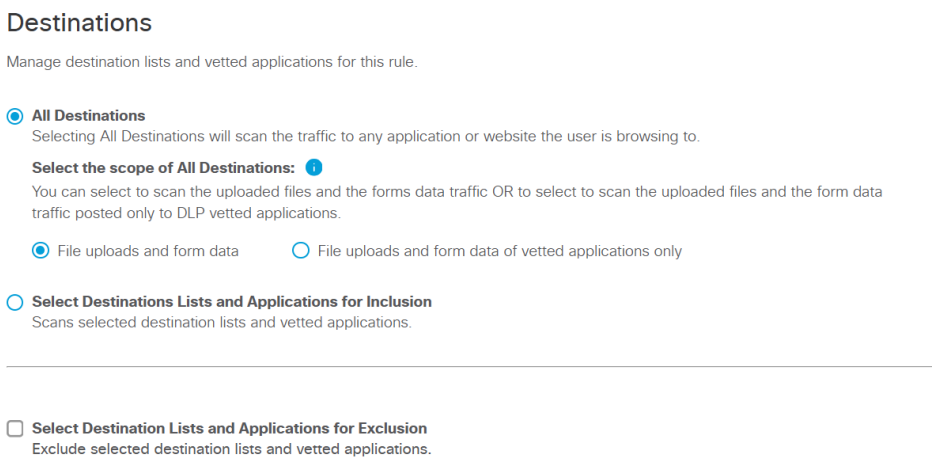
Under **Destinations**, select **All Destinations** or **Select Destination Lists and Applications for Inclusion**.

- **All Destinations**–Monitors all outbound web requests or blocks all file uploads that originate from the selected identities for this rule. When **All Destinations** is selected, you can select the type of data Secure Access monitors:
  - Choose **File uploads and form data** to monitor all uploaded files and forms data for all web destinations users visit.

    Warning

    Use care when choosing **All Destinations File uploads and form data** because it significantly widens the scope of the data the rule scans and can result in excessive false positives, blocking users' access to many sites inappropriately. We recommend that rules applied to all destinations not include built-in identifiers with lenient tolerances or custom identifiers with regexes that define a broad scope. Design regexes to narrowly identify the data you seek, and include threshold and proximity criteria.

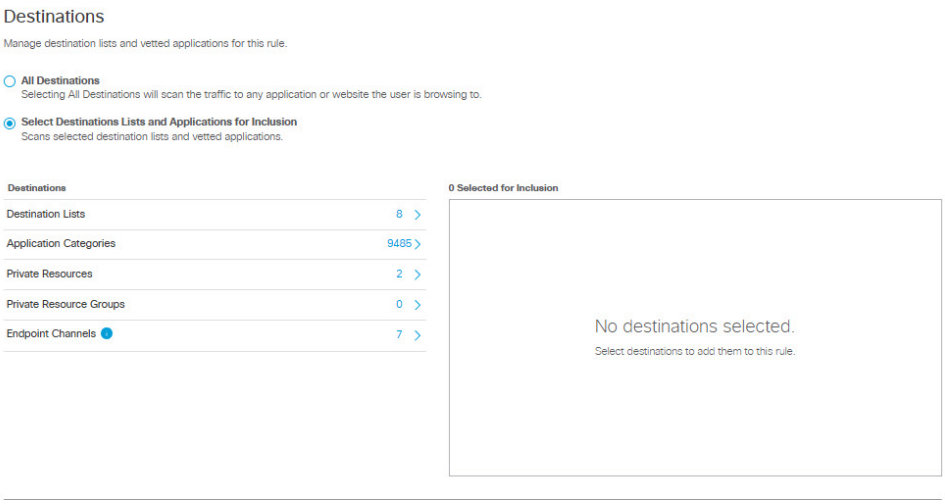
  - Choose **File uploads and form data of vetted applications only** to monitor all uploaded files and forms data associated only with DLP Supported Applications.



Note

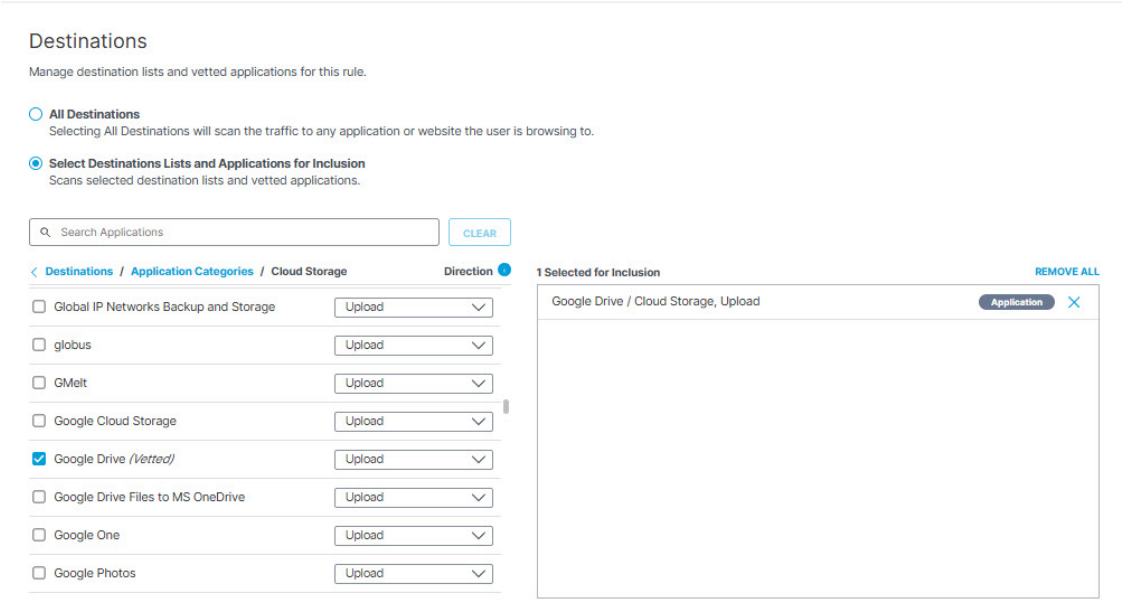
Selecting **All Destinations** option does not automatically include endpoint channels.

- **Select Destination Lists and Applications for Inclusion**–Monitors all web requests and blocks all file uploads matching the identities selected on the rule, the selected destination lists, and supported applications.



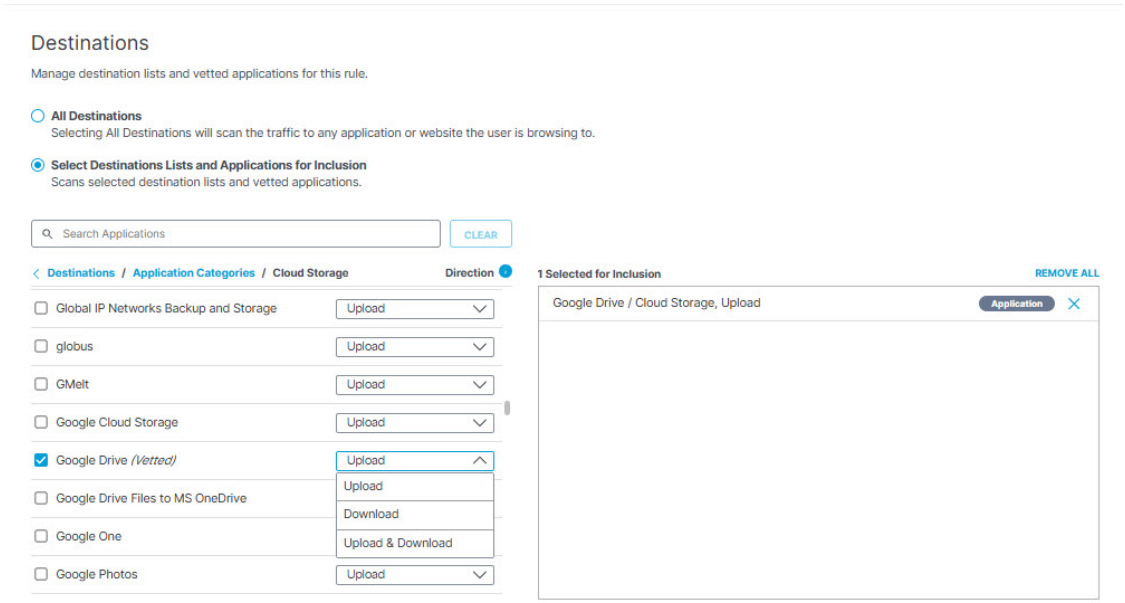
- To add applications for inclusion, under **Destinations** expand **Application Categories**. (See Application Categories) for a list of available categories. Expand categories and check the checkboxes for the applications you want to add to the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.



You can scan one of three traffic direction options for application and categories: **Upload** (from your system to the application), **Download** (from the application to your system), or **Upload and Download**. When you select a traffic direction for an application category, that selection applies to all applications within that category.

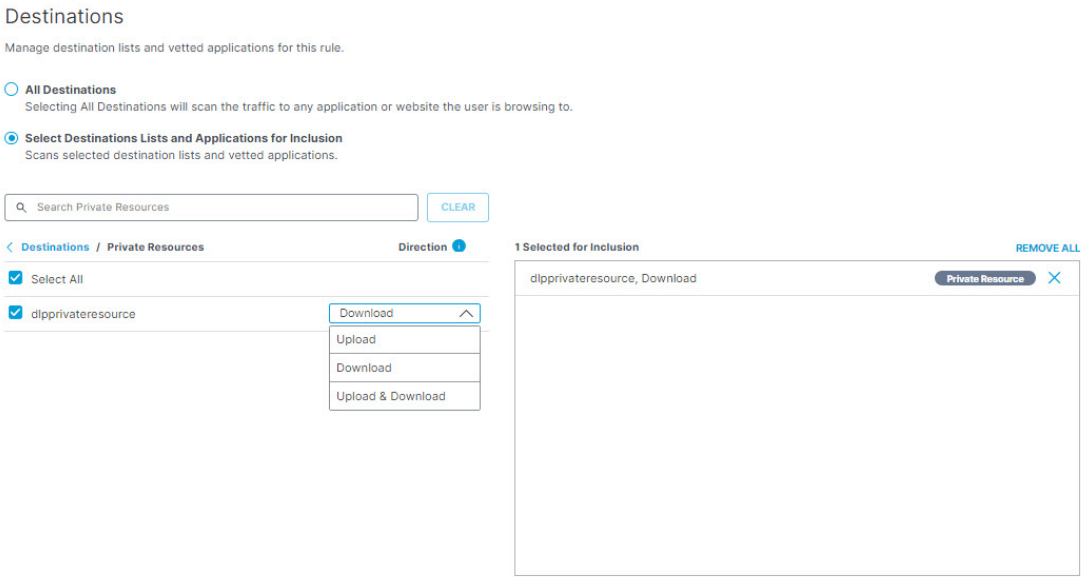
> **Note**
>
> Not all applications support scanning of all three traffic direction options. The system does not display a traffic direction option for an application unless that option is supported.



- To add private resources for inclusion, under **Private Resources** select the resource you want to scan. You can also select the direction of traffic associated with the resources that you want scanned: **Upload**, **Download**, or **Upload & Download**. You can search for a resource by entering at least three consecutive letters from the resource name in the search box.

> **Note**
>
> If you create a real time rule to protect any destinations that are private resources you must first:
>
> - Define the private resource.
> - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
> - Enable global decryption.

> **Note**
>
> It is not possible to search for a private resource with fewer than three letters in its name–for example, "QQ" or "YY." These resources must be manually selected, or wildcarded in search–for example, "QQ*". This behavior is by design.



Secure Access DLP supports scanning private resources in HTTP/s and non-HTTP/s traffic (such as SMB and FTP) traffic in both upload and download directions for all supported file types, but does not support scanning forms data.

- To add private resource groups for inclusion, under **Private Resource Groups** select the resource group you want to scan. You can also select the direction of traffic associated with the resource groups that you want scanned: **Upload**, **Download**, or **Upload & Download**. You can search for a resource group by entering at least three consecutive letters from the resource group name in the search box.

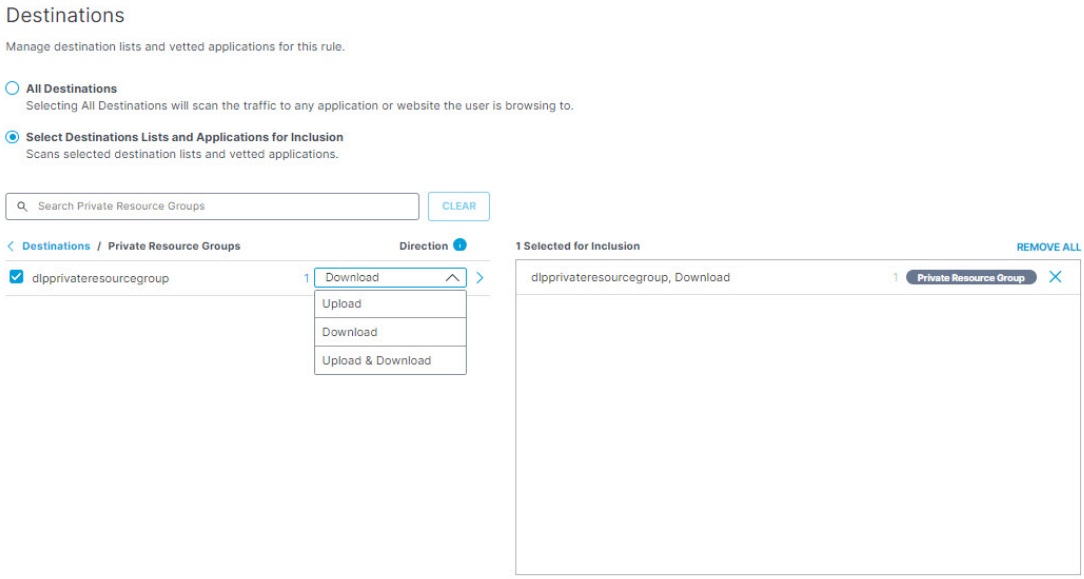
Note

If you create a real time rule to protect any destinations that are private resources you must first:

- Define the private resource.
- Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
- Enable global decryption.

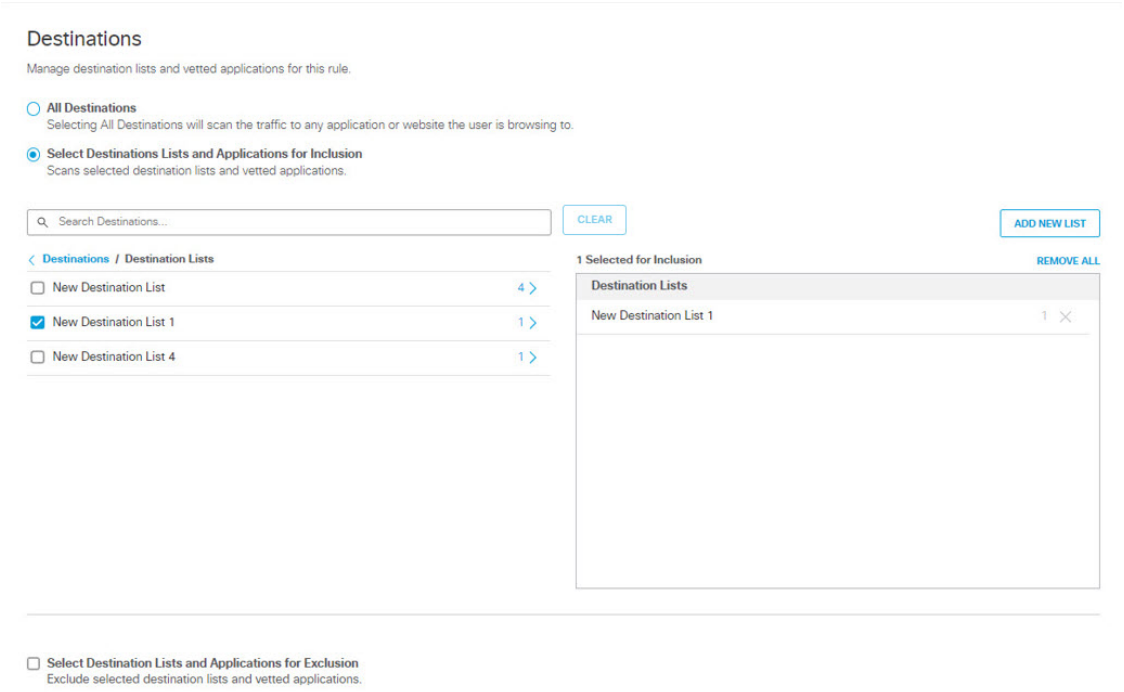
Note

It is not possible to search for a private resource group with fewer than three letters in its name–for example, "QQ" or "YY." These resource groups must be manually selected, or wildcarded in search–for example, "QQ*". This behavior is by design.



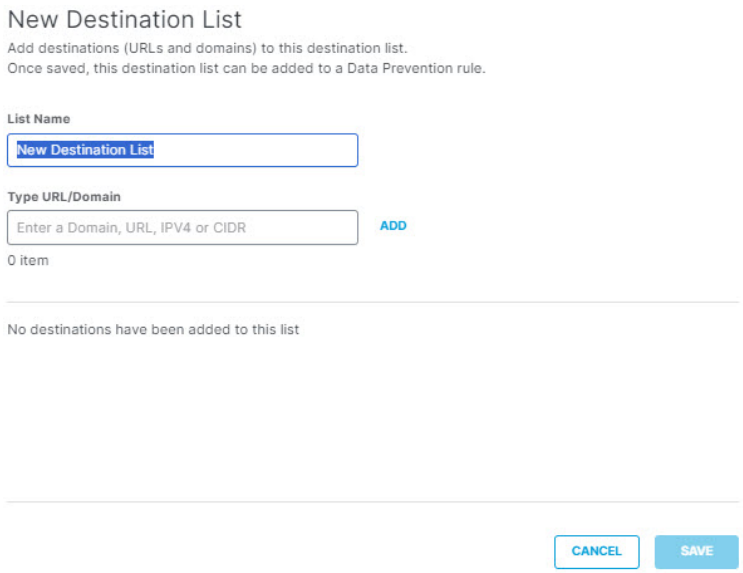
Secure Access DLP supports scanning private resources in HTTP/s and non-HTTP/s (such as SMB and FTP) traffic in both upload and download directions for all supported file types, but does not support scanning forms data.

- To add destination lists for inclusion, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to add to the rule.

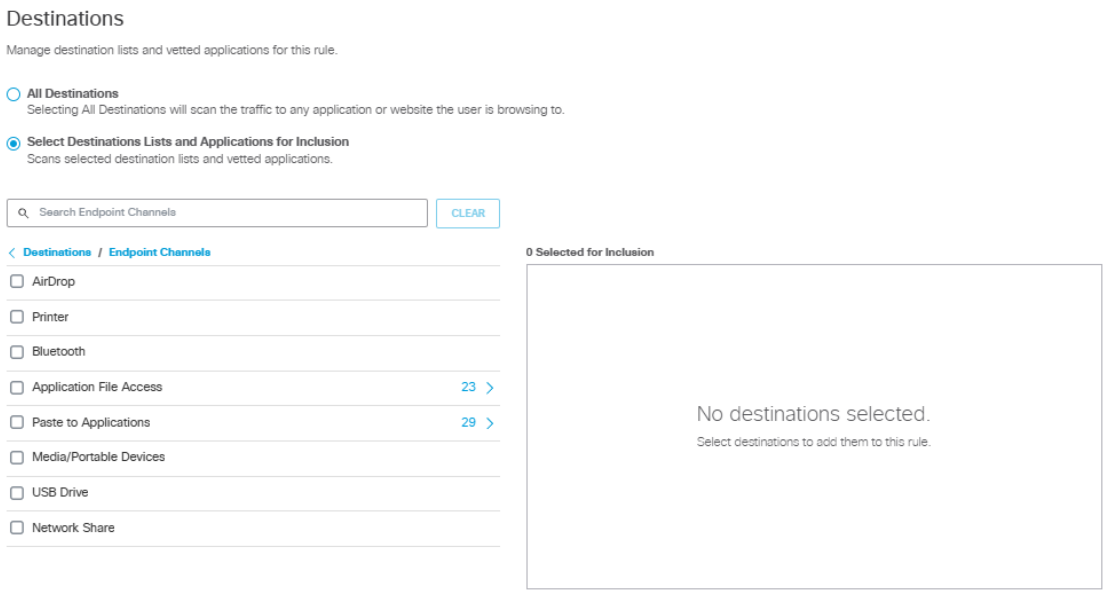


- To create a new destination list and add it for inclusion, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** when done.

> **Note**
>
> Adding a new destination list to the rule here automatically adds it for inclusion.



- To add endpoint channels for inclusion, under **Destinations**, expand **Endpoint Channels**, and check the boxes for the endpoint channels you want to add to the rule. You can search for an endpoint channel by entering at least three consecutive letters from the endpoint channel in the search box.



Warning

When you configure **Paste to Applications** in a rule, the target application may become unresponsive during paste operations. For endpoint versions earlier than 1.4.0.253, if the rule blocks paste actions with an override and requires a business justification, the application remains unresponsive until you provide the justification.

Note

If clipboard content matches one or more DLP rules and the operation is blocked, the destination application may display an error message.

Within the **Paste to Applications** and **Application File Access** channel, select applications using the following methods:

- **Individual Selection:** Manually select one or more applications from the list.
- **Category Selection**: Select a specific category to automatically include all applications within that category.
- **Entire Channel Selection**: Select the entire channel to automatically include all applications across all categories.

> **Note**
>
> DLP based on file names is not supported for all applications in the **Application File Access** channel. Additionally, some applications use custom file dialogs that the system does not monitor. Interacting with these dialogs may cause performance degradation or generate unintended DLP notifications when you preview sensitive files.

> **Note**
>
> Within the **Paste to Application**, **ChatGPT (Desktop)** is available under **AI Apps** and **MS Teams** is available under **Collaboration**; both require Endpoint DLP for Windows version 1.8.0.376 or later.

> **Note**
>
> The Endpoint DLP module for Windows monitors the following applications for print activity (corresponding to Endpoint Channels → Printer): Adobe Acrobat, Chrome, MS Excel, Edge, MS Outlook, Paint, Notepad, Notepad++, MS OneNote, MS PowerPoint, Real PDF Viewer, and MS Word. These restrictions do not apply to Endpoint DLP for Mac.

Create a DLP Real Time Rule Step 6 — Select Destinations for Exclusion

Provides instructions for completing the Create a DLP Real Time Rule Step 6 – Select Destinations for Exclusion workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

This is the sixth step in the process to add a real time rule to a DLP policy, in which you select the identities to exclude from the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 5 – Select Destinations for Inclusion.
- For the next step in the process, see Create a DLP Real Time Rule Step 7 – Select the Rule Action.

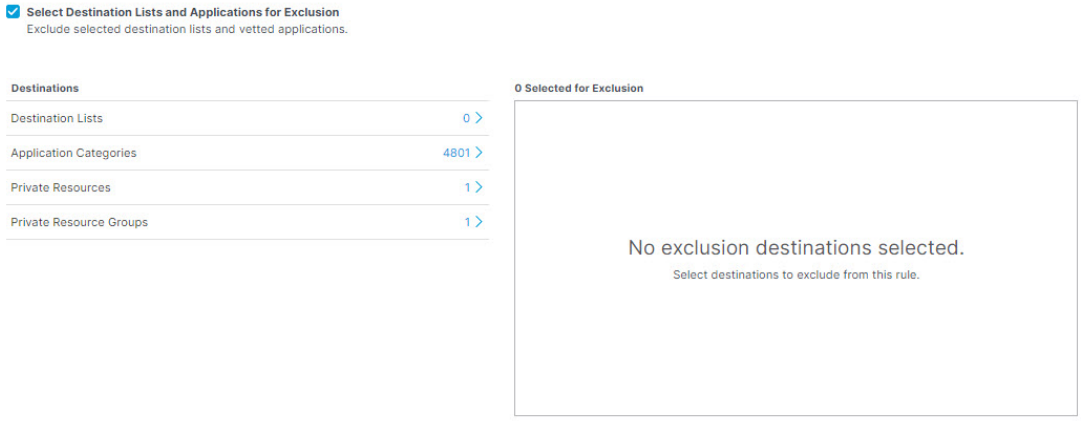
Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.

- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

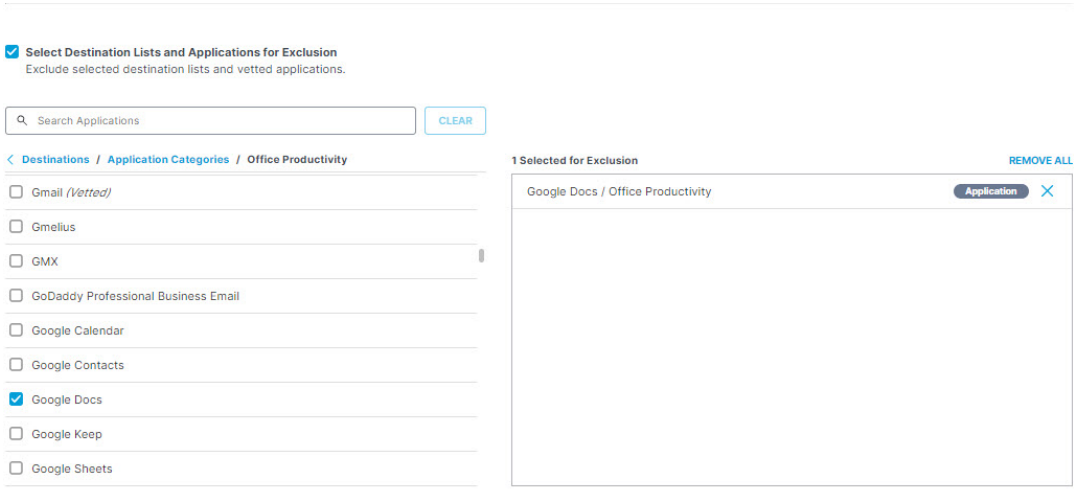
Procedure

Under **Destinations**, check the checkbox **Select Destination Lists and Applications for Exclusion** to select destinations and applications to exclude from this rule.



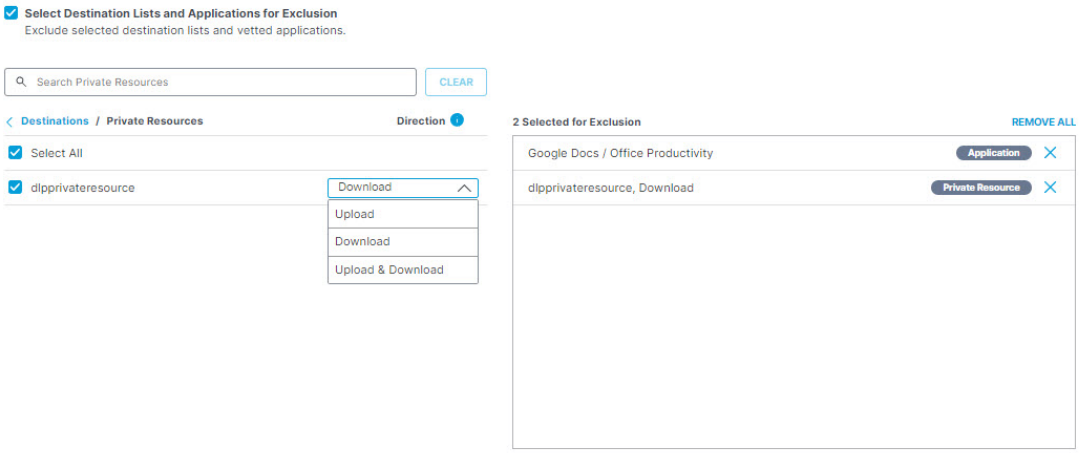
- To exclude applications, under **Destinations** expand **Application Categories**. (See Application Categories) for a list of available categories.) Expand categories and check the boxes for the applications you want to exclude from the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.



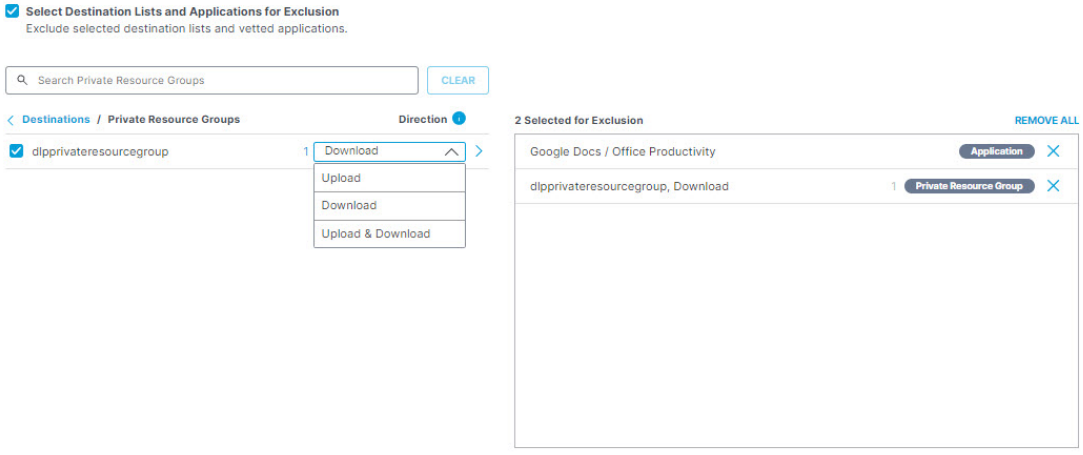
- To exclude private resources, under **Private Resources** select the resource you want to exclude from the rule. You can search for a resource by entering at least three consecutive letters from the resource name in the search box.

> **Note**
>
> It is not possible to search for a private resource with fewer than three letters in its name–for example, "QQ" or "YY." These resources must be manually selected, or wildcarded in search–for example, "QQ*". This behavior is by design.

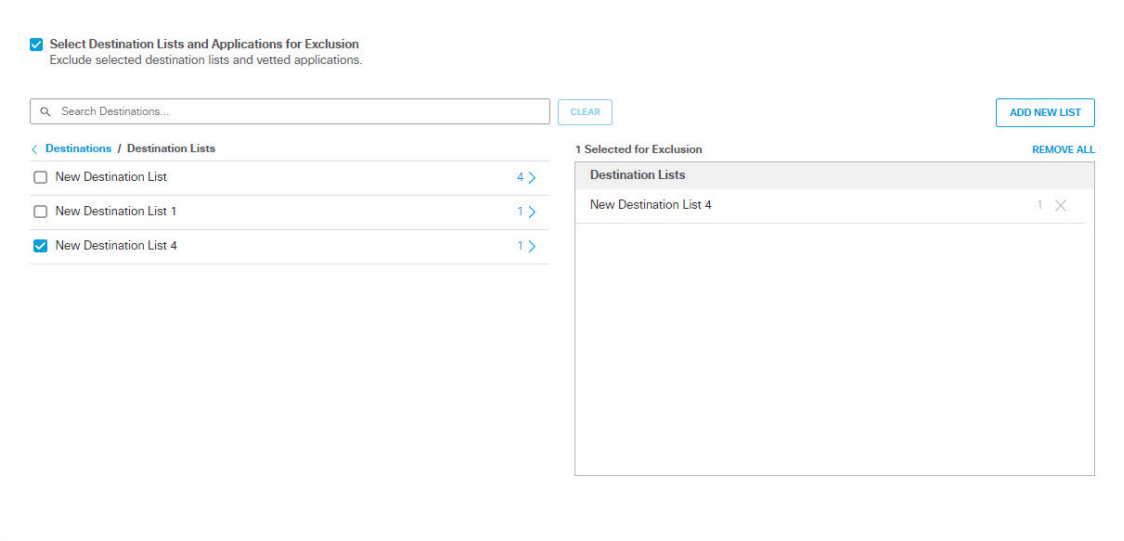


- To exclude private resource groups, under **Private Resource Groups** select the resource group you want to exclude from the rule. You can search for a resource group by entering at least three consecutive letters from the resource group name in the search box.

> **Note**
>
> It is not possible to search for a private resource group with fewer than three letters in its name–for example, "QQ" or "YY." These resource groups must be manually selected, or wildcarded in search–for example, "QQ*". This behavior is by design.



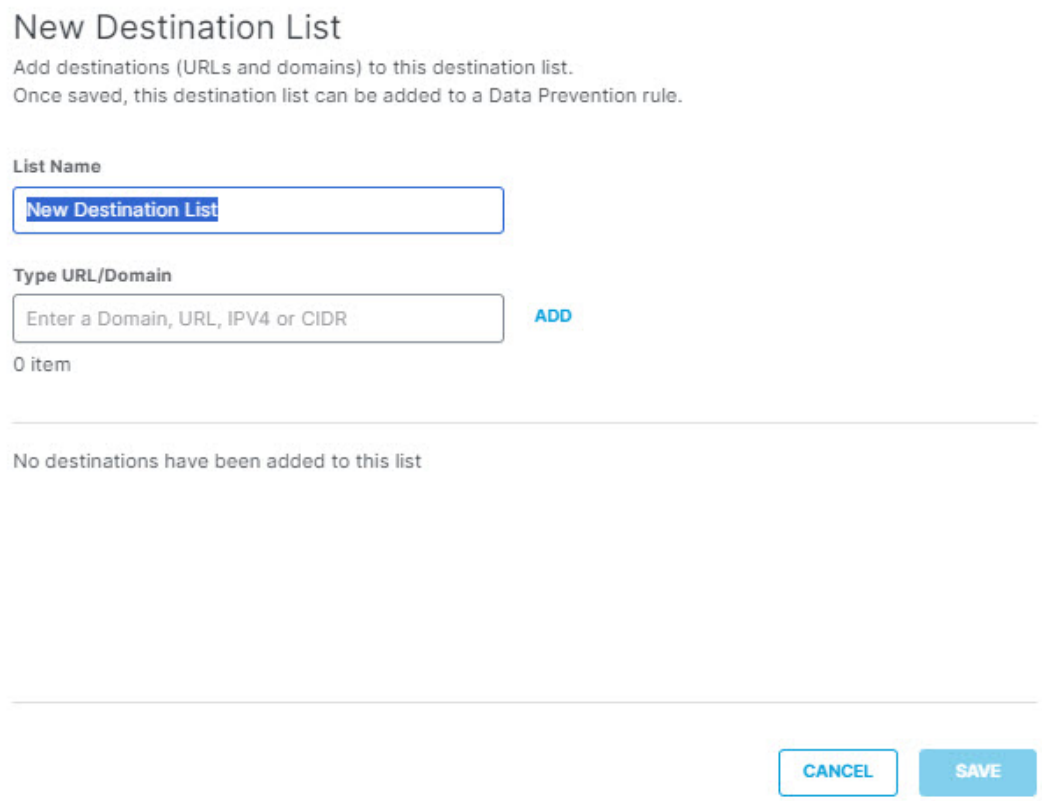
- To exclude destination lists, under **Destinations** expand **Destination Lists** and check the boxes for the destination lists you want to exclude from the rule.



- To create a new destination list and exclude it, under **Destinations** expand **Destination Lists** and click **ADD NEW LIST.** Under **List Name** enter a unique name for the list. For each URL/Domain to be in the list, enter a domain name, URL, IPV4 address or CIDR, and click **Add**. Click **Save** when done.

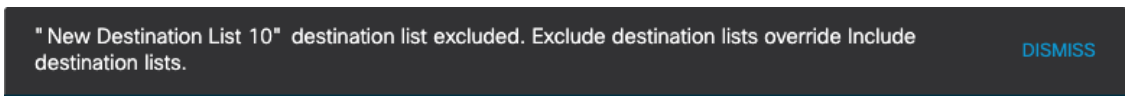
Note

Adding a new destination list to the rule here automatically adds it for exclusion.



Note

When a destination list is selected for both inclusion and exclusion in a rule, it will automatically be excluded. Exclusion destination lists always override inclusion destination lists. Similarly, if a domain is included on an inclusion destination list and an exclusion destination list, the domain will be excluded.



Create a DLP Real Time Rule Step 7 — Select the Rule Action

Provides instructions for completing the Create a DLP Real Time Rule Step 7 – Select the Rule Action workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule.

This is the seventh step in the process to add a real time rule to a DLP policy, in which you select an **Action** to be performed when data matches the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 6 – Select Destinations for Exclusion.
- For the next step in the process, see Create a DLP Real Time Rule Step 8 – Disable/Enable Payload Transmission for DLP Violations (ICAP Only).

Before you begin

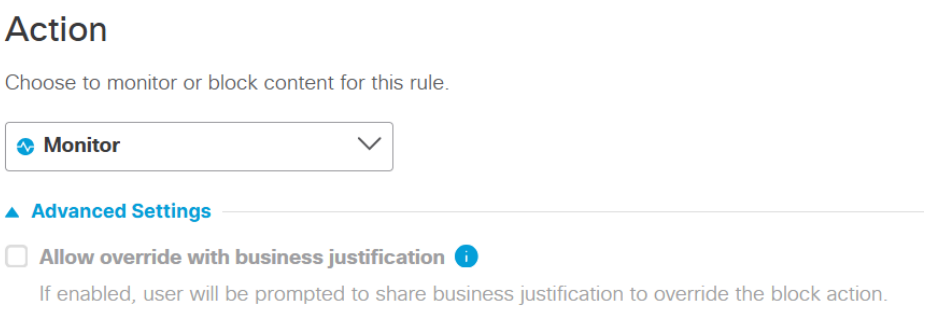
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

1. Under **Action**, from the drop-down list, choose **Monitor** or **Block**.
   - **Monitor**–Monitor file uploads and data submitted in web forms.

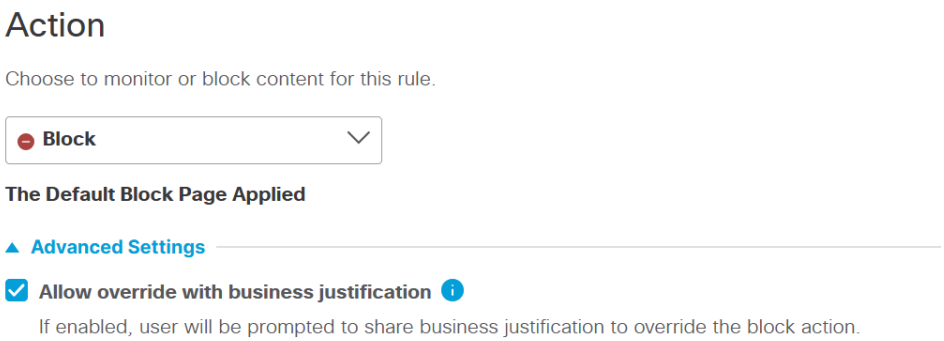
     The rule will search for content that matches supported workflows (See Supported Applications) and policy-configured destinations and identities.
   - **Block**–Block file uploads and data submitted in web forms.

     The rule will search for content that matches supported workflows (See Supported Applications) and the policy-configured destinations and identities. When content matches these workflows, the rule blocks the content.



2. For Endpoint DLP, you may optionally select the **Allow override with business justification** checkbox to allow data transfer with sensitive content.

   If you do not select any endpoint channels in **Destinations**, the **Allow override with business justification** option remains disabled.



3. You can optionally choose to block all password-protected files directed to destinations configured in the DLP rules.

   If enabled, this feature impacts all file types and all users and cannot be configured for finer granularity. This feature is released under controlled availability. If you wish to enable this feature, contact Secure Access Support for assistance.

Create a DLP Real Time Rule Step 8 — Disable/Enable Payload Transmission for DLP Violations (ICAP Only)

Provides instructions for completing the Create a DLP Real Time Rule Step 8 – Disable/Enable Payload Transmission for DLP Violations (ICAP Only) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the eighth step in the process to add a real time rule to a DLP policy, in which you may optionally disable transmission of Realtime DLP rule violations to an on-premesis DLP.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 7 – Select the Rule Action.
- For the next step in the process, see Create a DLP Real Time Rule Step 9 – Display Pop-Up Notifications for Endpoints.

If you have established a connection with an ICAP server, by default the payload of all active Realtime DLP rule violations will be sent to an on-premises DLP over ICAP. Disabling **Secure ICAP** for this rule will prevent payload transmission for DLP violations triggered by this rule.

> **Note**
>
> This feature is released under controlled availability. If you wish to enable this feature, contact Secure Access Support for assistance.

Before you begin

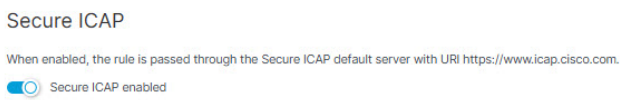
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.

- Enable global decryption.

- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

In the **Secure ICAP** area, click the toggle to enable or disable transmission of Realtime DLP rule violations to an on-premesis DLP.



Create a DLP Real Time Rule Step 9 — Enable and Configure Pop-Up Notifications for Violations

Provides instructions for completing the Create a DLP Real Time Rule Step 9 – Enable and Configure Pop-Up Notifications for Violations workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the ninth step in the process to add a real time rule to a DLP policy, in which you may optionally select to display a pop-up notification for endpoints when data matches the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 8 – Disable/Enable Payload Transmission for DLP Violations (ICAP Only).
- For the next step in the process, see Create a DLP Real Time Rule Step 10 – Enable and Configure Email Notifications for Violations.

Before you begin

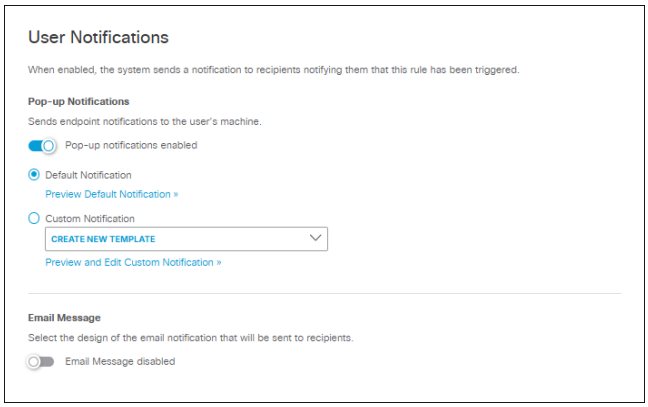
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.
- To enable pop-up notifications for any Real Time rule, you must have at least one Real Time rule defined that applies to an endpoint channel destination.
- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

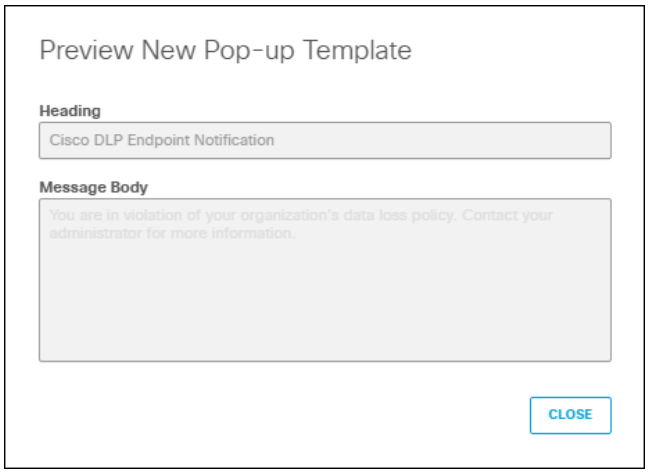
1. Under **User Notifications**, you can enable the **Pop up Notifications** option to display pop-up notifications of violations to the end user.

> **Note**
>
> If you have no real time rules with at least one endpoint channel selected under Destinations, the **Pop up Notification** option remains disabled.

> **Note**
>
> If you choose **Allow override with business justification** under **Action** **Advanced Settings**, the **Pop up Notification** option is automatically enabled and cannot be disabled.



2. Define the message to appear in the pop up dialog when files match a rule.
   - **To use the default Pop Up Template:**
     a. Click **Default Notification**.
     b. To preview the content of the pop up text, click on **Preview Default Notification**. You can review the text, but you cannot change it.



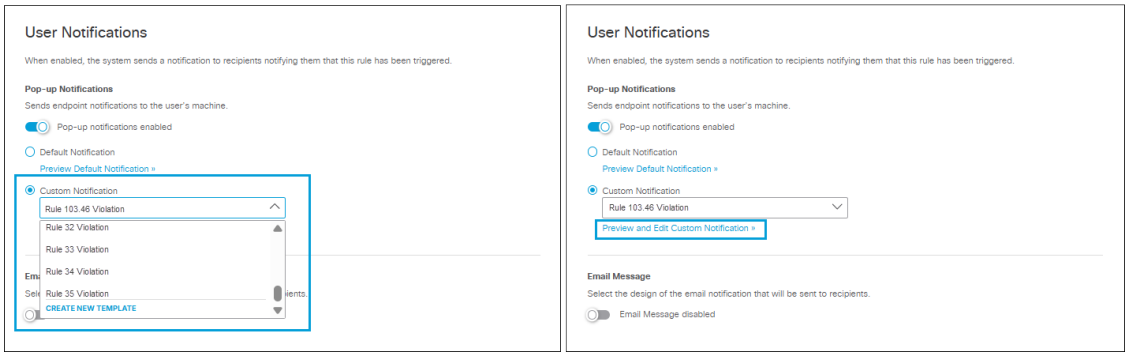
     c. Click **CLOSE** to close the preview.

- **To use a Custom Pop Up Template:**

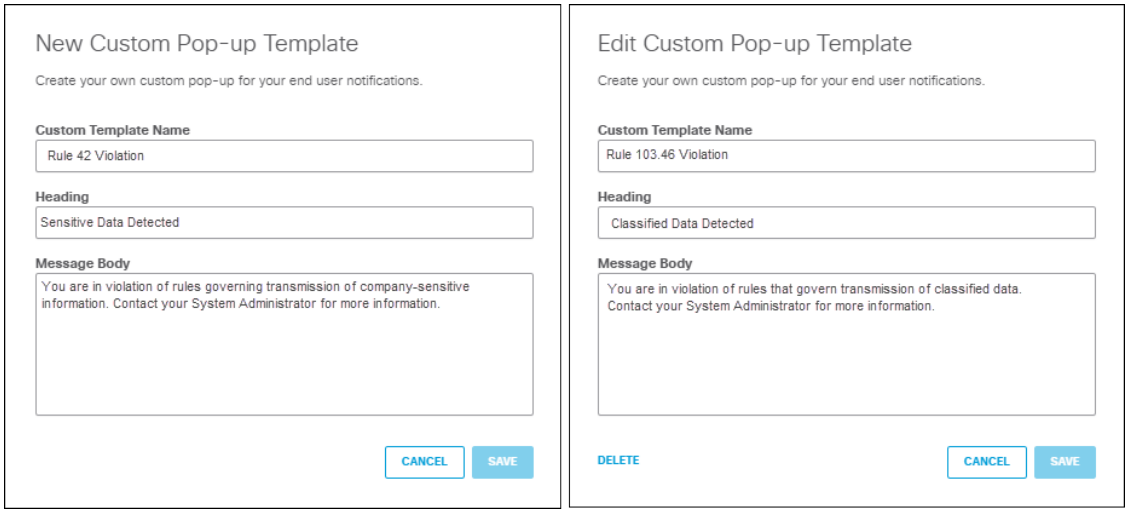
  a. Click **Custom Notification**.

  > **Note**
  >
  > On macOS, **Custom Notification** content is not available for Endpoint Destinations.

  b. From the drop-down list, select an existing custom template, or choose **CREATE NEW TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Notification** to review and change the template.



  c. When you choose to create or edit a custom template for pop up text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Pop-up Template** dialog includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the heading text for the pop up in the **Heading** text box.
3. Enter the message text for the pop up in the **Message Body** text box.

4. Click **SAVE** to complete the changes.

Create a DLP Real Time Rule Step 10 — Enable and Configure Email Notifications for Violations

Provides instructions for completing the Create a DLP Real Time Rule Step 10 – Enable and Configure Email Notifications for Violations workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the tenth and final step in the process to add a real time rule to a DLP policy, in which you may optionally select to configure and enable email notifications to send users when data matches the rule.

- For an overview of the entire process, see Add a Real Time Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Real Time Rule Step 9 – Display Pop-Up Notifications for Endpoints.

Under **User Notifications** for any destination you can enable and configure an email notification to be sent to any of the following users:

- The manager of the user who triggered the violation.
- Any email address(es) of your choice.

You can use a default email template provided by the system, or create your own custom template.

> **Note**
>
> The system gets the "send to" address for the email from UPN field in the authenticated active directory. Some identity configurations may not be able to provide the end user's email address, in which case the system will be unable to send the email. These cases include:
>
> - The user uses network or tunnel identities, in which case the user's IP address will be available to the system, but not the email address.
> - The user did not authenticate through active directory, so the system has no information about the user.
> - The user's email address is not stored in the UPN field in the authenticated active directory.

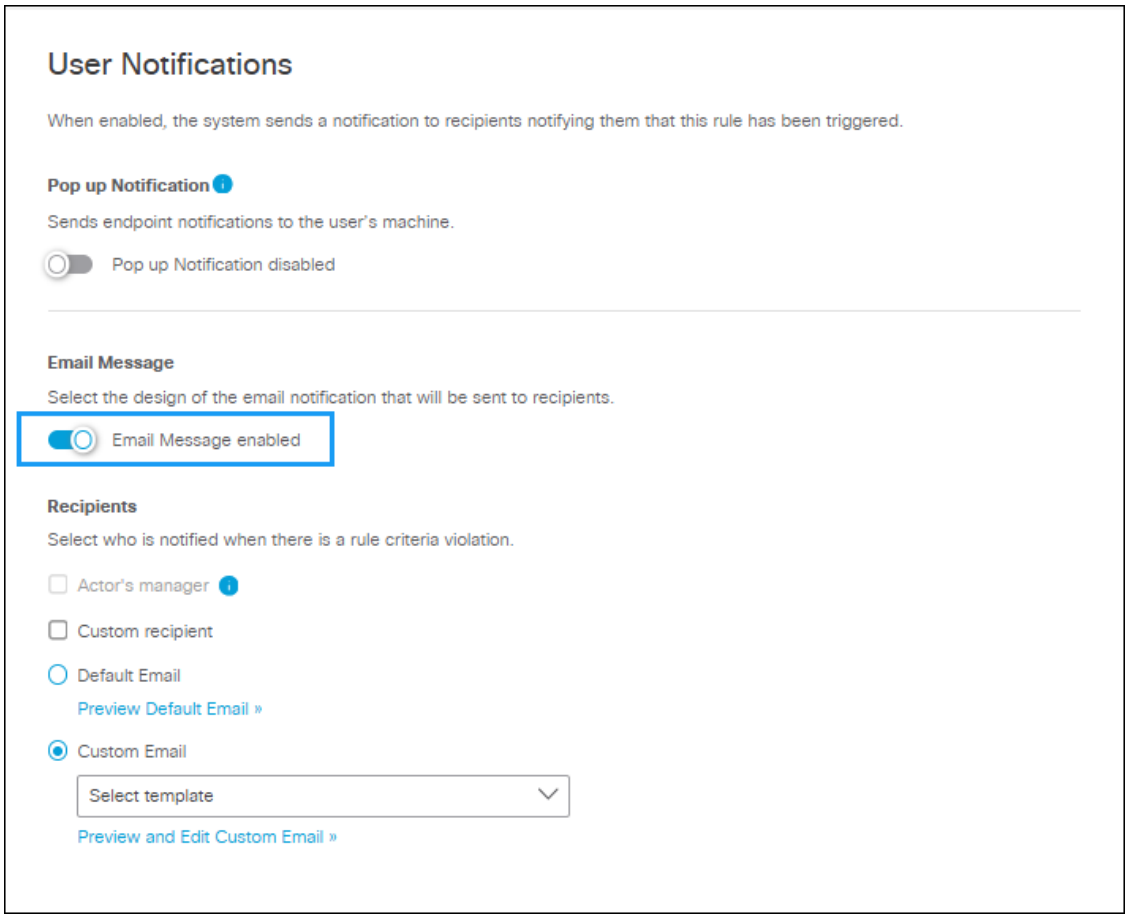
Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in a DLP rule. For example, if the resource "Network A" is configured for a DLP rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.
- If you create a real time rule to protect any destinations that are private resources you must first:
  - Define the private resource.
  - Define the certificate the Data Loss Prevention policy needs to decrypt the traffic going to that destination. See Add a Private Resource for details.
  - Enable global decryption.

- You must have the Secure Access full Admin user role. For more information, see Manage Accounts.

Procedure

1. Enable user notifications.



2. Select one or more of the following email recipients:

   - **Actor's manager**–The manager of the user who triggered the violation.

     This feature is available only when email addresses for reporting managers in Active Directory are synchronized for DLP notifications. As a result, the **Actor's manager** checkbox appearance varies depending upon the current configuration settings when viewing a rule:

Checkbox Appearance	Meaning
☐ Actor's manager	Reporting manager's email sync is enabled, but notifications to the actor's manager are not selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.
☑ Actor's manager	Reporting manager's email sync is enabled, and notifications to the actor's manager are selected for this rule. Email notifications for violations will be sent to the event actor's manager.

Checkbox Appearance	Meaning
Actor's manager	Reporting manager's email sync is disabled, and notifications to the actor's manager are not selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.
Actor's manager	Reporting manager's email sync is disabled, and notifications to the actor's manager are selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.

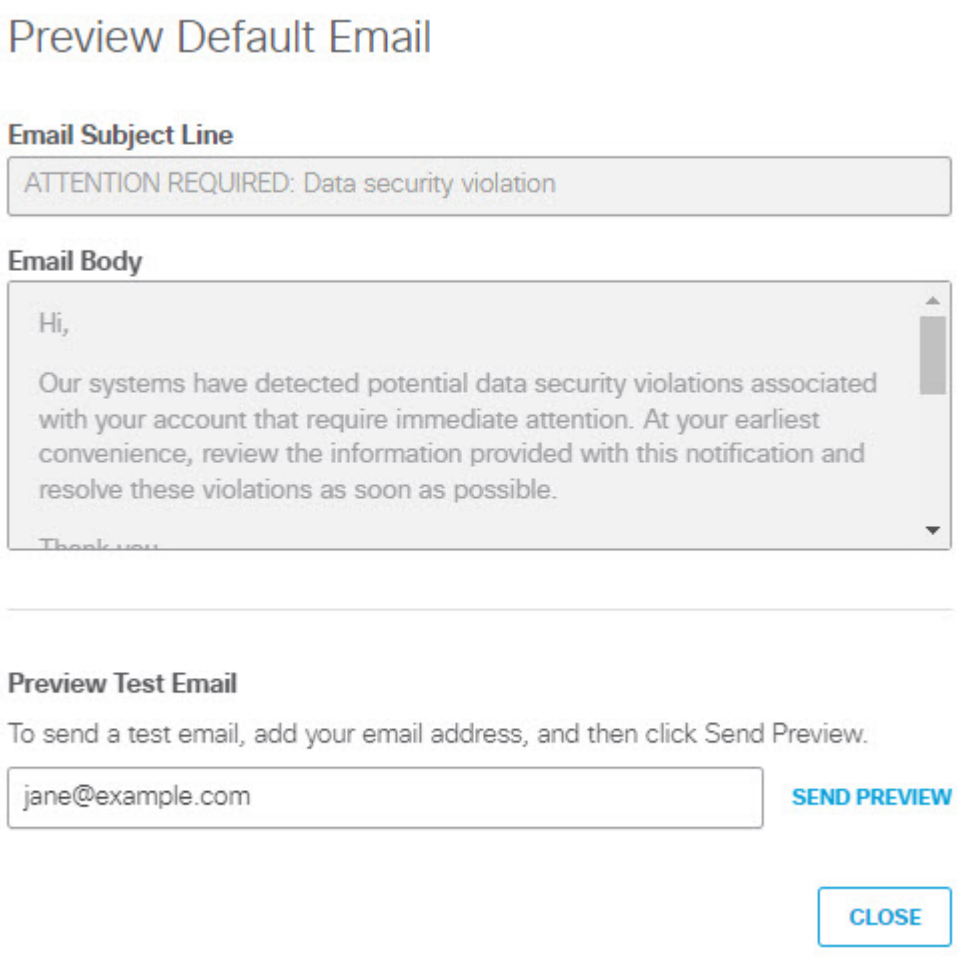
- **Custom recipient**–Allows you to specify email addresses of your choice. To use this option, select the **Custom recipient** checkbox, and enter one or more valid email addresses in the text box. These addresses will receive notifications whenever this rule is violated.

3. Choose the email template:

   To Use the Default Email Template:

   a. Click **Default Email**.

   b. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.



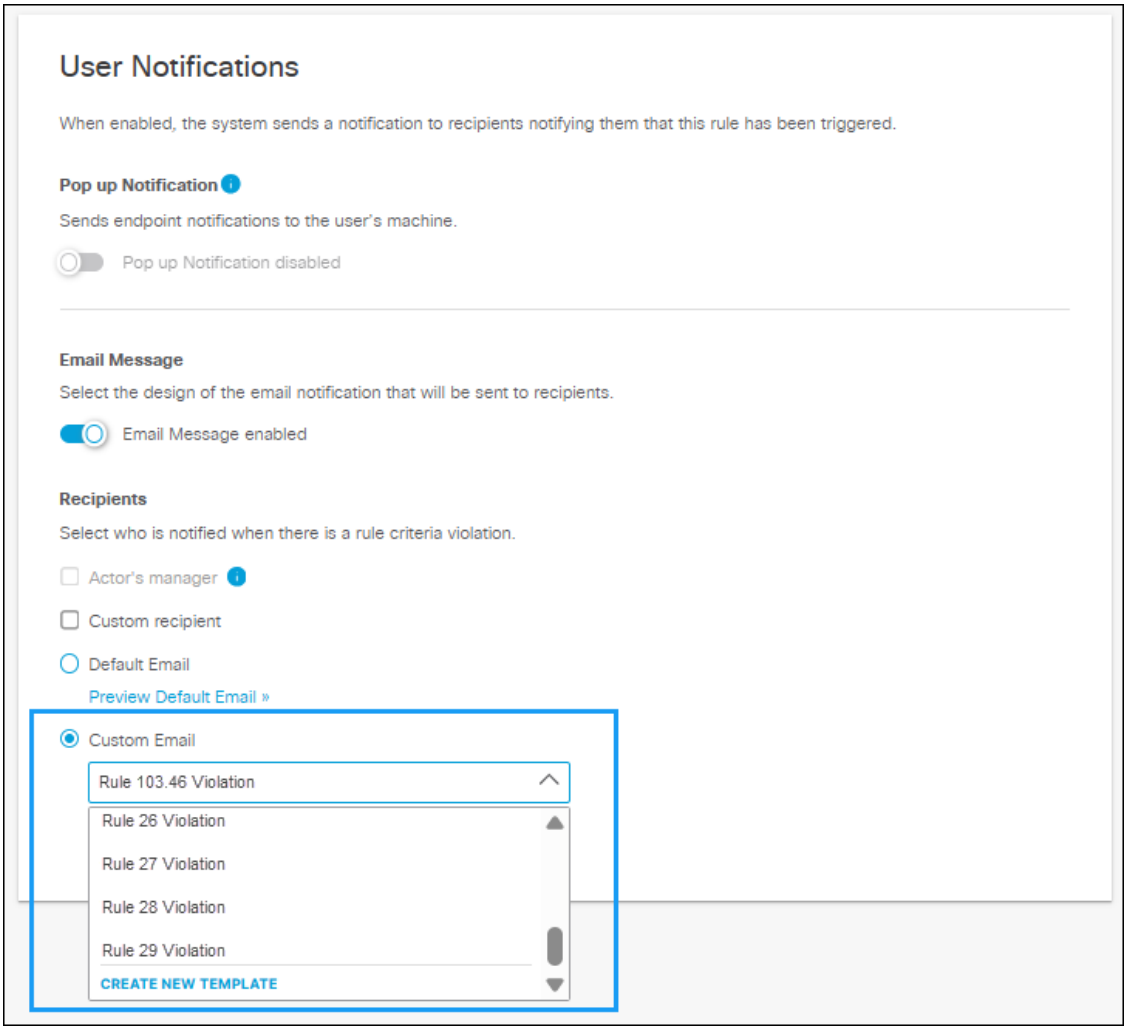
c. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

d. Click **CLOSE** to return to the Data Loss Prevention Policy page.

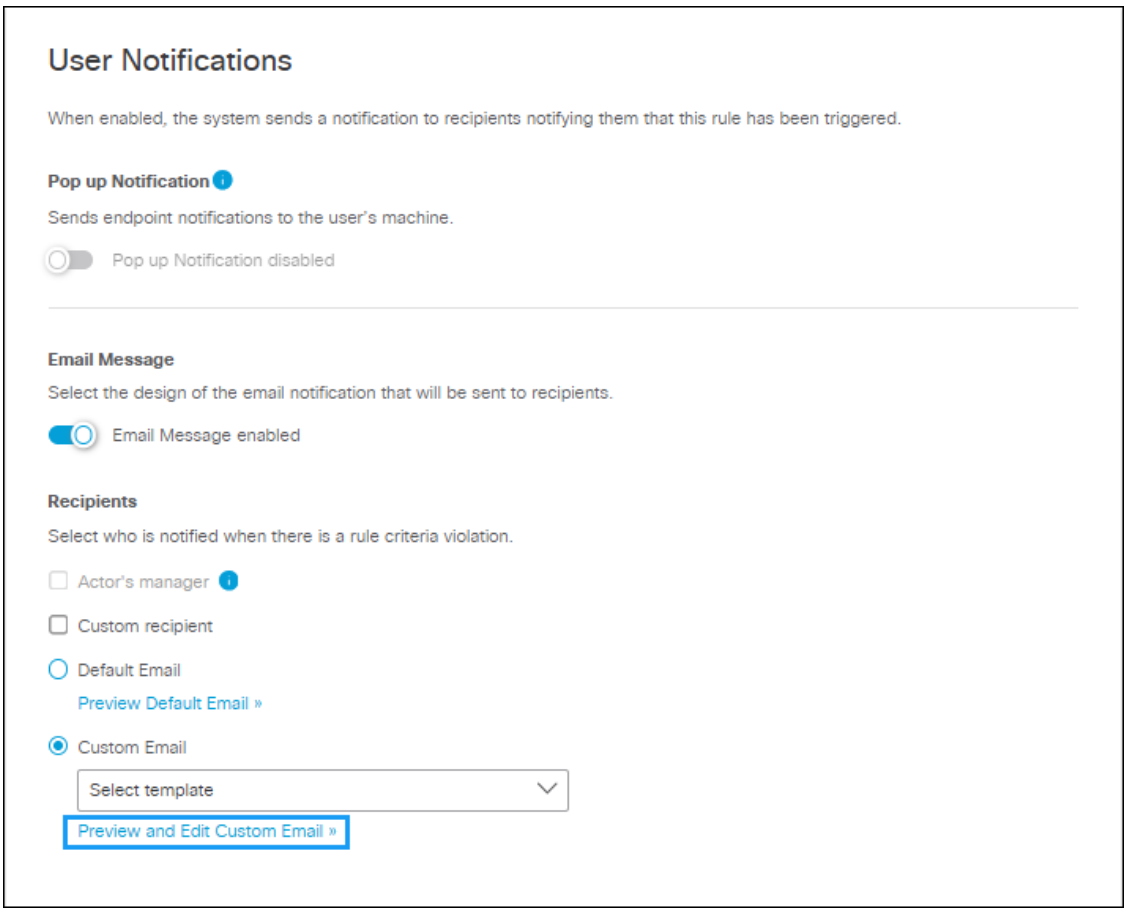
To Use a Custom Email Template:

a. Click **Custom Email**.

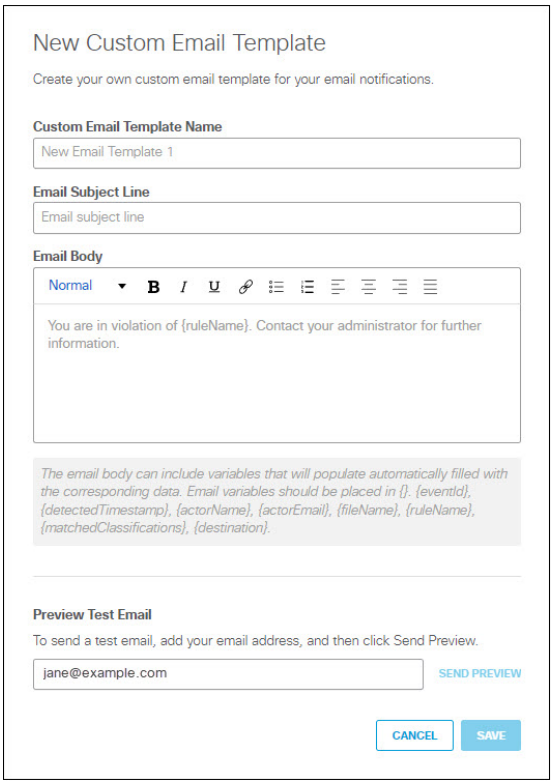
b. From the drop down menu, select an existing custom template, or choose **CREATE NEW TEMPLATE**.

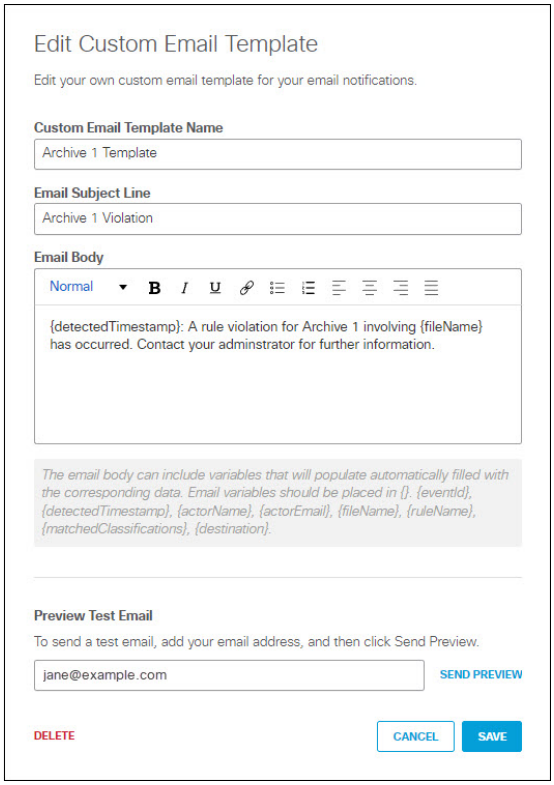


If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.



c. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:





The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Email Template Name**.
2. Enter an **Email Subject Line**.
3. Enter the text of the email in the **Email Body** text box.

   The email text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
   - **{destination}** - URL or IP address of the intended destination for the monitored request.

   > **Note**
   >
   > The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

4. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
5. Click **SAVE** to return to return to the Data Loss Prevention Policy page.

4. Click **Save** to save the rule and make it a part of your DLP policy.

> **Note**
>
> All fields must have options selected to save.

Add a SaaS API Rule to the Data Loss Prevention Policy

Provides instructions for completing the Add a SaaS API Rule to the Data Loss Prevention Policy workflow in Cisco Secure Access. Configure an SaaS API Rule to set the criteria as to what triggers the scanning.

Configure an SaaS API Rule to set the criteria as to what triggers the scanning. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file against this rule's criteria. If a match is made, this rule's action is immediately enforced. If Secure Access detects a violation, the offending file is listed in the Data Loss Prevention Report.

An SaaS API Rule must have at least one of the following two criteria defined:

- Data Classifications – Include files that match data classification of your own making or a built-in data classification provided by Secure Access.
- File Labels – Include files that have specific file label names configured in the value of the files' document properties, or include files that have no labels configured. Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.
  - Microsoft Information Protection (MIP) labels are used to classify and protect data in Microsoft 365 files.
  - Titus labels are a third-party classification system provided by Fortra that can provide additional classification and protection features for Microsoft 365 files.
  - Microsoft Office Sensitivity Labels are a specific type of MIP label focused on indicating the sensitivity of data within Microsoft 365 files.

  The types of file labels Secure Access can scan varies depending on the platform of the tenant:
  - For AWS S3, Azure Storage, Confluence, Dropbox, GitHub, Google Drive, Jira, ServiceNow, Slack, and Webex Teams you can apply filters for MIP and Titus labels.
  - For Microsoft 365 and Box you can apply filters for MIP and Titus labels, and Microsoft Office Sensitivity Labels. (Within the Box application, sensitivity labels are referred to as classification labels.)
  - For Salesforce you can apply filters for Microsoft Office document properties, or Adobe PDF document properties.

> **Note**
>
> Changes to the share permissions or other options on a folder does not trigger a scan of the contents of that folder.

SaaS API rules configured to scan Microsoft Outlook messages scan only outgoing messages. Violations can be triggered by material found in the email subject, message body, or attachments; a single email message may trigger multiple violations: one for the message subject and body, and one for each attachment.

Procedure

1. Create a DLP SaaS API Rule Step 1 – Establish General Settings
2. Select **Data Classifications** to apply to the rule.
3. Make **Files Control** selections for the rule
4. Select **Platform** and **Tenant** for the rule
5. Select **Users** whose files are included or excluded from scanning for this rule
6. Select **Resource Labels** for the rule
7. Select **Resources** for the rule

8. Configure **Exposure Settings** for processing the files to search for data violations
9. Select **Action** to be performed when data matches the rule
10. Enable and configure an **Email Notifications** to be sent to users when a violation occurs

Create a DLP SaaS API Rule Step 1 — Establish General Settings

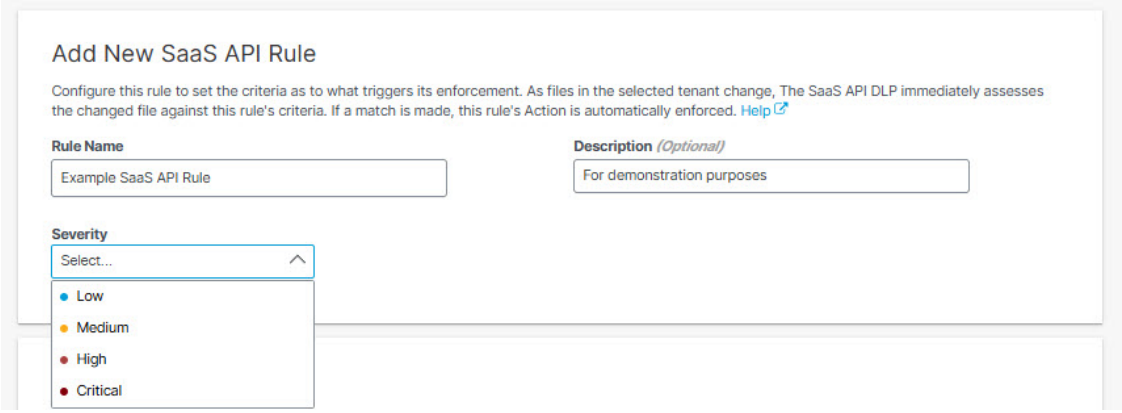
Provides instructions for completing the Create a DLP SaaS API Rule Step 1 – Establish General Settings workflow in Cisco Secure Access. This is the first step in the process to add a SaaS API rule to a DLP policy, in which you create the rule and establish its basic characteristics.

This is the first step in the process to add a SaaS API rule to a DLP policy, in which you create the rule and establish its basic characteristics.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the next step in the process, see Create a DLP Saas API Rule Step 2 – Select Data Classifications

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, click **Add Rule**, and choose **SaaS API Rule**.
2. In the **Add New SaaS API Rule** page, enter a meaningful **Rule Name** and **Description**. Choose a **Severity** value from the drop-down based on the risk involved or importance within the ruleset. (Assigning severity values can help later on when you need to filter events in the Data Loss Prevention report.)



Create a DLP SaaS API Rule Step 2 — Select Data Classifications

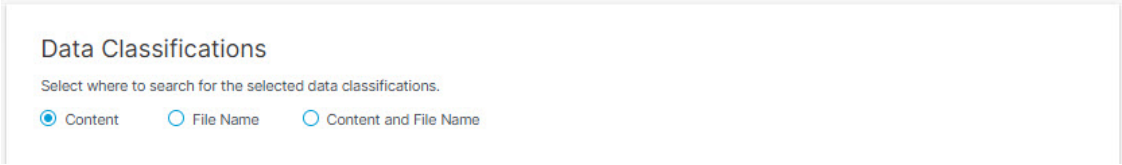
Provides instructions for completing the Create a DLP SaaS API Rule Step 2 – Select Data Classifications workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the second step in the process to add a SaaS API rule to a DLP policy, in which you select the data classifications to apply to the rule.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 1 – Establish General Settings
- For the next step in the process, see Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant

Procedure

1. Under **Data Classifications** select where in scanned files you would like this rule to search for the data classifications that you choose:



Content–(Default) Scans only the content of files for the selected data classifications.

- For Outlook this option scans the subject line and message body of incoming email, and the file content of attachments to incoming email.
- For Salesforce, chatter posts and sObjects can be scanned for content only.
- For Confluence, this option scans page headings and contents, file attachments to pages, and comment headings and contents. Secure Access does not scan file attachments to Confluence comments, or Confluence database tables or whiteboards.
- For Jira, this option scans page headings and contents, comment headings and contents, and file attachments to pages and comments.

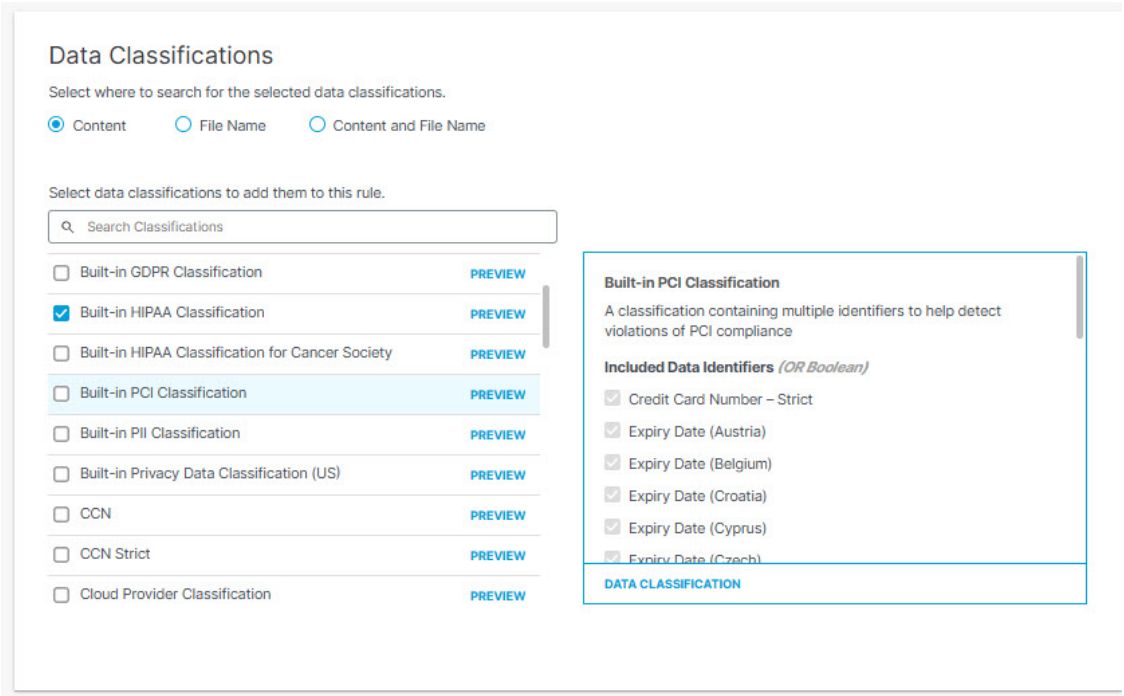
File Name–Scans only file names for the selected data classifications.

- For Outlook this option scans the subject line and message body for incoming email, and the file name for attachments to incoming email.
- For Confluence this option scans page headings and contents, and the file names for attachments to pages. Secure Access does not scan file attachments to Confluence comments, or Confluence database tables or whiteboards.
- For Jira this option scans page headings and contents, and the file names for attachments to pages and comments.

Content and File Name–Scans content and file names for the selected data classifications. Both content and file name do not need to match for the rule to apply, only one or the other.

> **Note**
>
> Choosing **Content**, **File Name**, or **Content and File Name** refers to scanning file uploads for the selected data classifications and configured file labels.

2. Select Data Classifications to apply this rule; you can choose data classifications of your own making or built-in data classifications provided by Secure Access. (See Manage Data Classifications and Built-In Data Classifications.) Hover over **PREVIEW** to view data identifiers associated with each data classification.



Create a DLP SaaS API Rule Step 3 — Select Platform and Tenant

Provides instructions for completing the Create a DLP SaaS API Rule Step 4 – Select Platform and Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the third step in the process to add a SaaS API rule to a DLP policy, in which you select one platform and tenant for the rule.

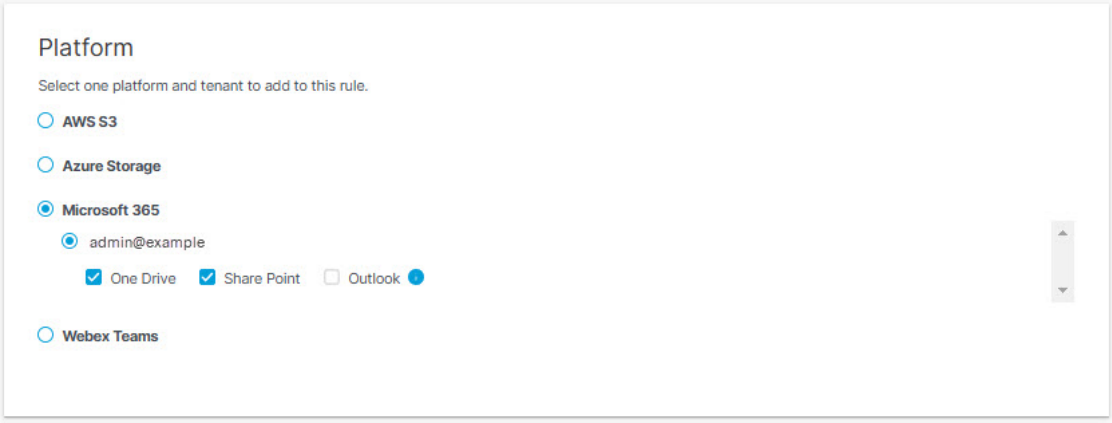
- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Saas API Rule Step 2 – Select Data Classifications
- For the next step in the process, see Create a DLP SaaS API Rule Step 4 – Select Files Controls

Procedure

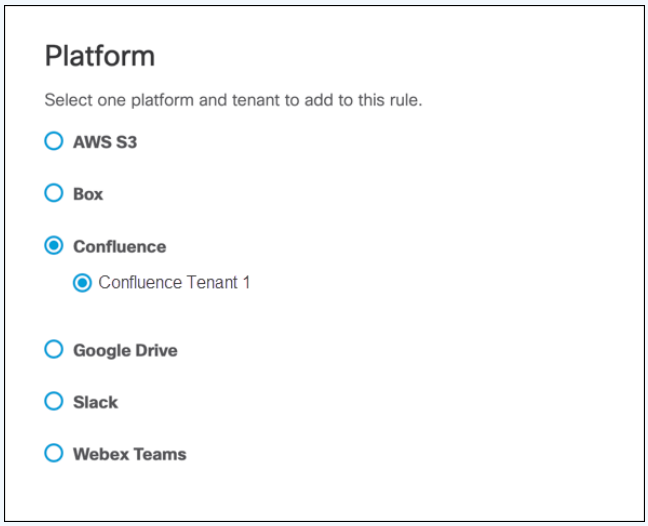
In the **Platform** area, select one platform and tenant for this rule. Only platforms with authorized tenants will appear in the list.

Note

- When you select Microsoft 365 you can select both OneDrive and SharePoint, but you cannot select Outlook in combination with Microsoft OneDrive or SharePoint in the same rule.



- When you select Confluence or Jira, each of the tenants you have established for that platform will appear; you must choose one.



Create a DLP SaaS API Rule Step 4 — Select Files Controls

Provides instructions for completing the Create a DLP SaaS API Rule Step 3 – Select Files Controls workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the fourth step in the process to add a SaaS API rule to a DLP policy, in which you select the files controls to apply to the rule.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 3 – Select Platform and Tenant
- For the next step in the process, see Create a DLP SaaS API Rule Step 5 – Select Users on page 1490

In the **Files Control** area, choose the file filters to apply to this rule. The file filters available depend on the platform you have chosen:

- For AWS S3, Azure Storage, Dropbox, Google Drive, Salesforce, ServiceNow, Slack, and Webex Teams you can apply filters for MIP and Titus labels, and file size. You can also filter for files with no labels.
- For Microsoft 365 and Box you can apply filters for MIP and Titus labels, Microsoft Office Sensitivity Labels, and file size. (Within the Box application, sensitivity labels are referred to as classification labels.) You can also filter for files with no labels.

> **Note**
>
> You cannot select labels for filtering and filter for files with no labels in a single rule.

Procedure

1. For all platforms select **File Size** filter criteria.

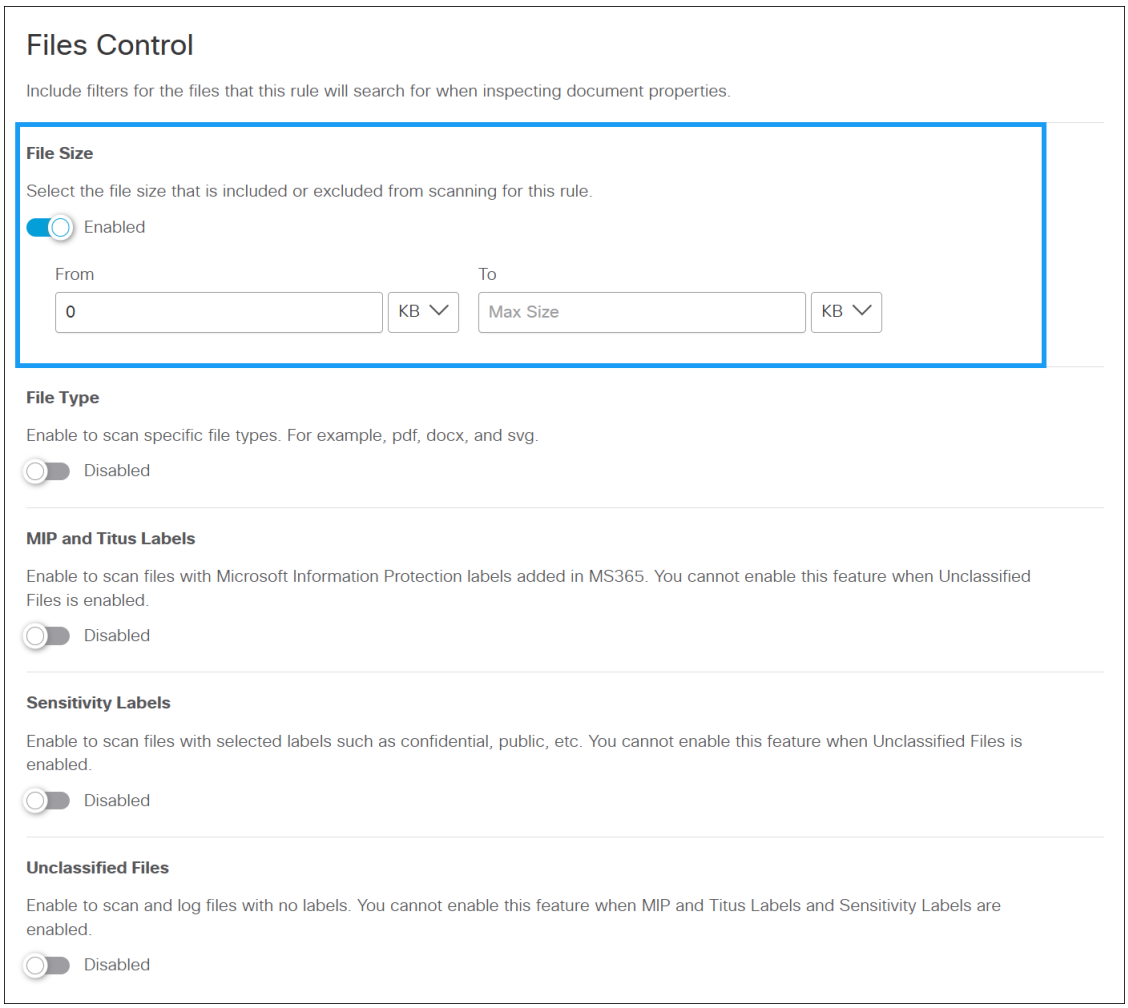
   The **File Size** area has two use cases:

   - In a rule with only custom file size criteria, DLP applies the rule action to files that match the file size criteria, regardless of content. (This may be useful in situations where you want to exclude certain low-risk files below a certain size from inspection, so as not to waste processing time on insignificant events.)
   - In a rule that specifies a custom file size along with other criteria such as Data Classification, the DLP applies the rule action to files that match the other criteria within the file size specified up to the first 50 MB of plain text. (Secure Access does not scan file content beyond the first 50 MB regardless of the file size specified here.)

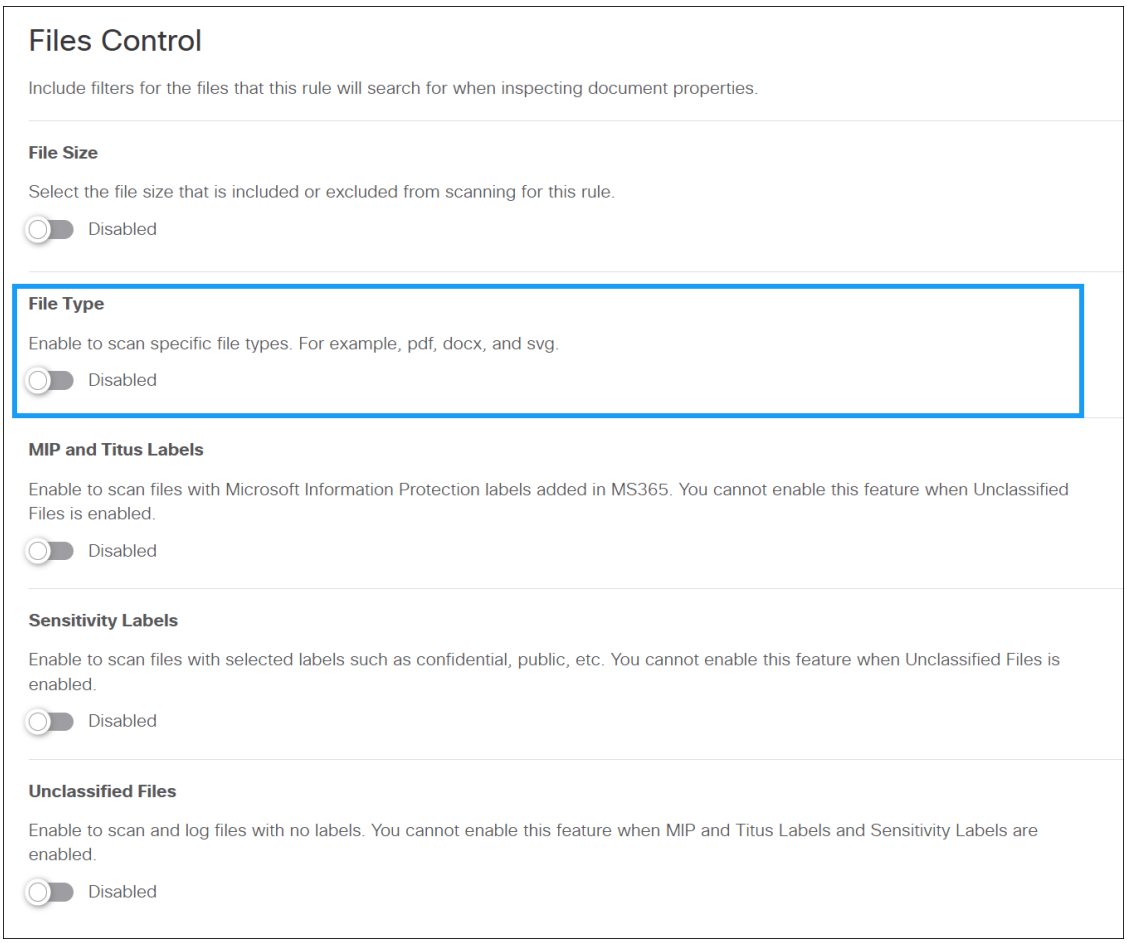
   In the **File Size** area choose from two options:

   - To scan up to the first 50 MB of plain text of all files that meet other criteria defined by this rule, enable the **File Size** toggle and do not select custom sizes. (A rule that uses this option must also specify Data Classifications.)
   - To specify the minimum and maximum size limits the system will scan for files that meet other inclusion criteria defined by this rule, if there are any, enable the **File Size** toggle and select custom size values. If the file size exceeds the first 50 MB of the file, Secure Access scans only up to the first 50 MB of plain text in the file. (I.e., if you specify a minimum file size greater than 50 MB, Secure Access will not scan for other criteria specified in the rule.)

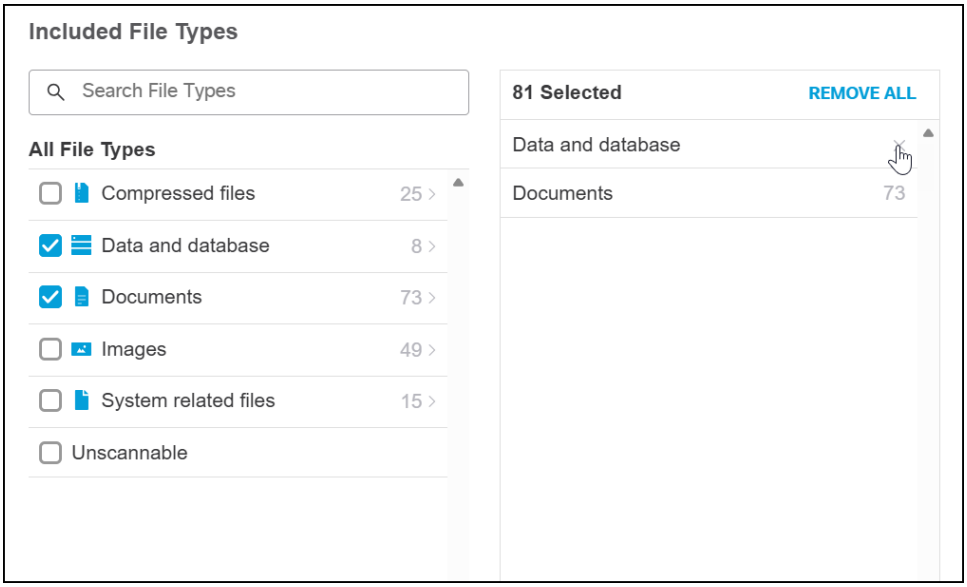
     You can choose to apply the rule action only to files that are greater than a minimum size you specify, or to files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB.



2. In the **File Type** area, configure the rule to include specific file types or to exclude unrecognized file types.
   a) Click the toggle to enable file type filtering.

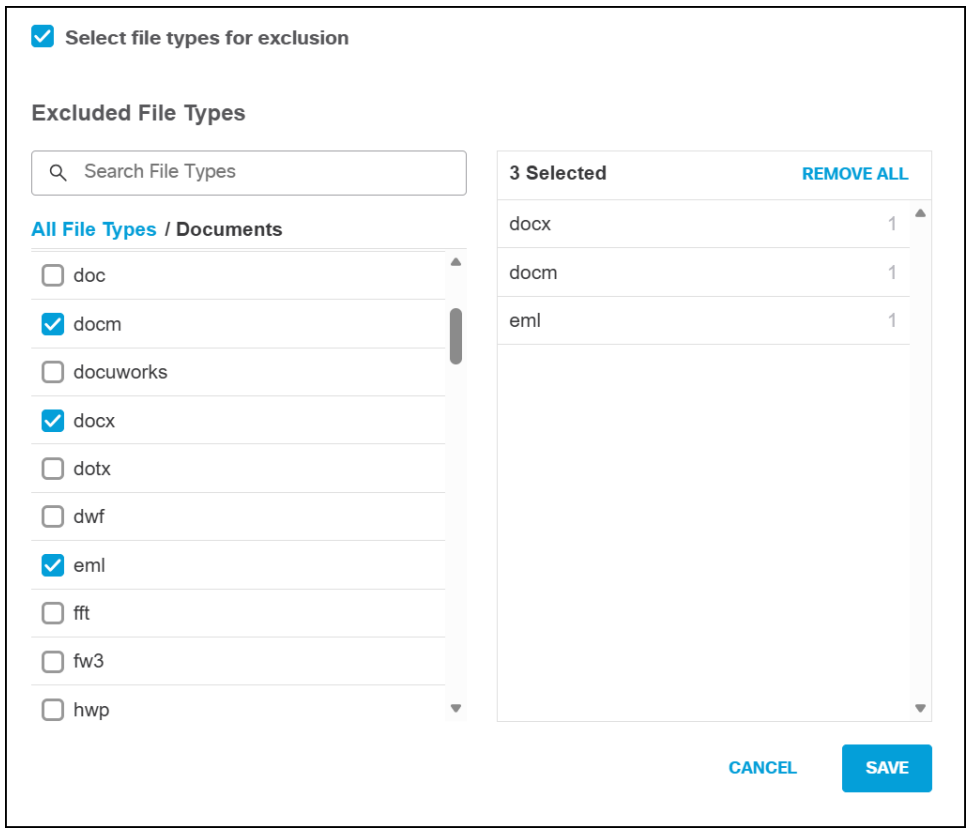


b) To include file types, use the search box to search for file types or browse within the lists for file types. Check the boxes for the file types to include individually or by group. Selected file types appear on the right.



c) To exclude file types, check **Select the file type for exclusion** check box.

In **Excluded File Types** section, use the search box to search for file types or browse within the lists for file types. Check the boxes for file types to exclude individually or by group. Selected file types appear on the right.

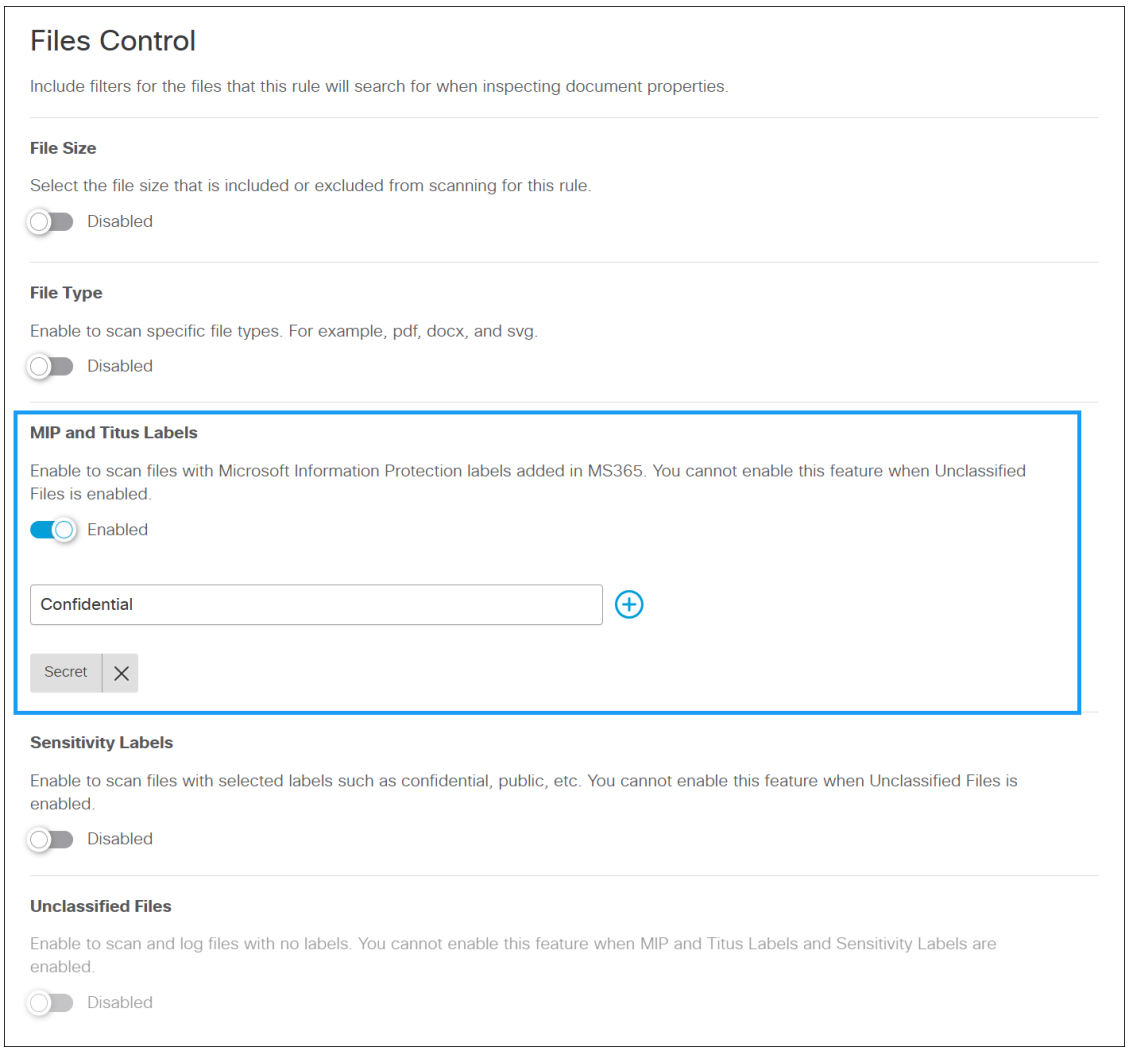


3. Specify **MIP and Titus labels**.

   For all platforms, you can enable MIP and Titus labels and add up to 10 case-sensitive file label names to apply to the rule. The rule will search for any of the configured label names in the files' document properties. This includes Microsoft Office Document Properties and Adobe PDF Document Properties.

   For Outlook, this applies to files attached to incoming mail. File uploads to Confluence and Jira are not scanned for file labels.

   Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.



4. For Microsoft 365 OneDrive or Sharepoint tenants, or for Box tenants, select **Sensitivity Labels**.

   For Microsoft 365 OneDrive or Sharepoint tenants, or for Box tenants, you can enable sensitivity labels and select from the list of sensitivity labels that have been created for your tenant. You may select any number of the labels displayed.

   Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

Note

Within the Box application, these labels are referred to as classification labels.

Note

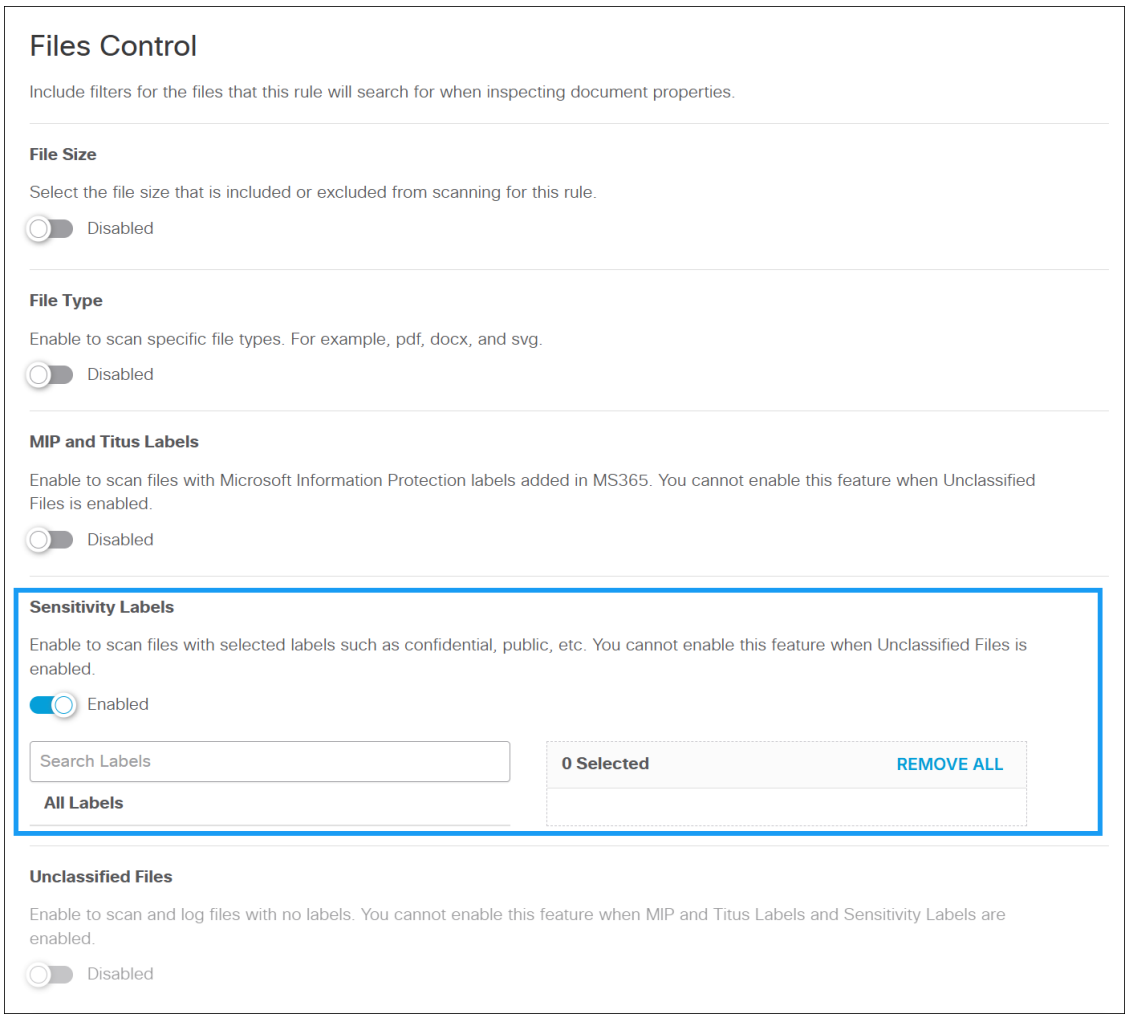
Secure Access supports the detection of Microsoft sensitivity labels in the inspected file's properties values for Microsoft Word, Excel, PowerPoint, and .pdf files. Ensure you configure the rule with the name of the sensitivity labels, not the display names.

The system does not scan the following for file labels:

- Files attached to Outlook emails.
- File uploads to Jira.
- File uploads to Confluence.

Note

If you create new sensitivity labels for your Microsoft 365 or Box tenant, it may take up to four hours for them to appear in the Secure Access interface.

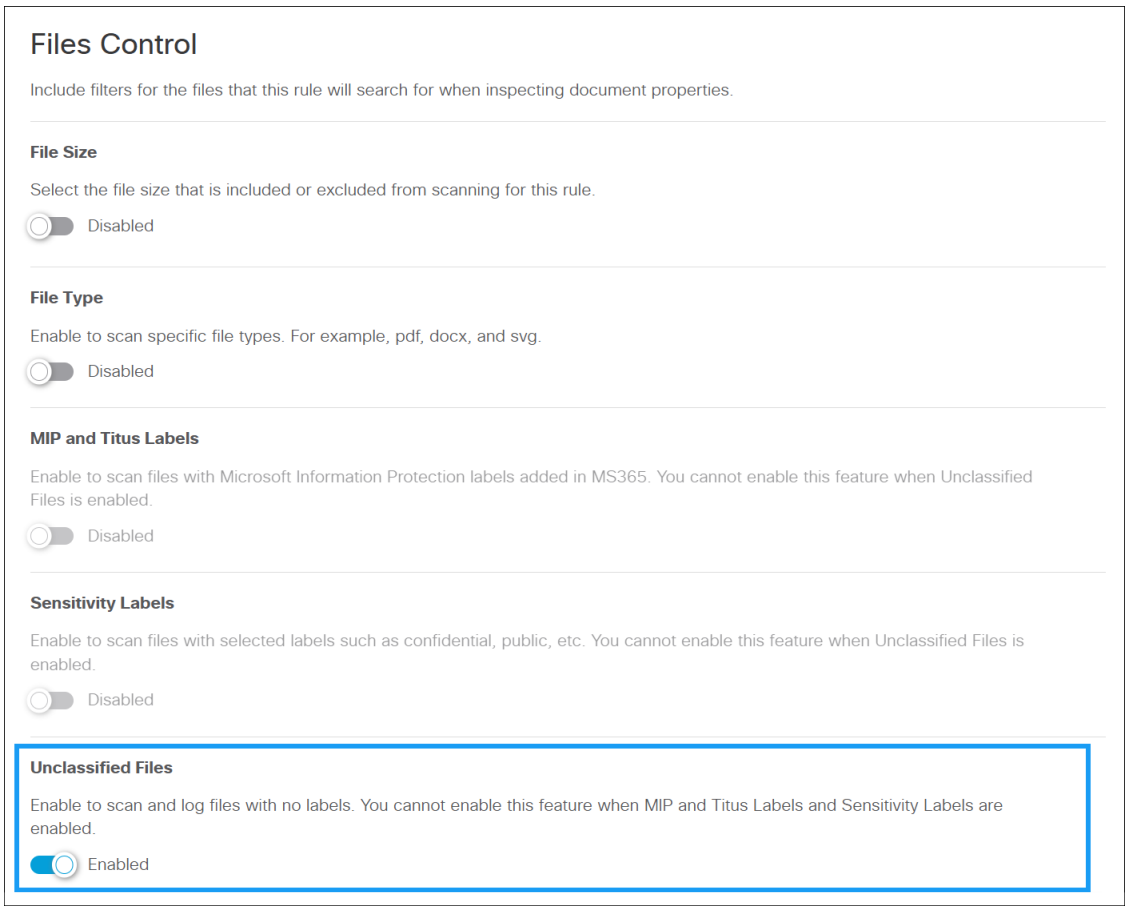


5. In the **Unclassified Files** area, click the toggle to include files that have no labels associated with them.

   This includes Microsoft Office Document Properties (or Titus labels) and Adobe PDF Document Properties, as well as Microsoft Office Sensitivity Labels (which are referred to as classification labels in Box).

   For Microsoft Office Document Properties, this includes only the Label Value field in the custom document properties.

   Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.



Create a DLP SaaS API Rule Step 5 — Select Users

Provides instructions for completing the Create a DLP SaaS API Rule Step 5 – Select Users workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the fifth step in the process to add a SaaS API rule to a DLP policy, in which you select users whose files are included or excluded from scanning for this rule.

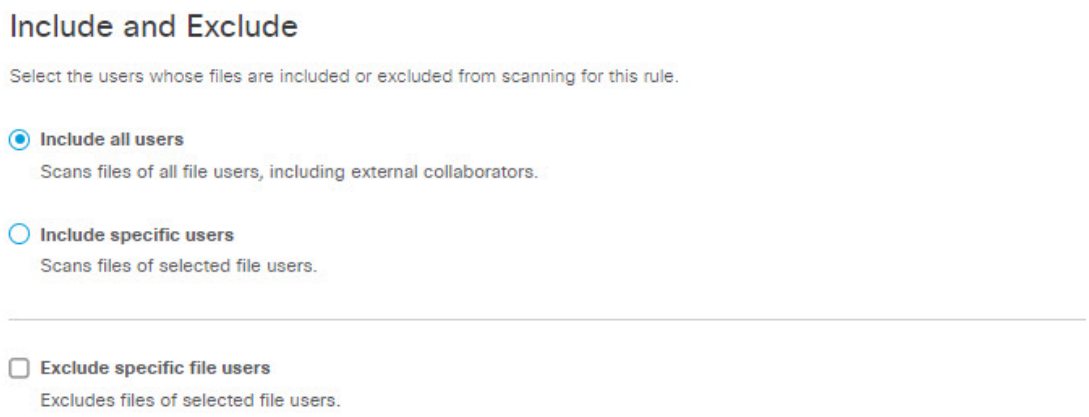
- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 4 – Select Files Controls
- For the next step in the process, see Create a DLP SaaS API Rule Step 6 – Select Resource Labels

Procedure

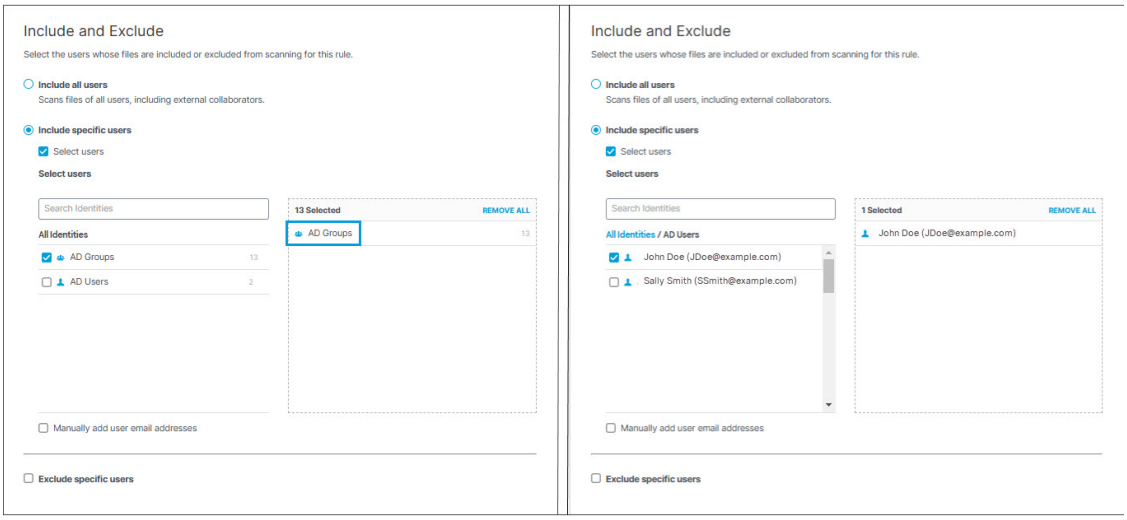
In the **Include and Exclude** area, select users whose files are included or excluded from scanning for this rule. Make selections to include or exclude users from being matched. (For Outlook, user refers to the email sender. For Confluence and Jira, user refers to the owner of the page to which the file is attached.)

- Click the **Include all users** radio button to scan files from all users, including external collaborators.

> **Note**
>
> If you have selected a Salesforce Commerce tenant, **Include all users** is the only option available.



- Click the **Include specific users** radio button to scan files from users selected in one of the following ways:
  - Check the **Select users** check box to include scanning for selected users as per the rule. You can select the entire AD group or search for identities by AD username or AD Group. The selected identities appear in the box on the right.

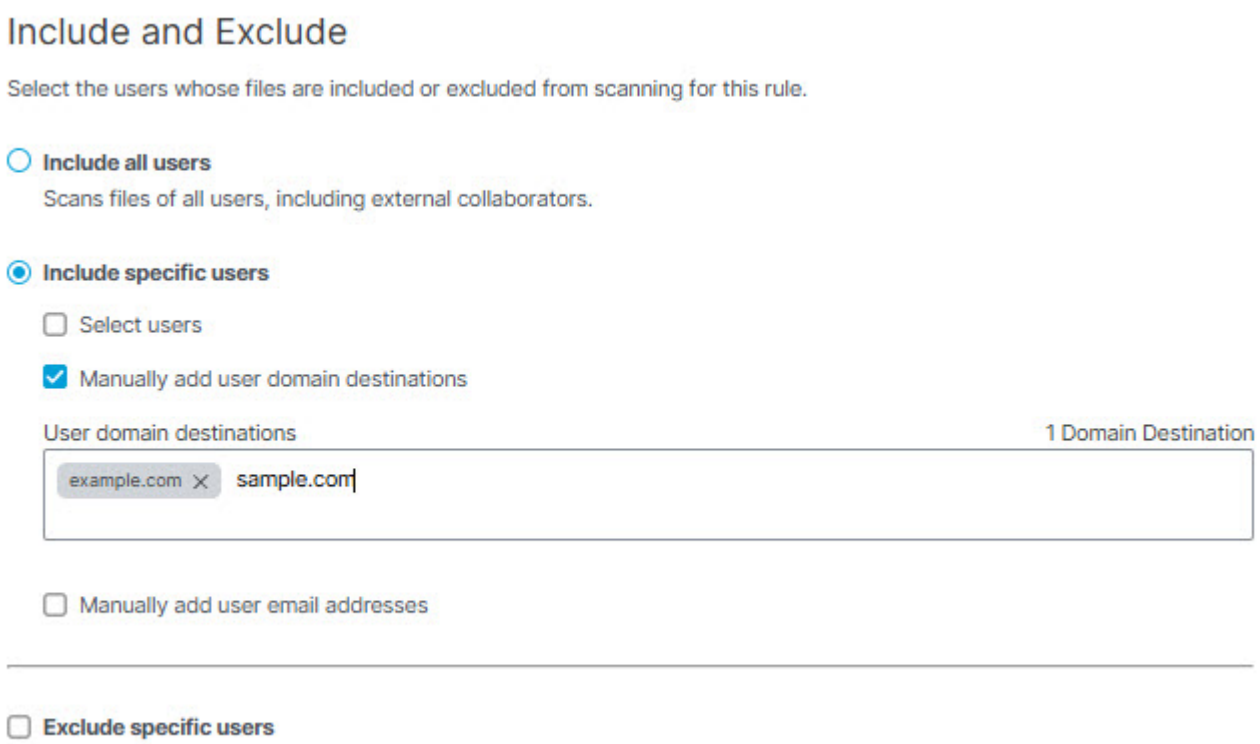


> **Note**
>
> Identities added to a category after the category has been included or excluded from a rule will be included or excluded from the rule as if they were part of the category at the time the rule was created.

  - Check the **Manually add user domain destinations** check box to specify domains where rules will apply to users within those domains.

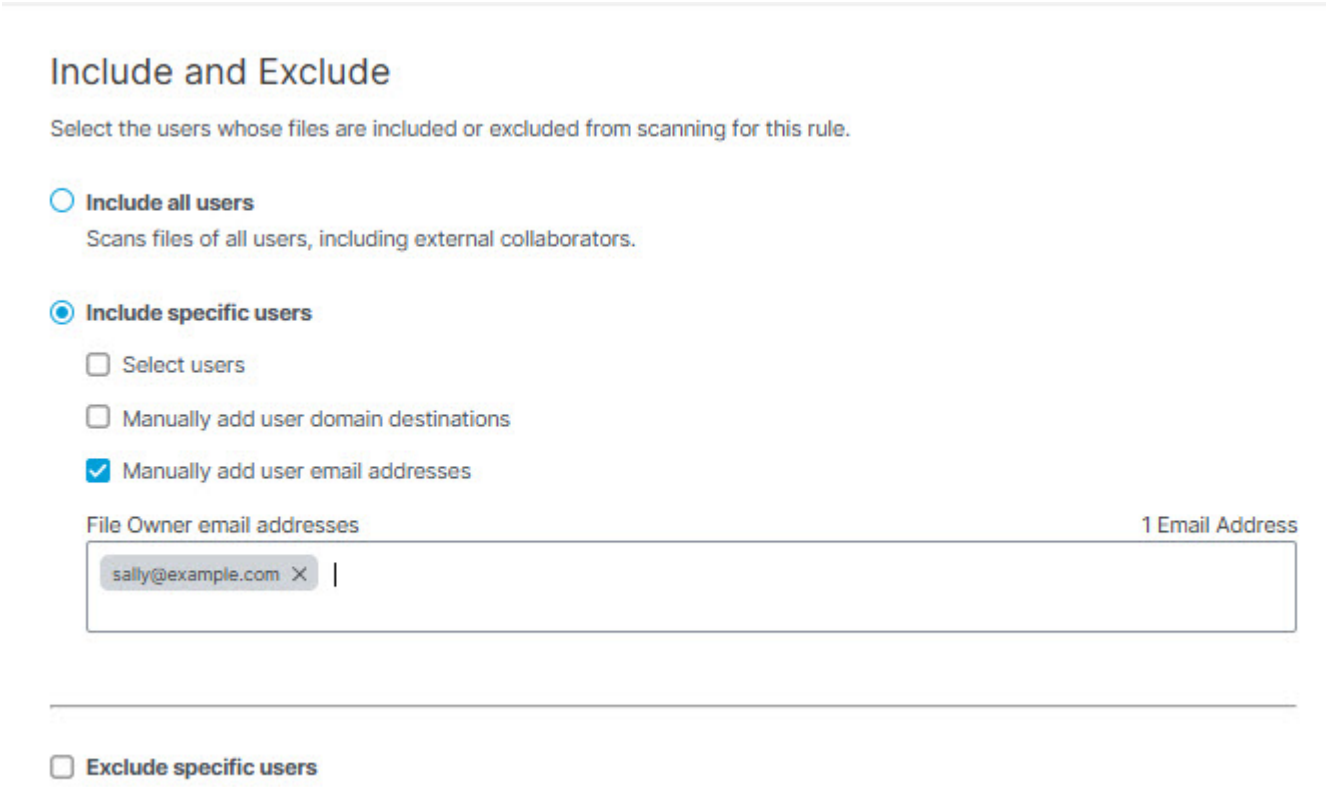
    This option appears only if you have chosen **Outlook** or **Webex Teams** for **Platform**. You can enter a maximum of 1,000 user domain destinations.

- For **Outlook** Secure Access scans message recipients for domain destination matches.
- For **Webex Teams** Secure Access scans the Webex space owner for domain destination matches.

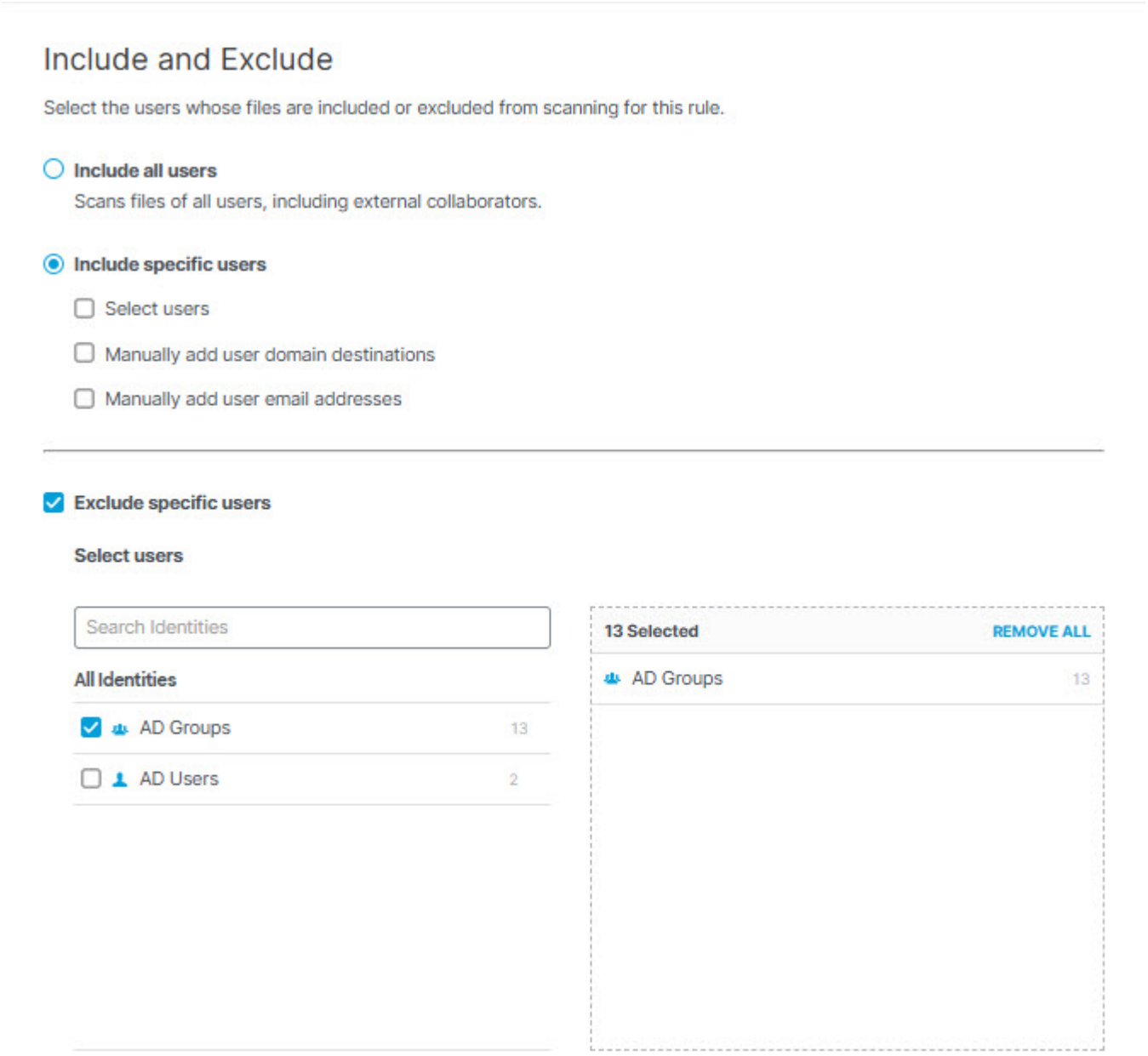


- Check the **Manually add user email addresses** check box to specify email addresses of file owners to which the rule will apply.

  Enter the users' email addresses in the text box.



- Check the **Exclude specific file users** check box to exclude selected users from being matched by this rule. Similarly to selecting identities for inclusion, you can select all AD groups, All AD Users, individual groups, or individual users. Search for identities by AD user name or by AD Group name. Selected identities will appear in the box on the right.



Create a DLP SaaS API Rule Step 6 — Select Resource Labels

Provides instructions for completing the Create a DLP SaaS API Rule Step 6 – Select Resource Labels workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the sixth step in the process to add a SaaS API rule to a DLP policy, in which you add the resource labels.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 5 – Select Users
- For the next step in the process, see Create a DLP SaaS API Rule Step 7 – Select Resources

Procedure

The **Resource Labels** area appears only if you have selected **AWS**, or **Azure** for **Platform**. In the **Resource Labels** area, enter key/value pairs you have applied as tags to objects in AWS S3 buckets or Azure storage accounts or containers. Each resource label you enter here identifies the data Umbrella will monitor within your buckets (for AWS) or storage accounts or containers (for Azure). It may take a few minutes for resource labels you enter here to propagate to the policy page, depending on how many there are and the state of the discovery process.



Create a DLP SaaS API Rule Step 7 — Select Resources

Provides instructions for completing the Create a DLP SaaS API Rule Step 7 – Select Resources workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

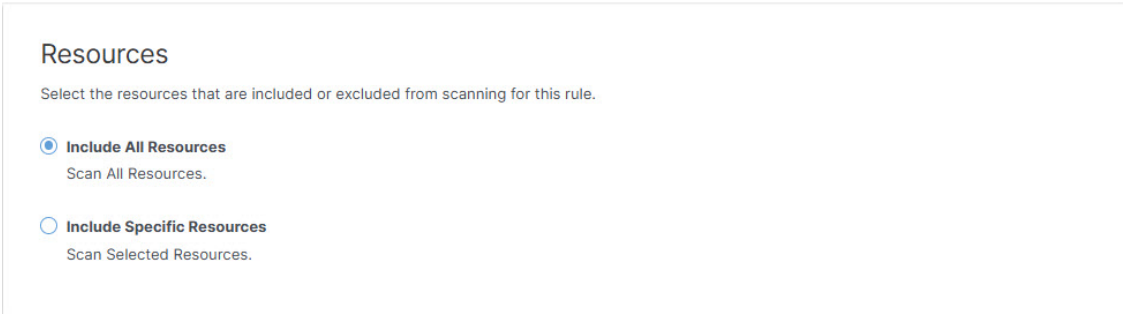
This is the seventh step in the process to add a SaaS API rule to a DLP policy, in which you add resources.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 6 – Select Resource Labels
- For the next step in the process, see Create a DLP SaaS API Rule Step 8 – Configure Exposure Settings

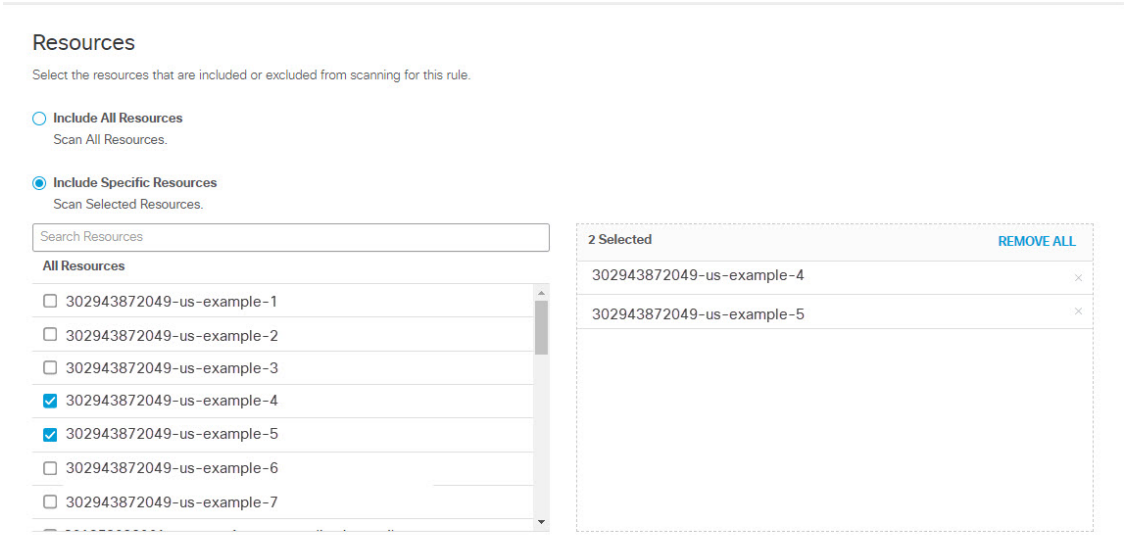
Procedure

The **Resources** area appears only if you have selected **AWS S3**, **Azure Storage**, or **Webex** for **Platform**.Under **Resources** make selections to define S3 buckets (for AWS) or containers (for Azure) to include or exclude from being matched by this rule:

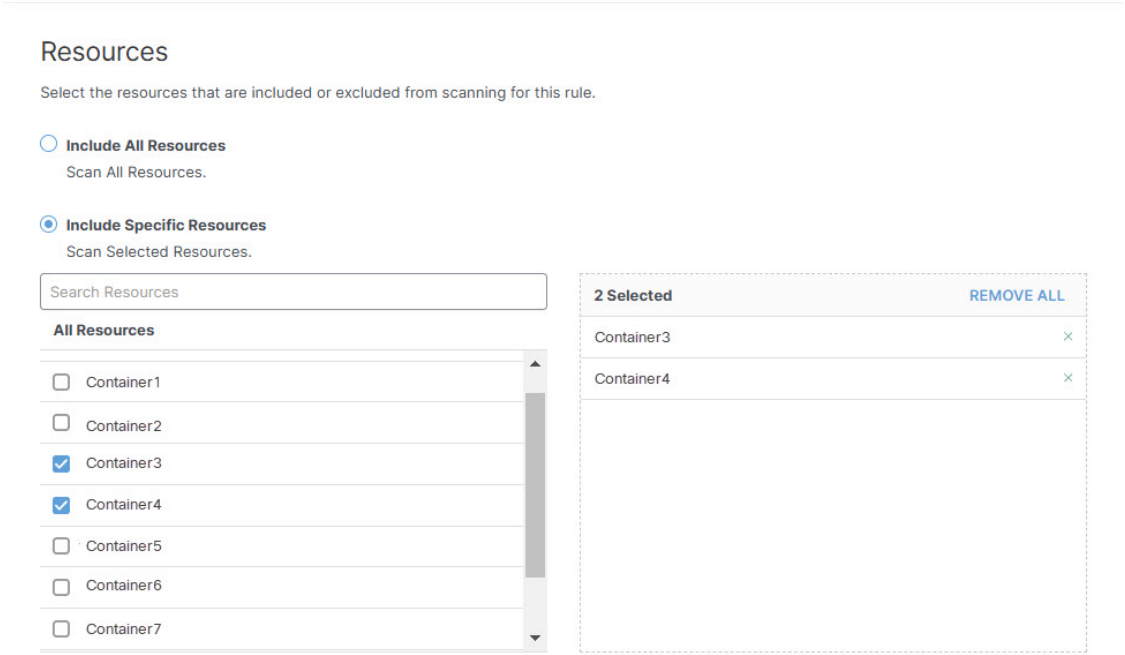
- Click the **Include all resources** radio button (the default) to include all resources available on your platform for scanning associated with your account (including non-admin resources).



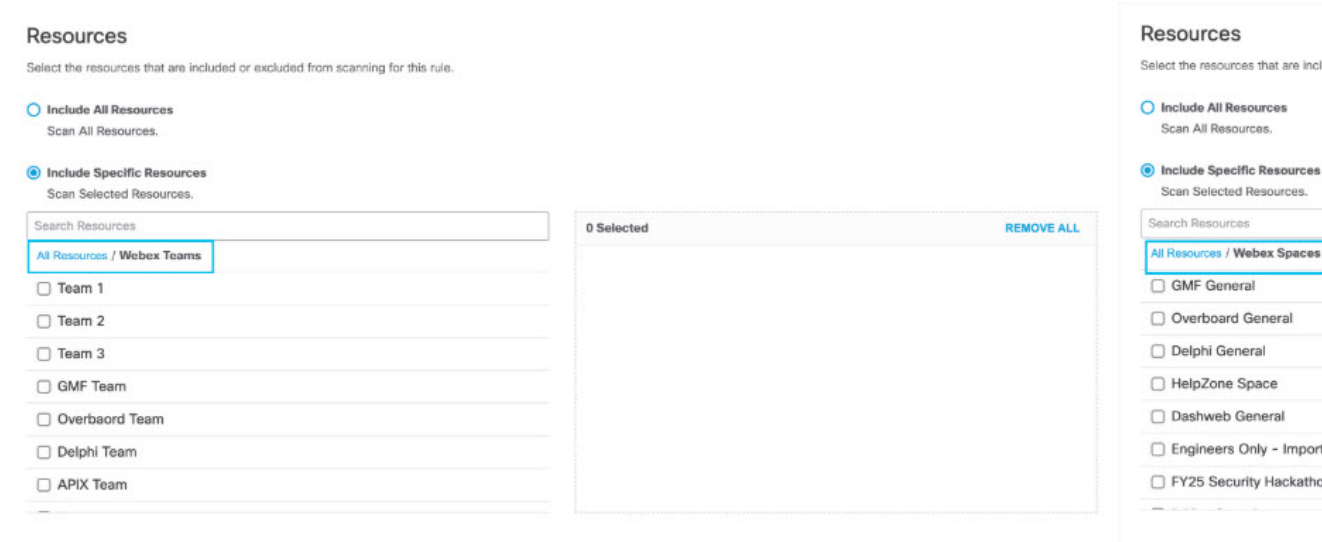
- Click the **Include specific resources** radio button to display a list of resources available and select the ones you want to include for matching.
  - For **AWS** you can select S3 buckets



- For **Azure** you can select containers



- For **Webex** you can select **Webex Teams** and **Webex Spaces**



Create a DLP SaaS API Rule Step 8 — Configure Exposure Settings

Provides instructions for completing the Create a DLP SaaS API Rule Step 8 – Configure Exposure Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the eighth step in the process to add a SaaS API rule to a DLP policy, in which you select the file sharing permissions for processing the files to search for data violations.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 7 – Select Resources
- For the next step in the process, see Create a DLP SaaS API Rule Step 9 – Select Action

Procedure

Under **Exposure**, optionally select the file sharing permissions to consider when processing files to search for data violations:

- **Shared Publicly**- Select to include files accessible to all users with the link to the file.
- **Shared with External Users**- Select to include files shared with users who do not belong to the authorized domains.
- **Domain-wide Share**- Select to include files shared with all users in a domain.
- **Shared with Internal Users**- Select to include files shared with users who belong to the authorized domains.
- **Shared with Specific Users**- Select to include files shared with specific users by their email addresses.
- **Shared with Specific domains**- Select to include files shared with specific, defined domains.

Note

A maximum of 1,000 users can be added as exclusions in a policy.

The table below indicates which **Exposure** settings are available for each platform:

	Shared Publicly	Domain-wide share	Shared with internal users	Shared with external users	Shared with specific users	Shared with specific domains
AWS S3	✓	–	✓	–	–	–
Azure Storage	✓	–	✓	–	–	–
Box	✓	–	–	✓	✓	–
Confluence	–	–	✓	–	✓	–
Dropbox	✓	✓	✓	✓	✓	–
GitHub	✓	–	–	–	–	–
Google	✓	✓	✓	✓	✓	✓
Jira	–	–	✓	–	✓	–
Microsoft Office 365 SharePoint Online	✓	✓	✓	✓	✓	✓
Microsoft Office 365 OneDrive	✓	✓	✓	✓	✓	✓
Microsoft Office 365 Outlook	–	–	✓	✓	✓	✓
Salesforce	✓	–	✓	✓	✓	✓
Service Now	✓	✓	–	✓	✓	–
Slack	–	✓	✓	✓	✓	–
Webex Teams	–	–	✓	✓	✓	–

Use the **Exclude** section to refine rule processing by omitting specific entities from your policy. Check **Exclude specific users** to enable the addition of individual email addresses or entire domains that you want to exclude from data violation monitoring

- **Add user email addresses**- Select to specify individual user email addresses to exclude from the rule.
- **Add user domains**- Check to specify user domains to exclude from the rule.

The table below indicates which **Exclude** settings are available for each platform:

	Add user email addresses	Add user domains
AWS S3	–	–
Azure Storage	–	–
Box	–	–
Confluence	–	–
Dropbox	–	–
GitHub	✓	✓
Google	✓	✓
Jira	–	–
Microsoft Office 365 SharePoint Online	✓	✓
Microsoft Office 365 OneDrive	✓	✓
Microsoft Office 365 Outlook	✓	✓
Salesforce	✓	✓
Service Now	–	–
Slack	–	–
Webex Teams	–	–

Note

You can configure a policy using only **Exposure** settings for M365, Google, Salesforce, and GitHub.

Note

Exclusion settings take precedence over inclusion settings; if a user or domain is selected in both sections, the exclusion will override the inclusion.

Note

A DLP rule can be configured with either Data Classifications, File Labels or both. Exposure is an optional criterion.

When a DLP rule is configured with all 3 criteria, then a DLP event is raised when any of the selected Data Classifications and when any of the configured file labels are detected in the inspected file and when the file's permissions match any of the selected exposure settings.

Create a DLP SaaS API Rule Step 9 — Select Action

Provides instructions for completing the Create a DLP SaaS API Rule Step 9 – Select Action workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the ninth step in the process to add a SaaS API rule to a DLP policy, in which you select an **Action** to be performed when data matches the rule.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 8 – Configure Exposure Settings
- For the next step in the process, see Create a DLP SaaS API Rule Step 10 – Enable and Configure Email Notifications

Procedure

1. From the **Action** drop-down list, choose **Monitor**, **Quarantine**, **Delete** or **Revoke Access**.
   - **Monitor**- Detects and logs a DLP event for every modified file violating this rule's criteria
   - **Quarantine**- Isolates a file that violates the rule criteria to the quarantine folder (except for Salesforce) and revokes all shares
   - **Delete**- Permanently deletes when a change is detected that violates the rule criteria (This option is available only for Webex Teams, and applies for a violation within a post, as well as a violation within a file attached to a post.)
   - **Revoke Access**- Removes public link, all external or internal users, and any share permission within the entire organization. This action also removes the file owner and transfers the ownership to the selected user.

   The table below indicates which Actions settings are available for each platform:

	Monitor	Quarantine	Delete	Revoke Access
AWS S3	✓	–	–	–
Azure Storage	✓	–	–	–
Box	✓	✓	–	✓
Confluence	✓	–	–	–
Dropbox	✓	✓	–	✓
GitHub	✓	–	–	–
Google	✓	✓	–	✓
Jira	✓	–	–	–
Microsoft Office 365 Sharepoint Online	✓	✓	–	✓
Microsoft Office 365 OneDrive	✓	✓	–	✓
Microsoft Office 365 Outlook	✓	–	–	–
Salesforce	✓	✓	–	–
Salesforce Commerce	✓	–	–	–

	Monitor	Quarantine	Delete	Revoke Access
Service Now	✓	✓	–	–
Slack	✓	–	✓	–
Webex Teams	✓	–	✓	–



If you choose **Quarantine** for Microsoft OneDrive, Sharepoint Online, Box, Dropbox, or Google Drive:

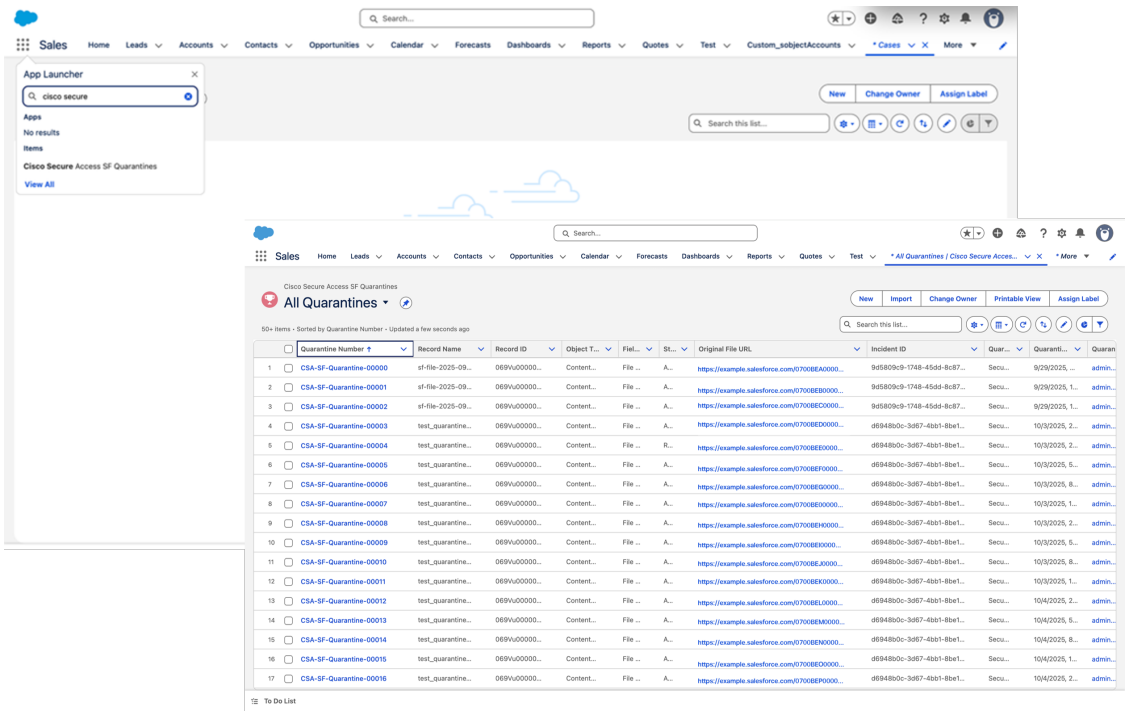
- The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Secure Access created in the root path of the Global Admin who authorized the tenant.
- In lieu of the quarantined file, a text file is left in the original location with the name *`filename`*`.ppt_`*`Unique-Event-ID`*`_Cisco_Quarantined.txt` explaining to the original File Owner that the file is identified as exposing sensitive data and for more information to contact their organization administrator.
- The user who authorizes access to Secure Access will have access to the quarantine folder. All other accesses and collaborators are removed.
- Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.

If you choose **Quarantine** for ServiceNow:

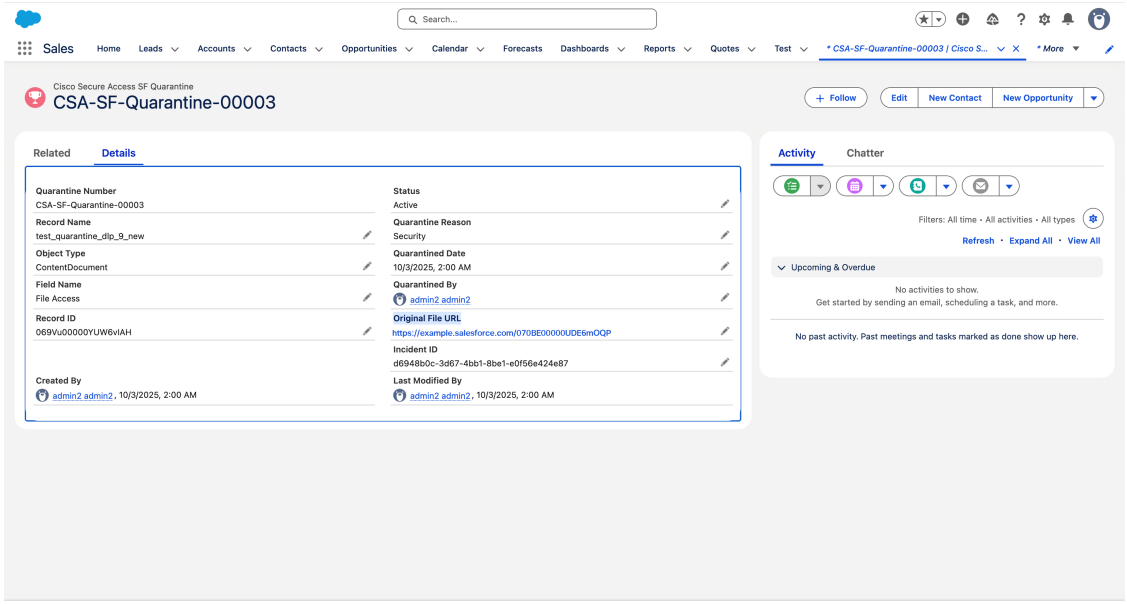
- The file identified as exposing sensitive data is moved to a table named **Cisco_Quarantine_Malware** which can be access only by the admin user who authorized the ServiceNow tenant.
- A footprint is attached to the notes\activities area of the table the file was originally attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.

If you choose **Quarantine** for Salesforce:

- Secure Access applies the **Quarantine** response action to files only (including those attached to chatter posts). Secure Access performs the following for quarantined Salesforce files:
  - Remove all collaborators and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.



Click on the listing for an individual file to see the information about it:



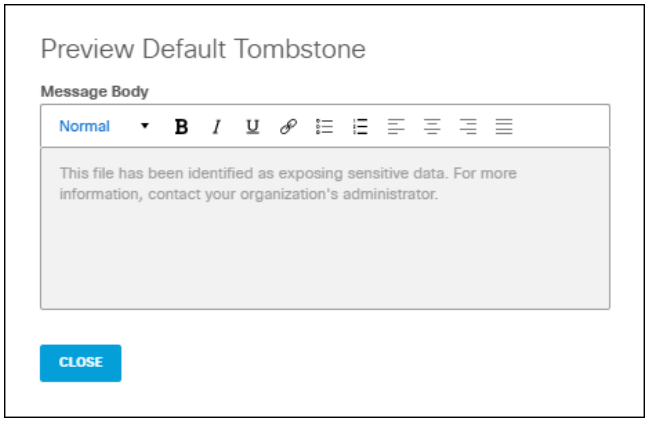
- Replace the file in its original location with a text file named `filename_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

> **Note**
>
> - Quarantine attempts may fail if the files have been locked or blocked by settings within their native platforms. Settings local to the platform where a file resides take precedence over Secure Access' ability to detect or remediate DLP violations or malware.
> - If your DLP rules process files from Microsoft OneDrive, SharePoint Online, Box, Dropbox, ServiceNow, Salesforce, or Google Drive and you restore a quarantined file that still violates rule criteria, the system will quarantine that file again. To prevent the system from quarantining the file again, remove the file's violation, or update the rule's criteria.

2. If you chose Microsoft Office 365 OneDrive, Microsoft Office Sharepoint Online, Box, Dropbox, Google Drive, or Service Now, you can define the message to appear in the **Tombstone File** when files are quarantined.

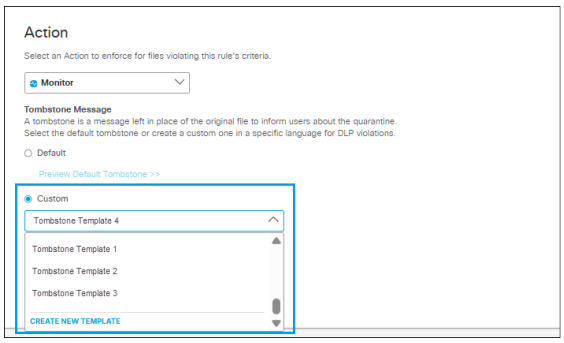
   A file with malicious content may be quarantined when first detected during the SaaS API scanning process, or the user may choose to manually quarantine a file when reviewing the Data Loss Prevention Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

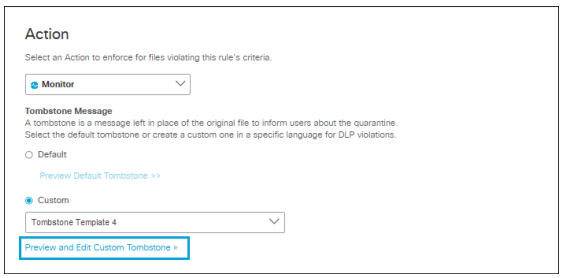
   - **To Use the Default Tombstone Template:**
     a. Click **Default**.
     b. To preview the content of tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.



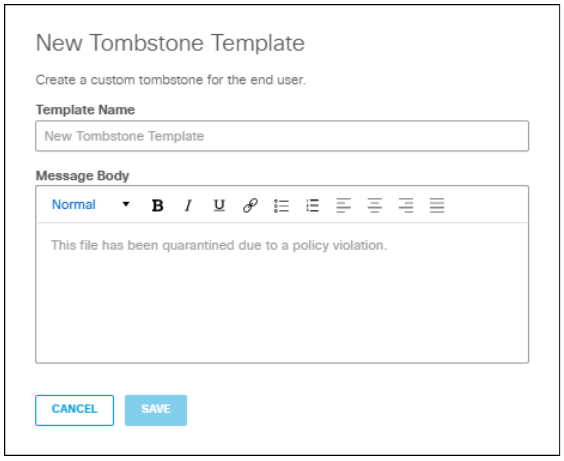
     c. Click **CLOSE** to close the preview.

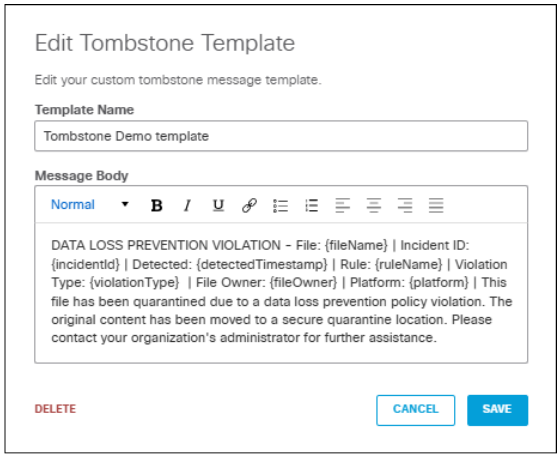
   - **To Use a Custom Tombstone Template:**
     a. Click **Custom**.
     b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.





c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:





The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

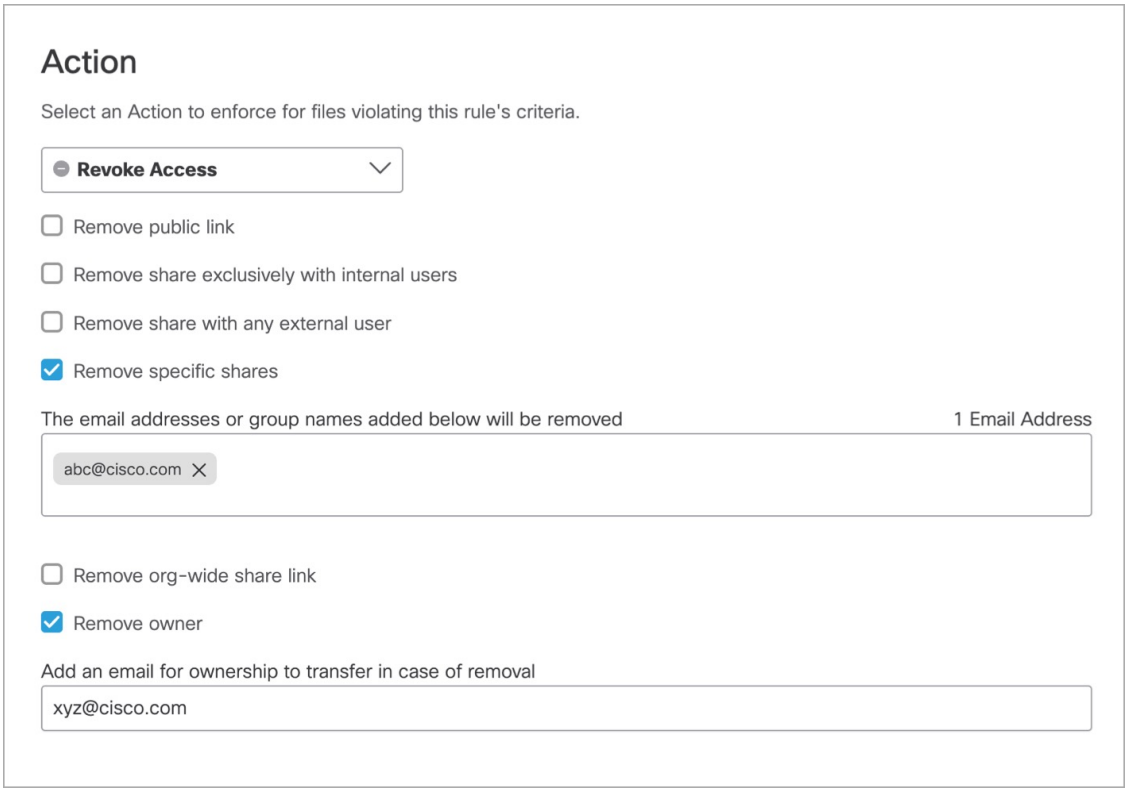
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

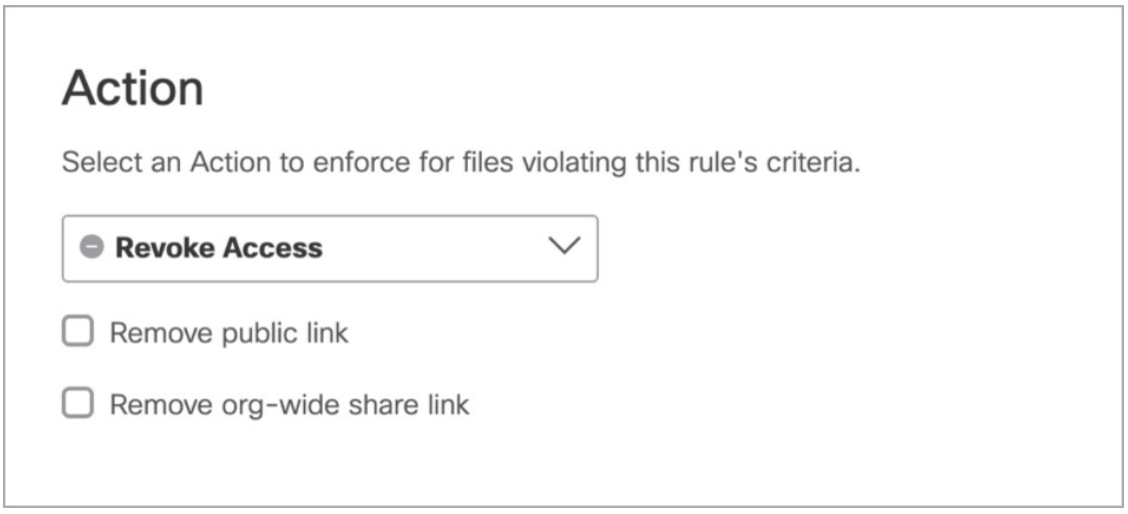
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

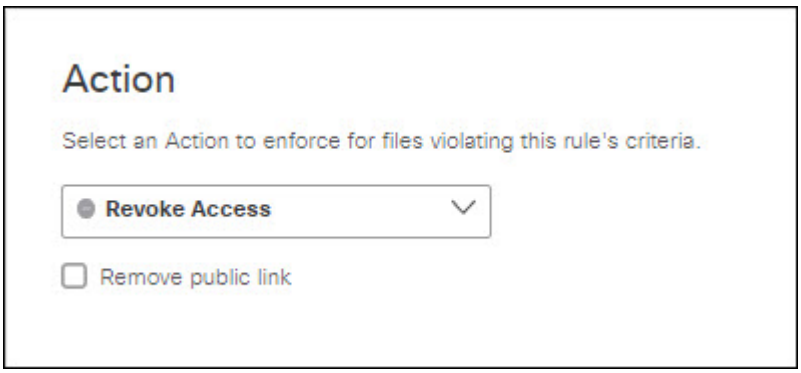
3. If you chose **Revoke Access** for **Action**:
   - If you chose **Google Drive** for the **Platform**, select from the following options:
     - **Remove public link**: Removes any file link that has public exposure.
     - **Remove share exclusively with internal users**: Removes all internal users of files that were shared with few specific internal users.
     - **Remove share with any external user**: Removes all external users. (External users are not part of the organization domain)
     - **Remove specific shares**: Entered email addresses or group email addresses are removed.
     - **Remove org-wide share link**: Removes any share permission with the entire organization.
     - **Remove owner**: Removes the file owner and transfers ownership to a new email address.



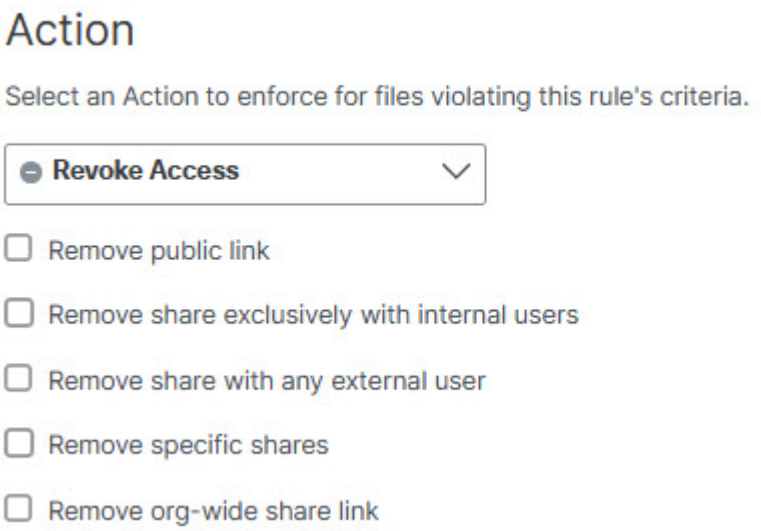
- If you chose **Microsoft 365 Sharepoint Online** or **Microsoft 365 OneDrive** for the **Platform**, select from the following options:
  - **Remove public link**: Removes any file link that has public exposure.
  - **Remove org-wide share link**: Removes any share permission with the entire organization.



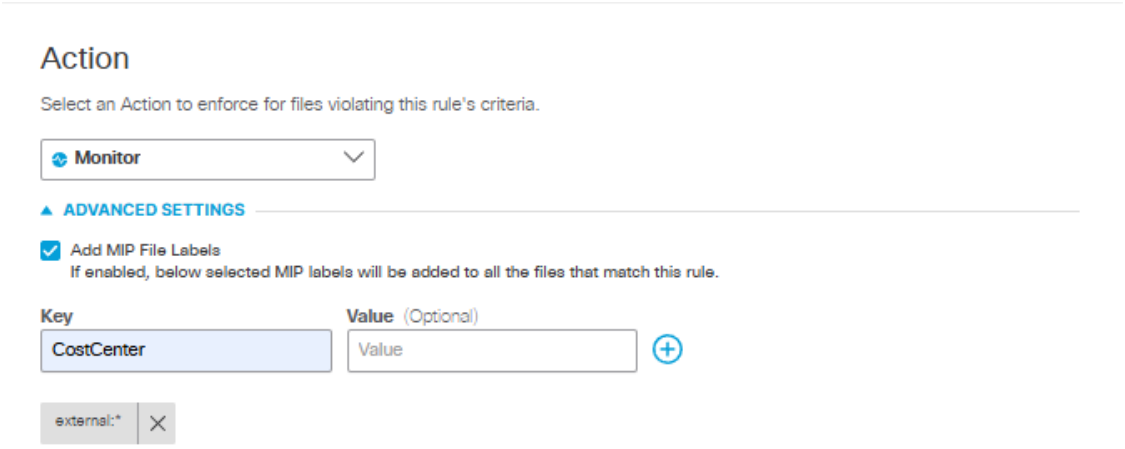
- If you chose **Box** for the platform, select the following option:
  - **Remove public link**: Removes any file link that has public exposure.



- If you chose **Dropbox** for the platform, select from the following options:
  - **Remove public link**: Removes any file link that has public exposure.
  - **Remove share exclusively with internal users**: Removes all internal users of files that were shared with few specific internal users.
  - **Remove share with any external user**: Removes all external users. (External users are not part of the organization domain.)
  - **Remove specific shares**: Entered email addresses or group email addresses are removed.
  - **Remove org-wide share link**: Removes any share permission with the entire organization.

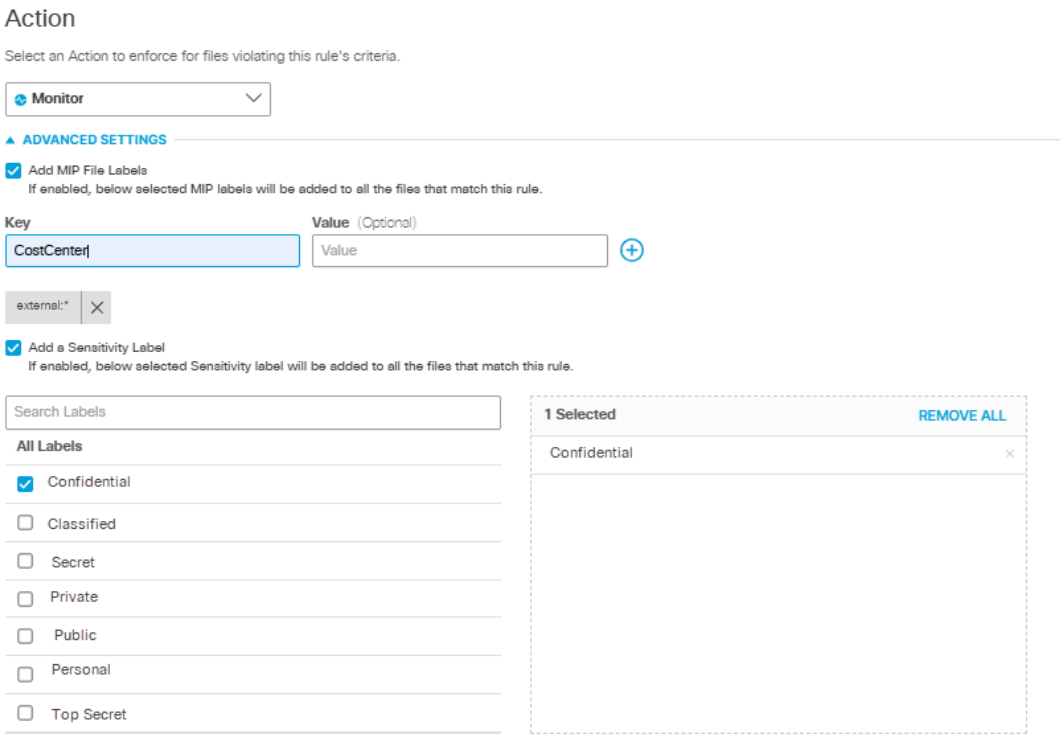


4. If you chose **Box** , **Microsoft Office 365 Sharepoint Online** , or **Microsoft Office 365 OneDrive** for platform, you can choose from **AdvancedSettings** under **Action**.
   - For **Microsoft Office 365 Sharepoint Online** or **Microsoft Office 365 OneDrive**, you can specify MIP file labels that Umbrella will apply to files that match the rule. Enter the **key** (and optionally the **value**) for each label to apply.



- For **Box**:
  - You can specify MIP file labels that Umbrella will apply to files that match the rule. Enter the **key** (and optionally the **value**) for each label to be applied.
  - You can also select from the list of sensitivity labels that have been created for your Box tenant. You may select any one of the labels displayed.

> **Note**
>
> If you create new sensitivity labels for your Box tenant, it may take up to four hours for them to appear in the Secure Access interface. Also be aware that within the Box application, these labels are referred to as classification labels.



Create a DLP SaaS API Rule Step 10 — Enable and Configure Email Notifications

Provides instructions for completing the Create a DLP SaaS API Rule Step 10 – Enable and Configure Email Notifications workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the tenth and final step in the process to add a SaaS API rule to a DLP policy, in which you may optionally select to configure and enable email notifications to send users when data matches the rule.

- For an overview of the entire process, see Add a SaaS API Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP SaaS API Rule Step 9 – Select Action

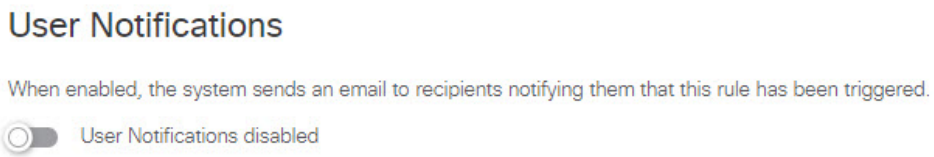
Procedure

1. Under **User Notifications** click the **User Notifications** toggle button to enable and configure an email notification to be sent to any of the following users:
   - The owner of the file associated with a rule violation (for Outlook, this is the sender of the email).

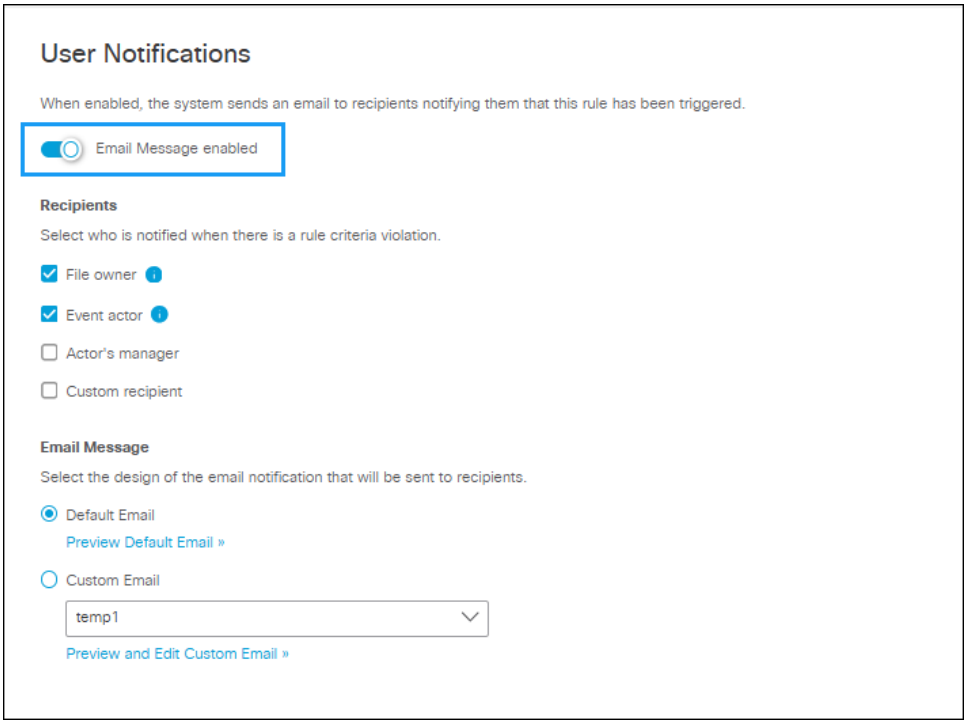
- The user who performs an action that triggers a rule violation (for Outlook, this is the sender of the email).
- The manager of the user who triggered the violation.
- Any email address(es) of your choice.

You can use a default email template provided by the system, or create your own custom template.

> **Note**
>
> If you select the Salesforce platform and the quarantine response action, **User Notifications** will be automatically enabled. Quarantine notifications will be sent to the file owner and the initiator of the event that triggered the quarantine action.



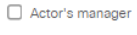
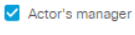
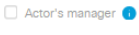
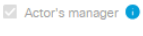
a. Click the **User Notifications** toggle button.



b. Select one or all of the following email recipients:

- **File owner** - The owner of the file associated with the rule violation
- **Event actor** - The user who performs an action that triggers the rule violation
- **Actor's manager**–The manager of the user who triggered the violation.

This feature is available only when email addresses for reporting managers in Active Directory are synchronized for DLP notifications. As a result, the **Actor's manager** checkbox appearance varies depending upon the current configuration settings when viewing a rule:

Checkbox Appearance	Meaning
	Reporting manager's email sync is enabled, but notifications to the actor's manager are not selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.
	Reporting manager's email sync is enabled, and notifications to the actor's manager are selected for this rule. Email notifications for violations will be sent to the event actor's manager.
	Reporting manager's email sync is disabled, and notifications to the actor's manager are not selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.
	Reporting manager's email sync is disabled, and notifications to the actor's manager are selected for this rule. Email notifications for rule violations will not be sent to the event actor's manager.

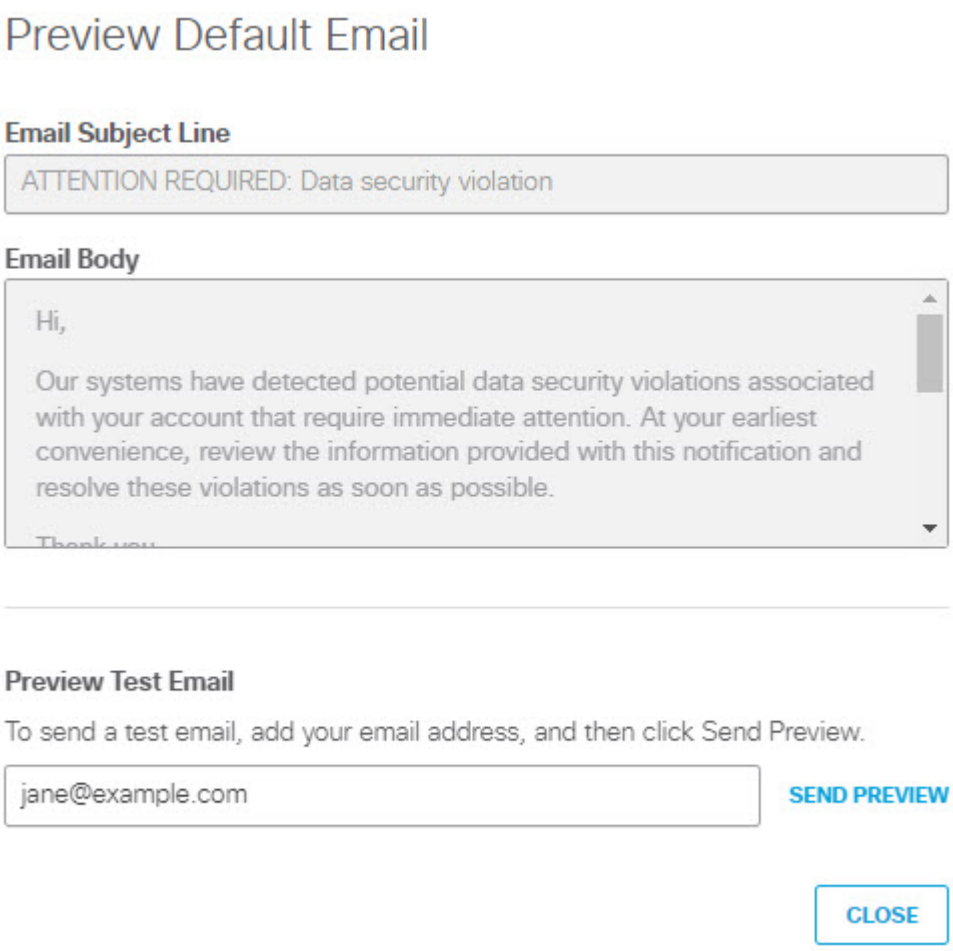
- **Custom recipient**–Allows you to specify email addresses of your choice. To use this option, select the **Custom recipient** checkbox, and enter one or more valid email addresses in the text box. These addresses will receive notifications whenever this rule is violated.

> **Note**
>
> If you have selected a Salesforce Commerce tenant, **Custom recipient** is the only option available.

c. Choose the email template:

To Use the Default Email Template:

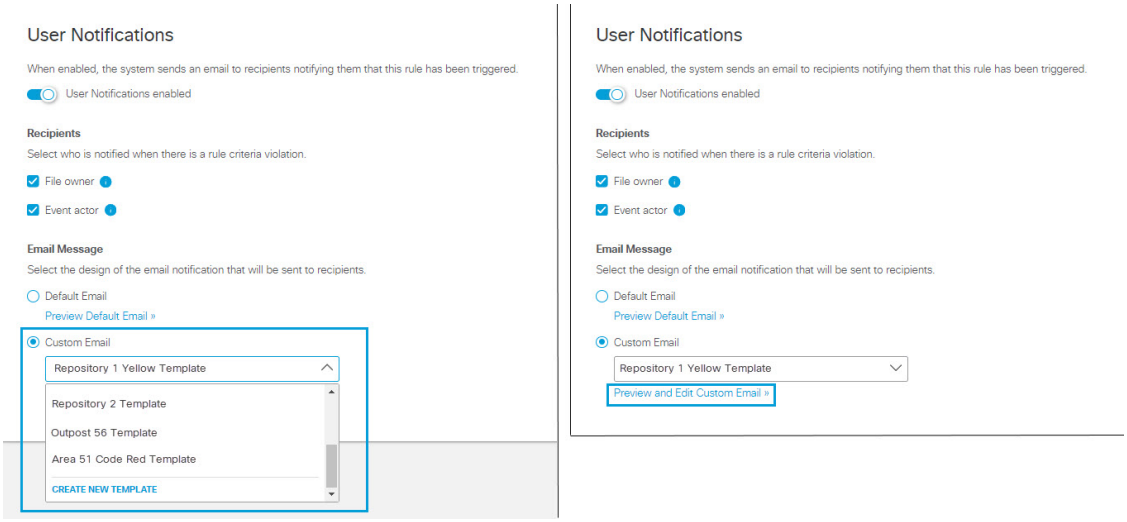
1. Click **Default Email**.
2. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.



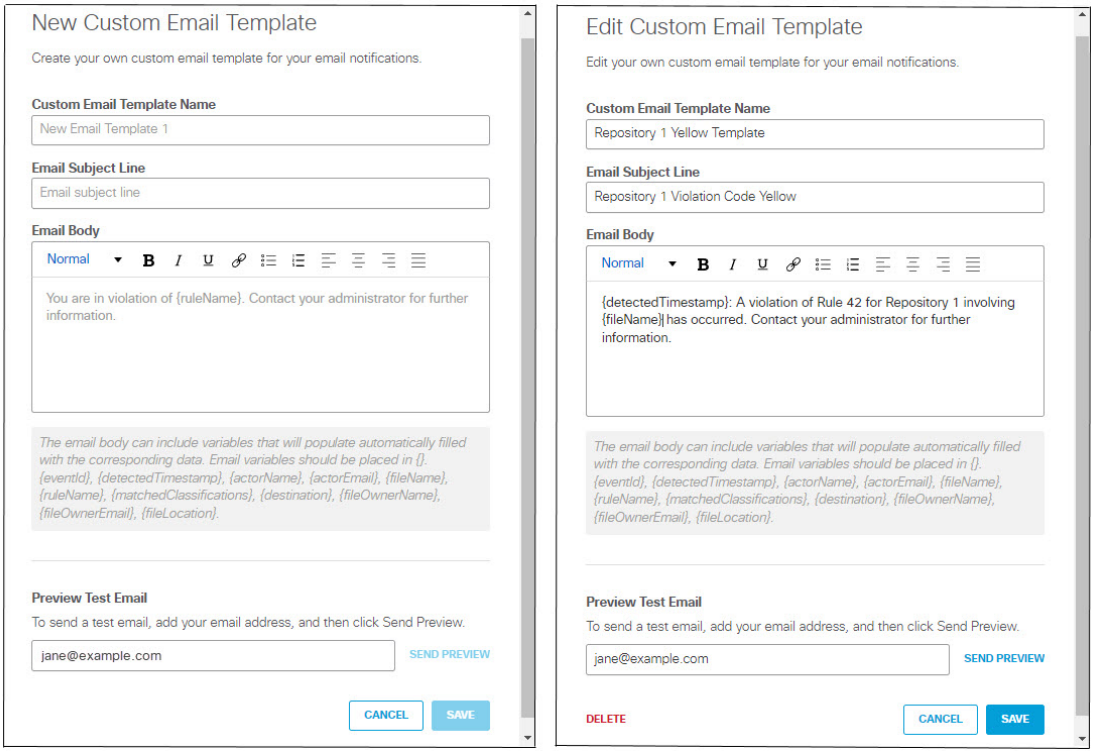
3. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
4. Click **CLOSE** to return to the Data Loss Prevention Policy page.

To Use a Custom Email Template:

1. Click **Custom Email**.
2. From the drop-down list, select an existing custom template, or choose **CREATE CUSTOM TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.



3. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:



The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

a. Enter a unique **Custom Email Template Name**.

b. Enter an **Email Subject Line**.

c. Enter the text of the email in the **Email Body** text box.

The email text can include the following variables, which you must enclose in braces (**{}**):

- **{eventId}** - The unique identifier the system generates for the policy violation event.

- **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileName}** - Name of the data file that triggered the violation.
- **{ruleName}** - Name of the rule that was triggered.
- **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
- **{destination}** - The application or platform type of the tenant associated with the violation. (E.g., Google Drive or One Drive; see Manage Tenant Controls.)
- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

d. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

e. Click **SAVE** to return to return to the Data Loss Prevention Policy page.

2. Click **Save**. All fields must have options selected to save.

Add an AI Guardrails Rule to the Data Loss Prevention Policy

Provides instructions for completing the Add an AI Guardrails Rule to the Data Loss Prevention Policy workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule.

AI guardrails rules operate within the data loss prevention policy to monitor prompts or response content exchanged with AI application, including uploaded files. The rules define what types of data to monitor, and whether content should be blocked or only monitored.

An AI Guardrails rule must have at least one of the following two criteria defined:

- Data Classifications – Include files that match data classification of your own making or a built-in data classification provided by Secure Access.
- File Labels – Include files that have specific file label names configured in the value of the files' document properties, or include files that have no file labels configured. (You cannot select both of these criteria in a single rule.) Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.
- File Size – Include files that meet custom size criteria.
- File Type – Include files that have a specific file type.

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Create the AI Guardrails rule and establish general settings.
2. Select **Data Classifications** to apply to the rule.
3. Make **Files Control** selections for the rule
4. Select **Identities** to apply to the rule.
5. Select **Destinations** to include for the rule.
6. Select an **Action** to be performed when data matches the rule.
7. For any destination you can enable and configure pop-up notifications for violations.
8. For any destination you can enable and configure an email notification to be sent to users when a violation occurs.

Create a DLP AI Guardrails Rule Step 1 — Establish General Settings

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 1 – Establish General Settings workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule.

This is the first step in the process to add a AI Guardrails rule to a DLP policy, in which you create the rule and establish its basic characteristics.

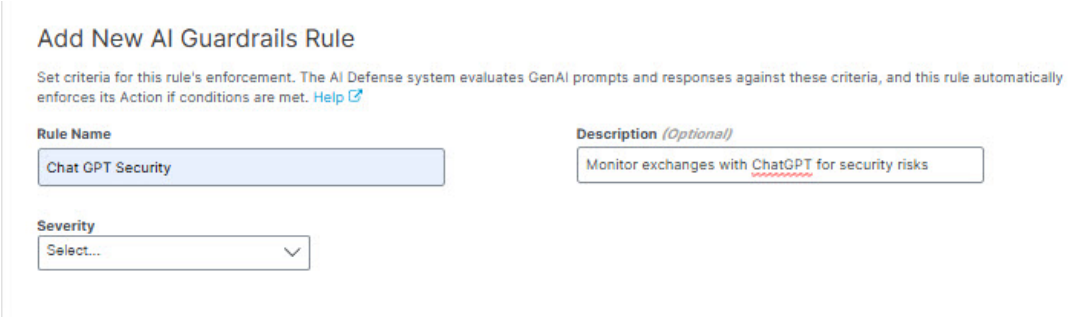
- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the next step in the process, see Create a DLP AI Guardrails Rule Step 2 – Select Data Classifications

Before you begin

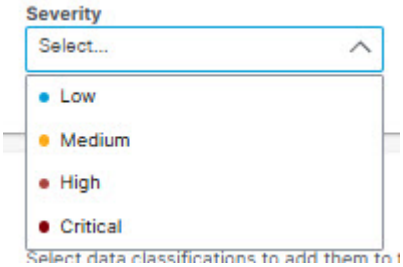
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, click **Add Rule**, and choose **AI Guardrails Rule**.
2. Under **Add New AI Guardrails Rule**, give your rule a meaningful name and description.



3. Choose a severity for your rule based on the risk involved or importance within the ruleset.



Create a DLP AI Guardrails Rule Step 2 — Select Data Classifications

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 2 – Select Data Classifications workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule.

This is the second step in the process to add a AI Guardrails rule to a DLP policy, in which you select the data classifications to apply to the rule.

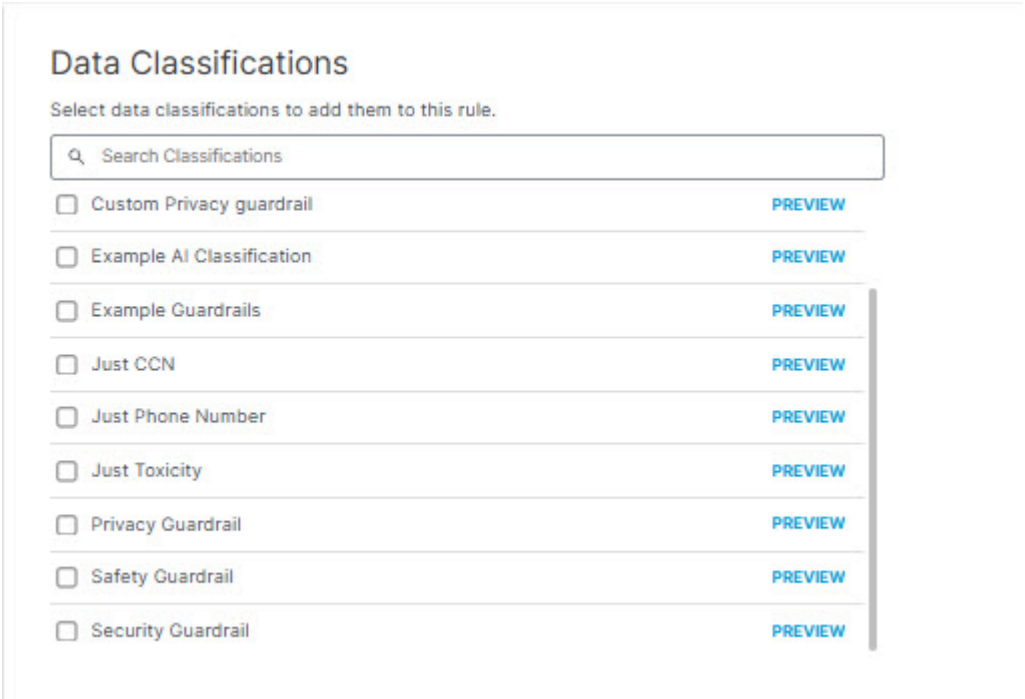
- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Real Time Rule Step 1 – Establish General Settings
- For the next step in the process, see Create a DLP AI Guardrails Rule Step 3 – Select Files Controls

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

In the **Data Classifications** section select AI guardrails classifications to apply this rule. You can choose a guardrails classification of your own making, or a built-in guardrails classification provided by Secure Access. (For more information, see Manage AI Guardrails Data Classifications.) Hover over **PREVIEW** to view data identifiers associated with each AI guardrails classification.



Create a DLP AI Guardrails Rule Step 3 — Select Files Controls

Configure file controls in an AI Guardrails rule using file labels, file size, and file type filters to enhance data protection.

This is the third step in the process to add a AI Guardrails rule to a DLP policy, in which you select the files controls to apply to the rule.

- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP AI Guardrails Rule Step 2 – Select Data Classifications
- For the next step in the process, see Create a DLP AI Guardrails Rule Step 4 – Select Identities

In the **Files Control** area, choose the file filters to apply to this rule. You can apply filters for:

- Specific File Labels, or files that have no file labels associated with them. (You cannot select both of these criteria in a single rule.)
- File Size
- File Type

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI

guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.

- Full Admin user role. For more information, see Manage Accounts.

Procedure

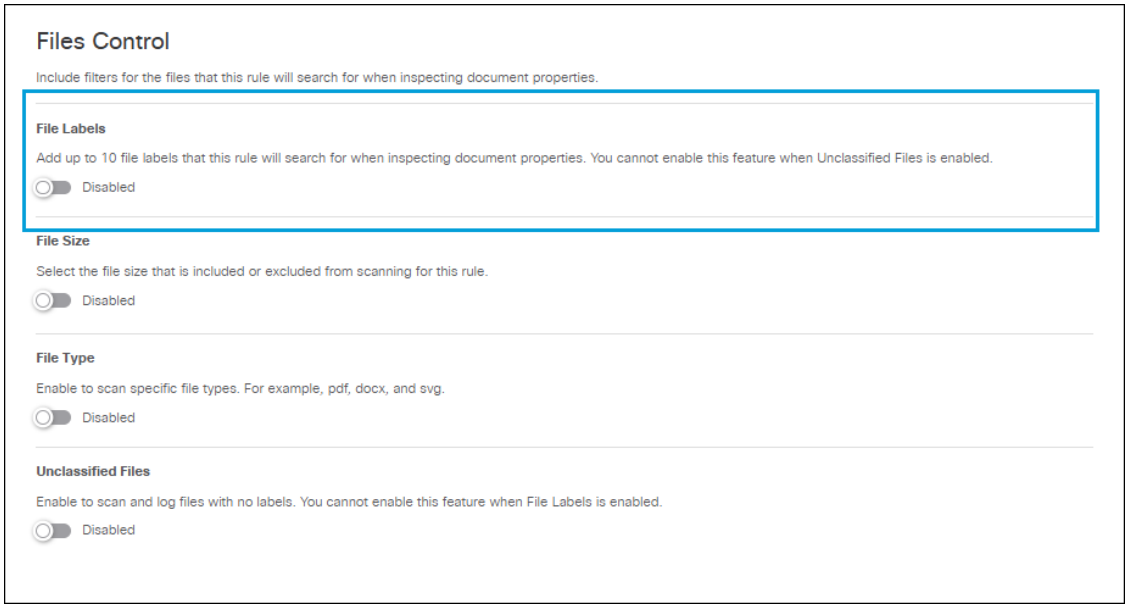
1. Choose **File Labels**.

   Add up to 10 case-sensitive file label names to apply to this rule. The rule searches for configured file label names in the files' document properties. This includes Microsoft Office Sensitivity Labels and Adobe PDF Document Properties. For Microsoft Office Document Properties (or Titus labels) , this includes only the Label Value field in the custom document properties.

   Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

   Note

   You can configure an AI Guardrails rule with data classifications, file labels, or both. When a rule is configured with both, then a DLP event is raised when any of the selected data classifications and when any of the configured file labels are detected in an inspected file.



   Note

   Secure Access currently supports detection of Microsoft sensitivity labels in the file properties' values of the inspected file for Microsoft Word, Excel, PowerPoint, and PDF files. Ensure you configure the rule with the name of the sensitivity labels, not the Display Names.

2. Choose **File Size** criteria for the rule.

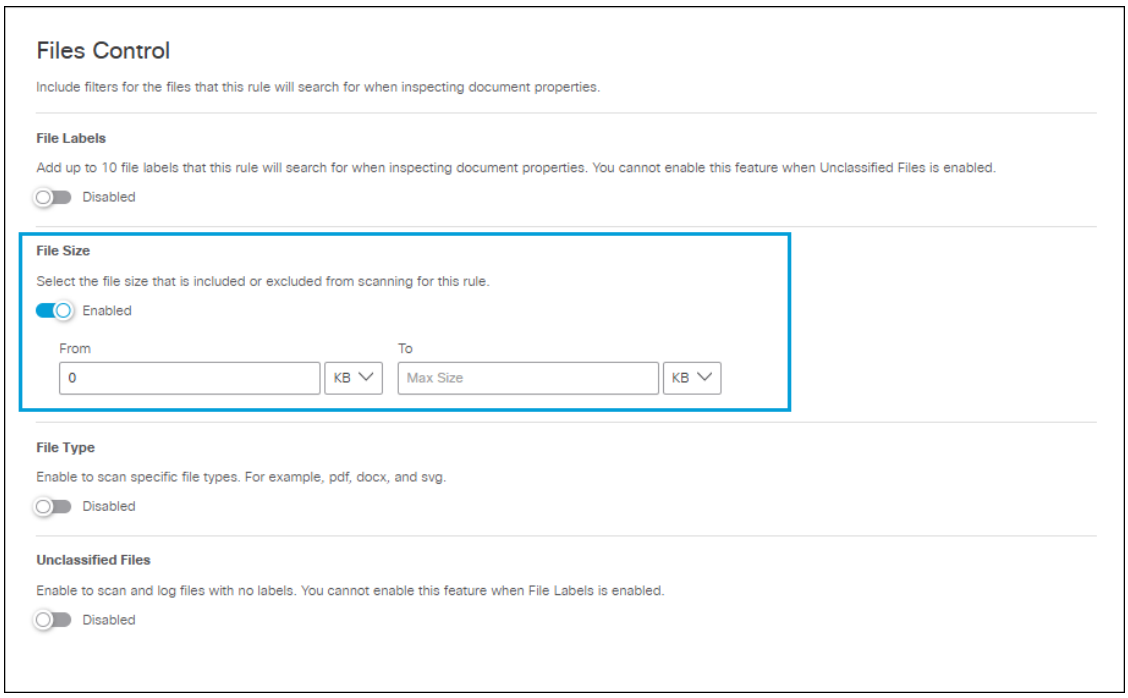
   The **File Size** area has two use cases:

- In a rule that specifies a custom file size but no other criteria, DLP applies the rule action to files that match the file size criteria, regardless of content. (This may be useful in situations where you want to exclude certain low-risk files below a certain size from inspection, so as not to waste processing time on insignificant events.)
- In a rule that specifies a custom file size along with other criteria such as Data Classification, the DLP applies the rule action to files that match the other criteria within the file size specified up to the first 50 MB of plain text. (Secure Access does not scan file content beyond the first 50 MB regardless of the file size specified here.)

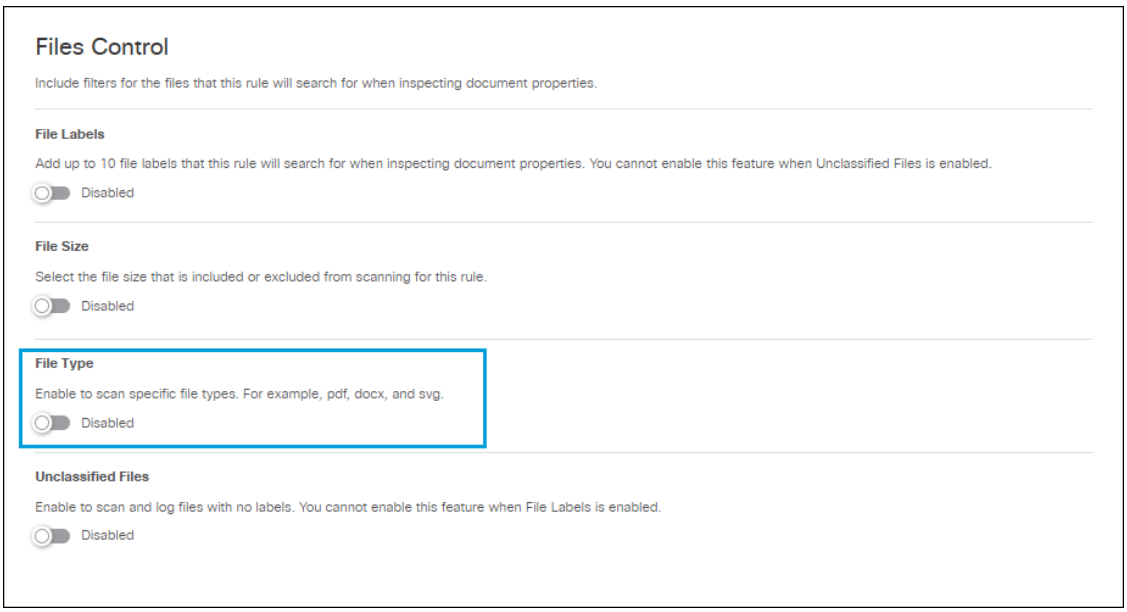
In the **File Size** area choose from two options:

- To scan up to the first 50 MB of plain text of all files that meet other criteria defined by this rule, enable the **File Size** toggle and do not select custom sizes. (A rule that uses this option must also specify Data Classifications.)
- To specify the minimum and maximum size limits the system will scan for files that meet other inclusion criteria defined by this rule, if there are any, enable the **File Size** toggle and select custom size values. If the file size exceeds the first 50 MB of the file, Secure Access scans only up to the first 50 MB of plain text in the file. (I.e., if you specify a minimum file size greater than 50 MB, Secure Access will not scan for other criteria specified in the rule.)

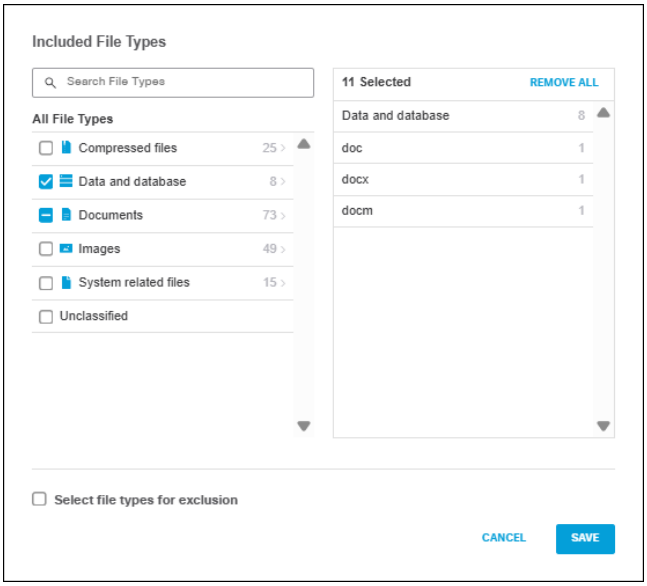
  You can choose to apply the rule action only to files that are greater than a minimum size you specify, or to files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB.



3. In the **File Type** area, configure the rule to include specific file types or to exclude specific file types.
   a) Click the toggle to enable file type filtering.

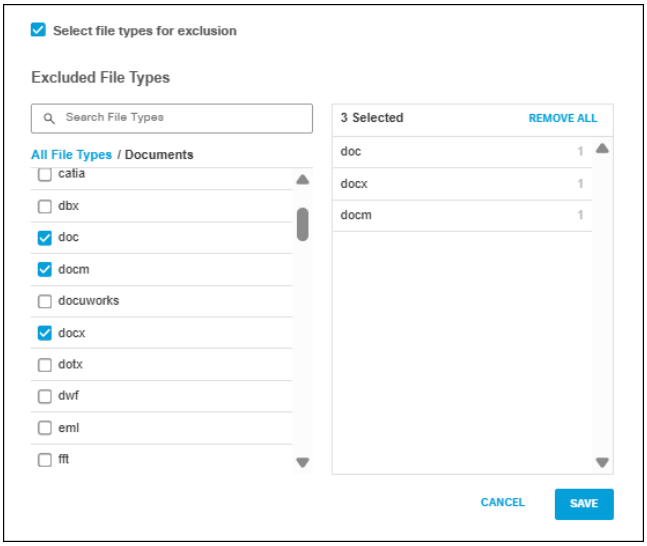


b) To include file types, use the search box to search for file types or browse within the lists for file types. Check the boxes for the file types to include individually or by group. Selected file types appear on the right.



c) To exclude file types, check **Select the file type for exclusion** check box.

In **Excluded File Types** section, use the search box to search for file types or browse within the lists for file types. Check the boxes for file types to exclude individually or by group. Selected file types appear on the right.

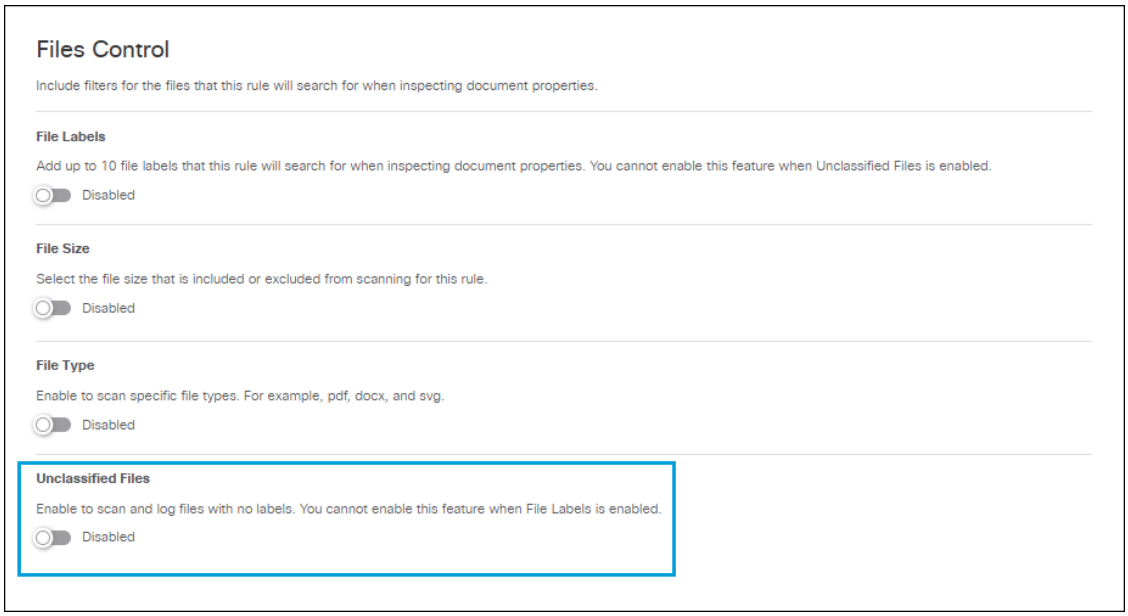


4. In the **Unclassified Files** area, click the toggle to include that have no labels associated with them.

   This includes Microsoft Office Sensitivity Labels and Adobe PDF Document Properties. For Microsoft Office Document Properties (or Titus labels) , this includes only the Label Value field in the custom document properties.

   Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.

> **Note**
>
> You can configure an AI Guardrails rule with data classifications, absence of file labels, or both. When a rule is configured with both, then a DLP event is raised when any of the selected data classifications are detected in an inspected file that has no file labels.



Create a DLP AI Guardrails Rule Step 4 — Select Identities

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 4 – Select Identities workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule.

This is the fourth step in the process to add a AI Guardrails rule to a DLP policy, in which you select the identities to apply to the rule.

- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP AI Guardrails Rule Step 3 – Select Files Controls
- For the next step in the process, see Create a DLP Real Time Rule Step 5 – Select Destinations

Before you begin

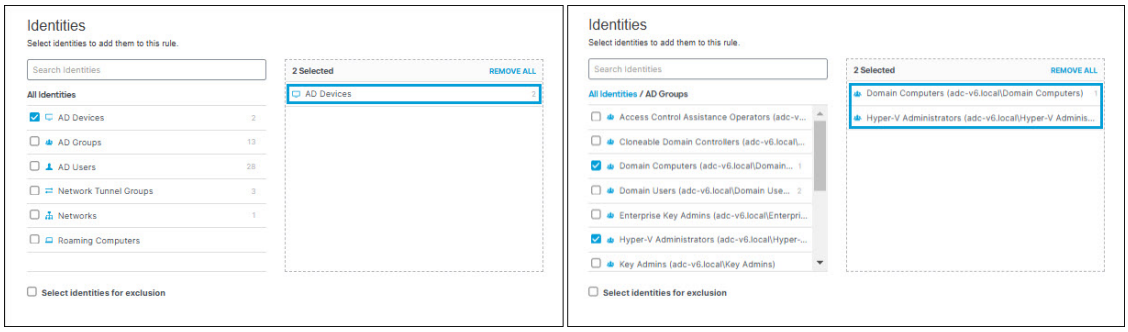
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

In the **Identities** section, select **Identities** to apply to this rule.

- Select entire identity categories to include, or expand categories to select individual identities. Search for user name or by group name. Selected identities will appear in the box on the right.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.



- Select **Select identities for exclusion** to exclude selected identities. Similarly to selecting identities for inclusion, you can select entire identity categories to exclude, or expand categories to select individual identities. Search for user name or by group name. Selected identities will appear in the box on the right.

> **Note**
>
> When an identity is selected for both inclusion and exclusion in a rule, it will automatically be excluded. Excluded identities always override included identities. Similarly, if an identity category is included on both an inclusion list and an exclusion list, the identity category will be excluded.

Create a DLP AI Guardrails Rule Step 5 — Select Destinations

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 5 – Select Destinations workflow in Cisco Secure Access. HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule.

This is the fifth step in the process to add a AI Guardrails rule to a DLP policy, in which you select the destinations to apply to the rule.

- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP AI Guardrails Rule Step 4 – Select Identities
- For the next step in the process, see Create a DLP Real Time Rule Step 6 – Select the Rule Action

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

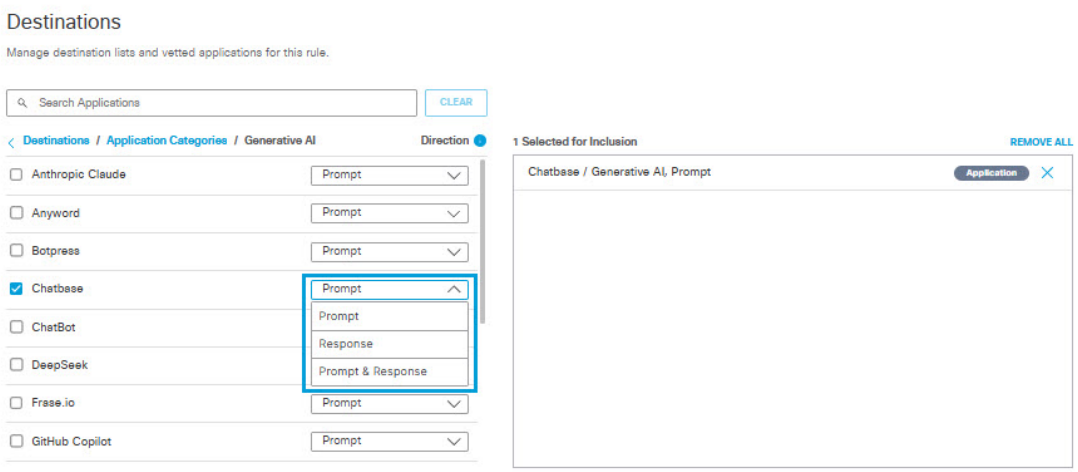
Procedure

Under **Destinations**, expand the destination categories and and check the boxes for the applications you want to add to the rule. You can search for an application by entering at least three consecutive letters from the application name in the search box.

> **Note**
>
> It is not possible to search for an application with fewer than three letters in its name–for example, "QQ" or "YY." These applications must be manually selected from the hierarchy under their respective categories, or wildcarded in search–for example, "QQ*". This behavior is by design.

For each application (except Microsoft Copilot), you can scan one of three traffic options: **Prompt** (from your system to the AI application), **Response** (from the AI application to your system), or **Prompt & Response**.

> **Tip**
>
> At this time, **Microsoft Copilot** is only supported in the Prompt direction.



Create a DLP AI Guardrails Rule Step 6 — Select the Rule Action

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 6 – Select the Rule Action workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the sixth step in the process to add a AI Guardrails rule to a DLP policy, in which you select an **Action** to be performed when data matches the rule.

- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Real Time Rule Step 5 – Select Destinations
- For the next step in the process, see Create a DLP AI Guardrails Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

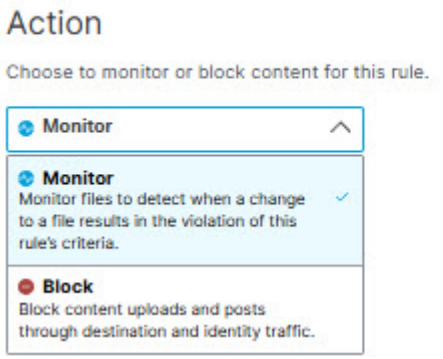
Under **Action**, from the drop-down list, choose **Monitor** or **Block**.

- **Monitor**–Monitor file uploads and data submitted in web forms.

The rule will search for content that matches supported workflows (See Supported Applications) and policy-configured destinations and identities.

- **Block**–Block file uploads and data submitted in web forms.

  The rule will search for content that matches supported workflows (See Supported Applications) and the policy-configured destinations and identities. When content matches these workflows, the rule blocks the content.



Create a DLP AI Guardrails Rule Step 7 — Enable and Configure Pop-Up Notifications for Violations

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the seventh step in the process to add a real time rule to a DLP policy, in which you may optionally select to display a pop-up notification for endpoints when data matches the rule.

- For an overview of the entire process, seeAdd a AI Guardrails Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP AI Guardrails Rule Step 6 – Select Rule Action.
- For the next step in the process, see Create a DLP AI Guardrails Rule Step 8 – Enable and Configure Email Notifications for Violations.

Before you begin

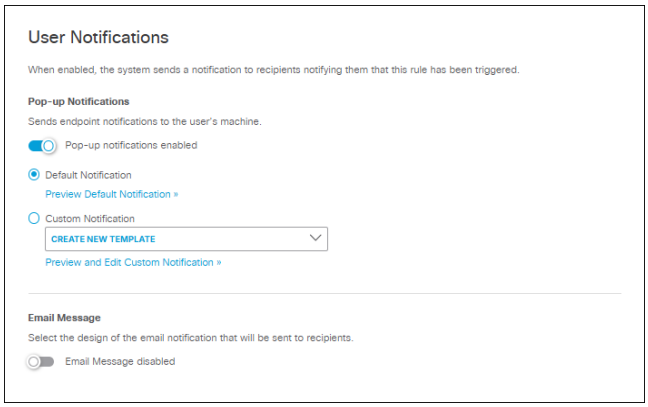
- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

Procedure

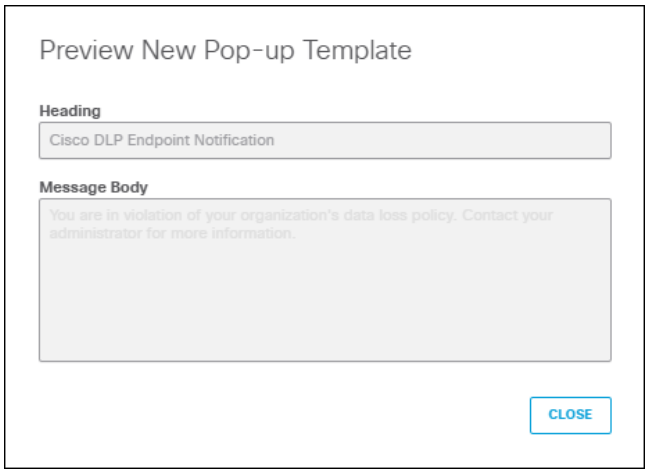
1. Under **User Notifications**, you can enable the **Pop up Notifications** option to display pop-up notifications of violations to the end user.

> **Note**
>
> If you have no real time rules with at least one endpoint channel selected under Destinations, the **Pop up Notification** option remains disabled.

> **Note**
>
> If you choose **Allow override with business justification** under **Action** **Advanced Settings**, the **Pop up Notification** option is automatically enabled and cannot be disabled.

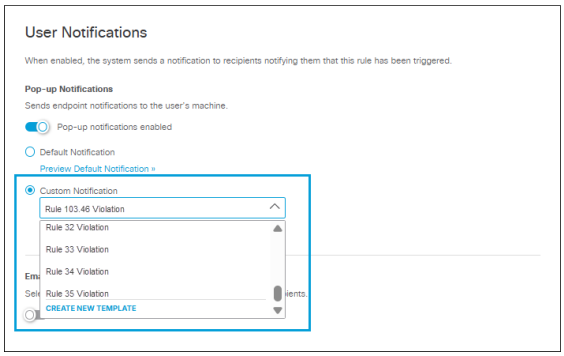


2. Define the message to appear in the pop up dialog when files match a rule.
   - **To use the default Pop Up Template:**
     a. Click **Default Notification**.
     b. To preview the content of the pop up text, click on **Preview Default Notification**. You can review the text, but you cannot change it.

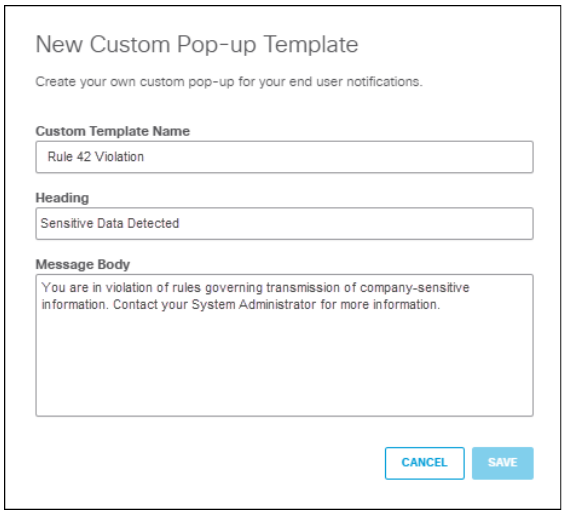


     c. Click **CLOSE** to close the preview.
   - **To use a Custom Pop Up Template:**
     a. Click **Custom Notification**.

b. From the drop-down list, select an existing custom template, or choose **CREATE NEW TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Notification** to review and change the template.



c. When you choose to create or edit a custom template for pop up text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Pop-up Template** dialog includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the heading text for the pop up in the **Heading** text box.
3. Enter the message text for the pop up in the **Message Body** text box.
4. Click **SAVE** to complete the changes.

Create a DLP AI Guardrails Rule Step 8 — Enable and Configure Email Notifications for Violations

Provides instructions for completing the Create a DLP AI Guardrails Rule Step 8 – Enable and Configure Email Notifications for Violations workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

This is the seventh and final step in the process to add a AI Guardrails rule to a DLP policy, in which you may optionally select to configure and enable email notifications to send users when data matches the rule.

- For an overview of the entire process, see Add a AI Guardrails Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP AI Guardrails Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations

Before you begin

- HTTPS Inspection must be enabled either on the default Access policy, or at least one access policy rule where the same identity is configured in an AI guardrails rule. For example, if the resource "Network A" is configured for an AI guardrails rule, it must also be configured for an access policy rule where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Security Profiles.
- Full Admin user role. For more information, see Manage Accounts.

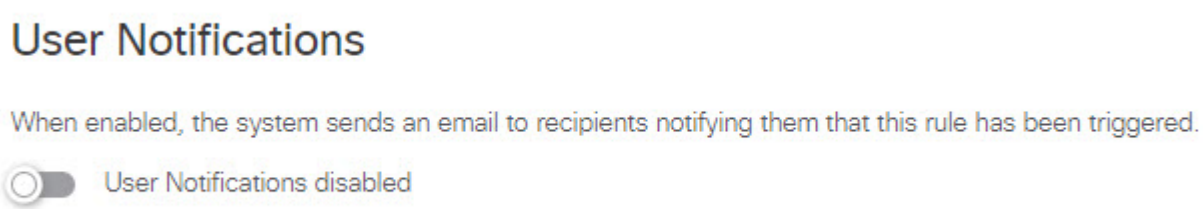
Procedure

1. Under **User Notifications** you can enable and configure an email notification to be sent to a user who performs an action that triggers a violation of the rule. You can use a default email template provided by the system, or create your own custom template.

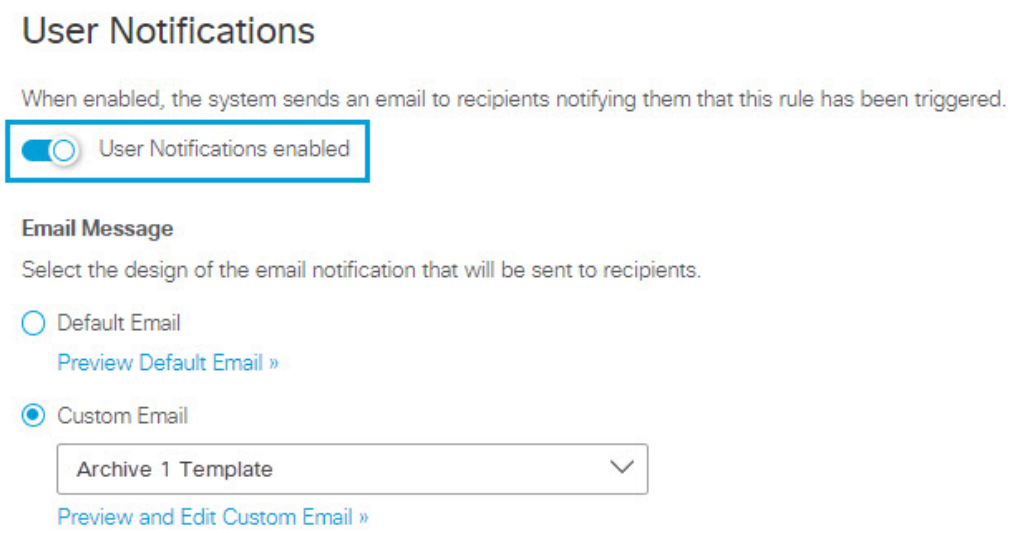
   a. **Note**

   The system gets the "send to" address for the email from UPN field in the authenticated active directory. Some identity configurations may not be able to provide the end user's email address, in which case the system will be unable to send the email. These cases include:

   - The user uses network or tunnel identities, in which case the user's IP address will be available to the system, but not the email address.
   - The user did not authenticate through active directory, so the system has no information about the user.
   - The user's email address is not stored in the UPN field in the authenticated active directory.



1. Enable user notifications.

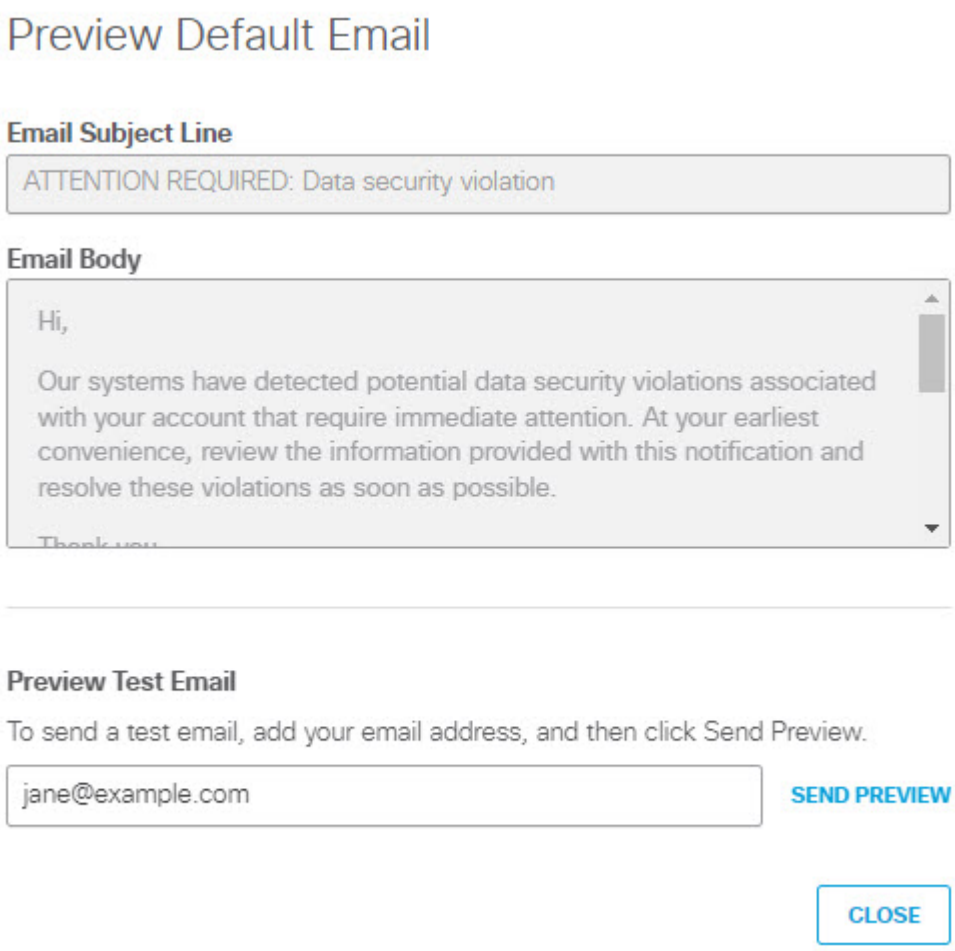


2. Choose the email template:

   To Use the Default Email Template:

   a. Click **Default Email**.

   b. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.



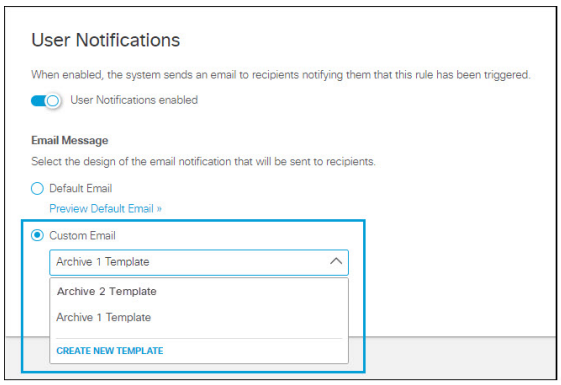
c. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

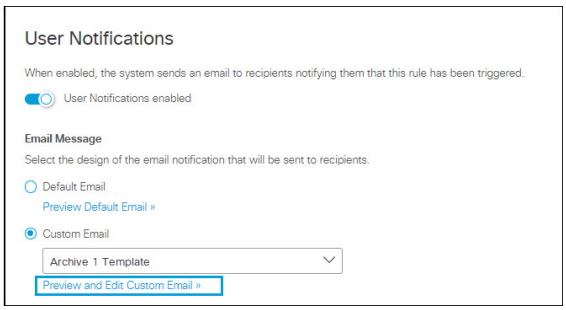
d. Click **CLOSE** to return to the Data Loss Prevention Policy page.

To Use a Custom Email Template:

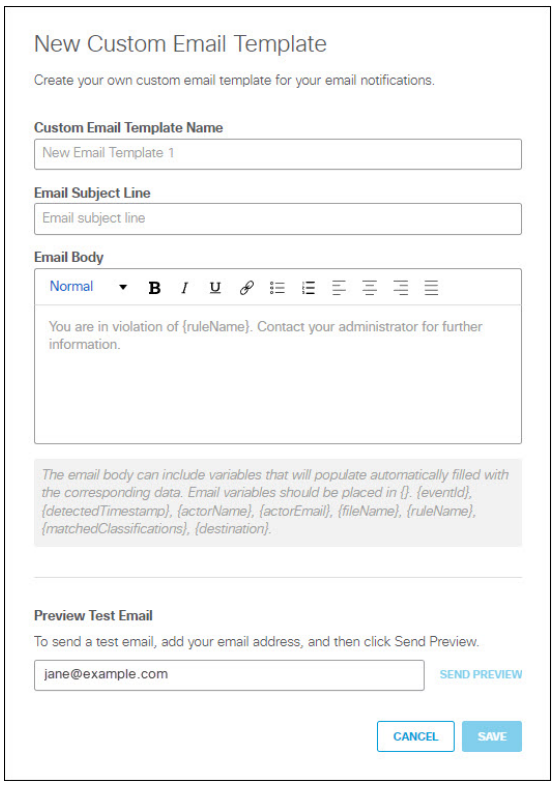
a. Click **Custom Email**.

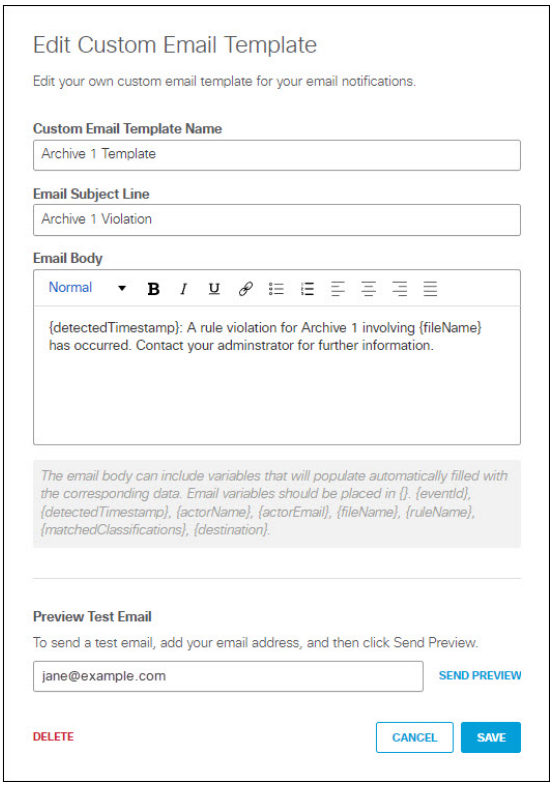
b. From the drop down menu, select an existing custom template, or choose **CREATE CUSTOM TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.





c. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:





The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Email Template Name**.
2. Enter an **Email Subject Line**.
3. Enter the text of the email in the **Email Body** text box.

   The email text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.

- **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- **{actorName}** - Name of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{actorEmail}** - Email address of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{fileName}** - Name of the data file that triggered the violation.
- **{ruleName}** - Name of the rule that was triggered.
- **{matchedClassifications}** - The guardrails classifications associated with the violation. (See Manage AI Guardrails Data Classifications.)
- **{destination}** - URL or IP address of the intended destination for the monitored request.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

(Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

Click **SAVE** to return to return to the Data Loss Prevention Policy page.

2. Click **Save**.

> **Note**
>
> All fields must have options selected to save.

Integrate Email Threat Defense with Secure Access DLP

Provides instructions for completing the Integrate Email Threat Defense with Secure Access DLP workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

Before using Email DLP rules to monitor or block cloud native email processed by Cisco's Secure Email Threat Defense, you must first integrate Email Threat Defense with Secure Access DLP, following the procedure below.

Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.

- You must install Cisco Secure Email Threat Defense.

Procedure

1. Generate an API key with the "DLP as A Service" scope. For detailed instructions, see Add Secure Access API Keys.
2. Use the generated credentials to enable DLP in Secure Email Threat Defense. For details see Enable DLP in the Email Threat Defense documentation.

You may now create Email DLP rules as described in Add an Email Rule to the Data Loss Prevention Policy.

Add an Email Rule to the Data Loss Prevention Policy

Provides instructions for completing the Add an Email Rule to the Data Loss Prevention Policy workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

The Secure Access Email DLP capability integrates with Cisco's Email Threat Defense, which provides cloud native email security. The system inspects the content of outgoing emails (`.eml` files) and assesses the content against the criteria of email DLP rules. You configure an Email rule to set the criteria as to what triggers enforcement. If a data violation is detected, the rule's action is immediately enforced. If Secure Access detects a violation, the offending content is listed in the Data Loss Prevention Report.

An Email must have at least one of the following four criteria defined:

- Data Classifications – Include email files that match data classification of your own making or a built-in data classification provided by Secure Access.
- File Labels – Include emails that have attacments with specific file label names configured in the value of the files' document properties, or include emails with attachment files that have no file labels configured. (You cannot select both of these criteria in a single rule.) Secure Access scans for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.
- File Size– Include email files meeting size requirements that you specify.
- File Type– Include or exclude files of types that you specify.

Email DLP rules scan only outgoing messages processed by Cisco's Email Threat Defense. Violations can be triggered by material found in the email subject, message body, or attachments; a single email message may trigger multiple violations: one for the message subject and body, and one for each attachment.

Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

1. Create a DLP Email Rule Step 1 – Establish General Settings
2. Select **Data Classifications** to apply to the rule
3. Make **Files Control** selections for the rule
4. Select **Senders** whose emails would be included or excluded from scanning this rule

5. Select **Receivers** whose emails would be included or excluded from scanning this rule
6. Select an **Action** to be performed when data matches the rule
7. For any destination you can enable and configure pop-up notifications for violations.
8. For any destination you can enable and configure an email notification to be sent to users when a violation occurs

Create a DLP Email Rule Step 1 — Establish General Settings

Provides instructions for completing the Create a DLP Email Rule Step 1 – Establish General Settings workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the first step in the process to add an email rule to a DLP policy, in which you create the rule and establish its basic characteristics.

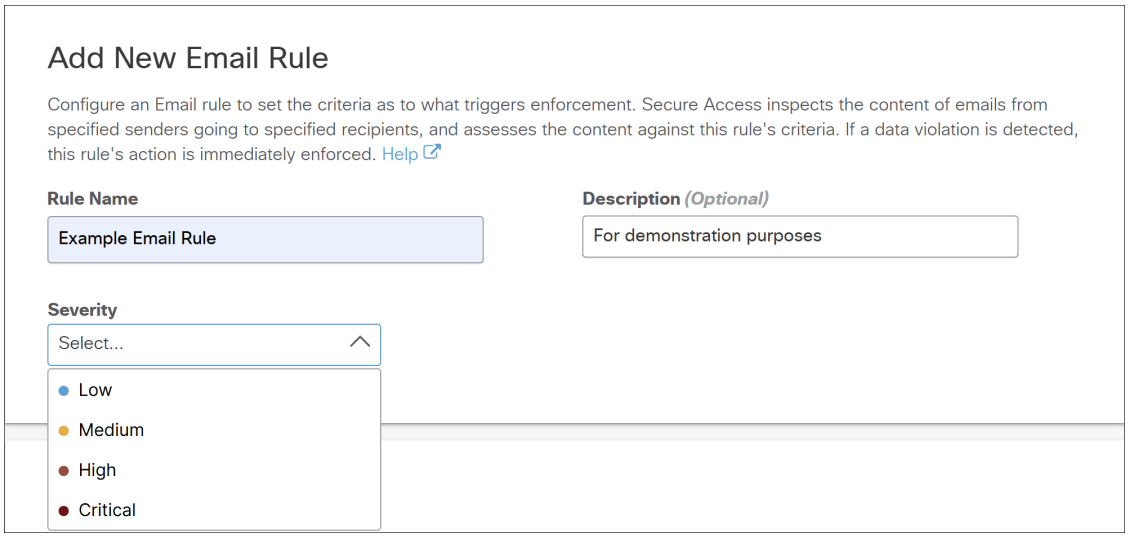
- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the next step in the process, see Create a DLP Email Rule Step 2 – Select Data Classifications

Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, click **Add Rule**, and choose **Email DLP Rule**.
2. In the **Add New Email Rule** area, enter a meaningful **Rule Name** and **Description**. Choose a **Severity** value from the drop-down based on the risk involved or importance within the ruleset. (Assigning severity values can help later on when you need to filter events in the Data Loss Prevention report.)



Create a DLP Email Rule Step 2 — Select Data Classifications

Provides instructions for completing the Create a DLP Email Rule Step 2 – Select Data Classifications workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the second step in the process to add an email rule to a DLP policy, in which you select the data classifications to apply to the rule.

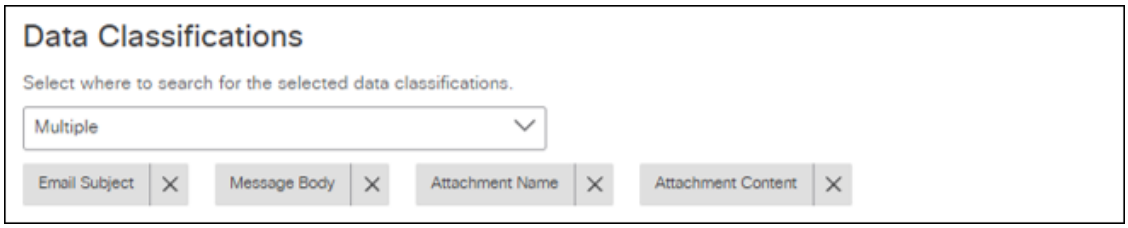
- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 1 – Establish General Settings
- For the next step in the process, see Create a DLP Email Rule Step 3 – Select Files Controls

Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

1. Under **Data Classifications** select where in scanned files you would like this rule to search for the data classifications that you choose:



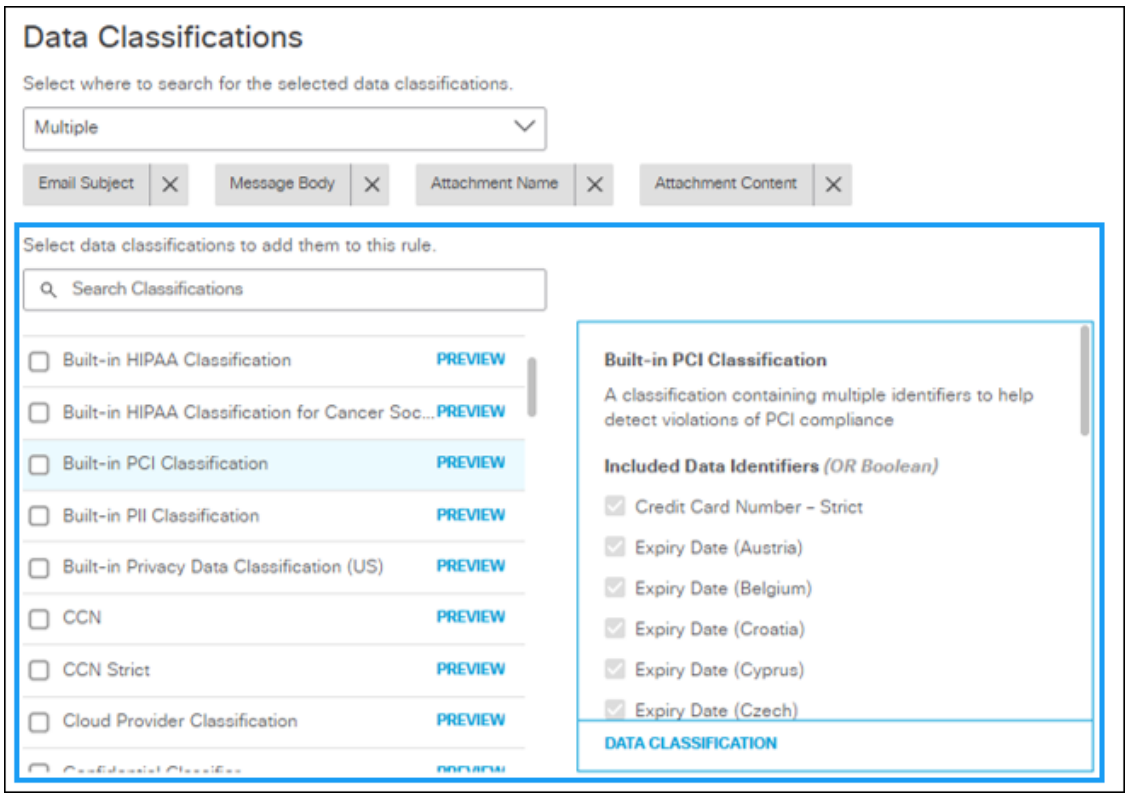
   Email Subject–Scans the subject line of the email.

   Message Body–Scans the message body of the email.

   Attachment Name–Scans the file names of attachments to the email

   Attachment Content–Scans the contents of attachments to the email.

2. Select **Data Classifications** to apply this rule; you can choose data classifications of your own making or built-in data classifications provided by Secure Access. (See Manage Data Classifications and Built-In Data Classifications.) Hover over **PREVIEW** to view data identifiers associated with each data classification.



Create a DLP Email Rule Step 3 — Select Files Controls

Provides instructions for completing the Create a DLP Email Rule Step 3 – Select Files Controls workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the third step in the process to add an email rule to a DLP policy, in which you select the files controls to apply to the rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 2 – Select Data Classifications
- For the next step in the process, see Create a DLP Email Rule Step 4 – Select the Senders

In the **Files Control** area, choose the file filters to apply to this rule. You can apply filters for:

- MIP and Titus Labels, or files that have no file labels associated with them. (You cannot select both of these criteria in a single rule.)
- File Size
- File Type

Before you begin

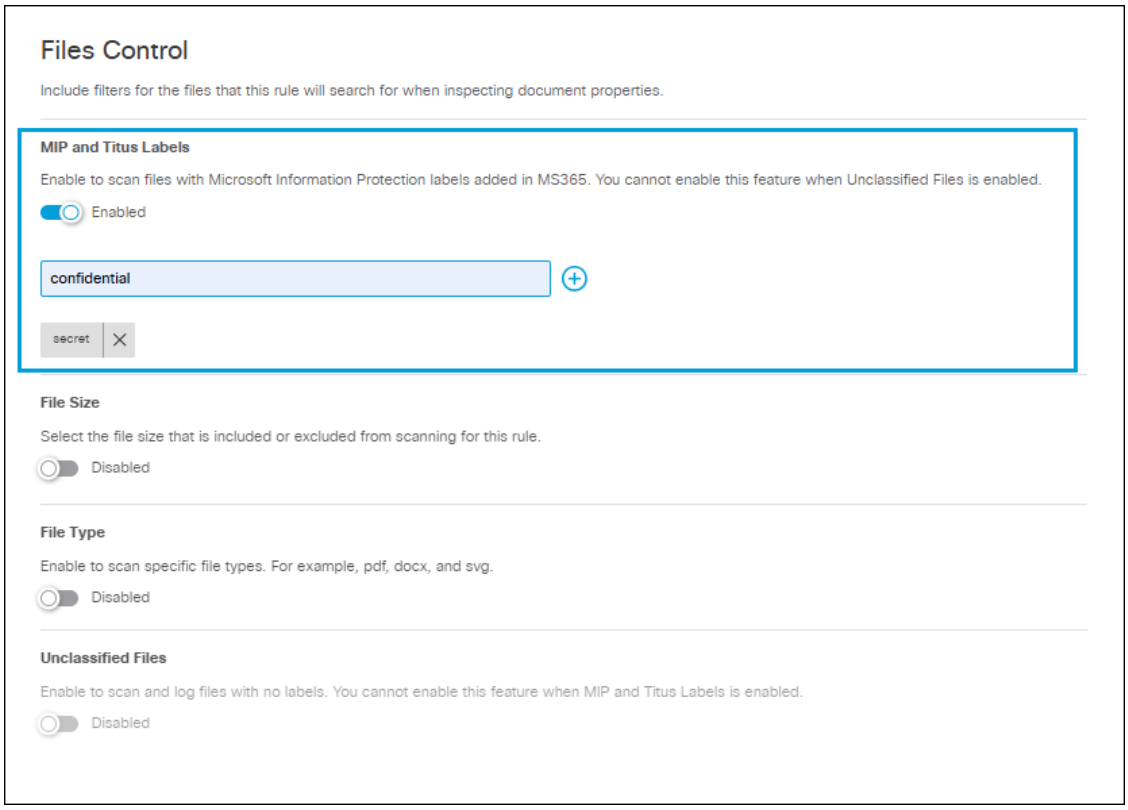
- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

1. You can enable **MIP and Titus Labels** and add up to 10 case-sensitive file label names to apply to the rule.

   The rule will search for any of the configured label names in document properties of email attachments. This includes Microsoft Office Document Properties and Adobe PDF Document Properties. For Microsoft Office Document Properties , this includes only the Label Value field in the custom document properties.

   Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.



2. Choose **File Size** criteria.

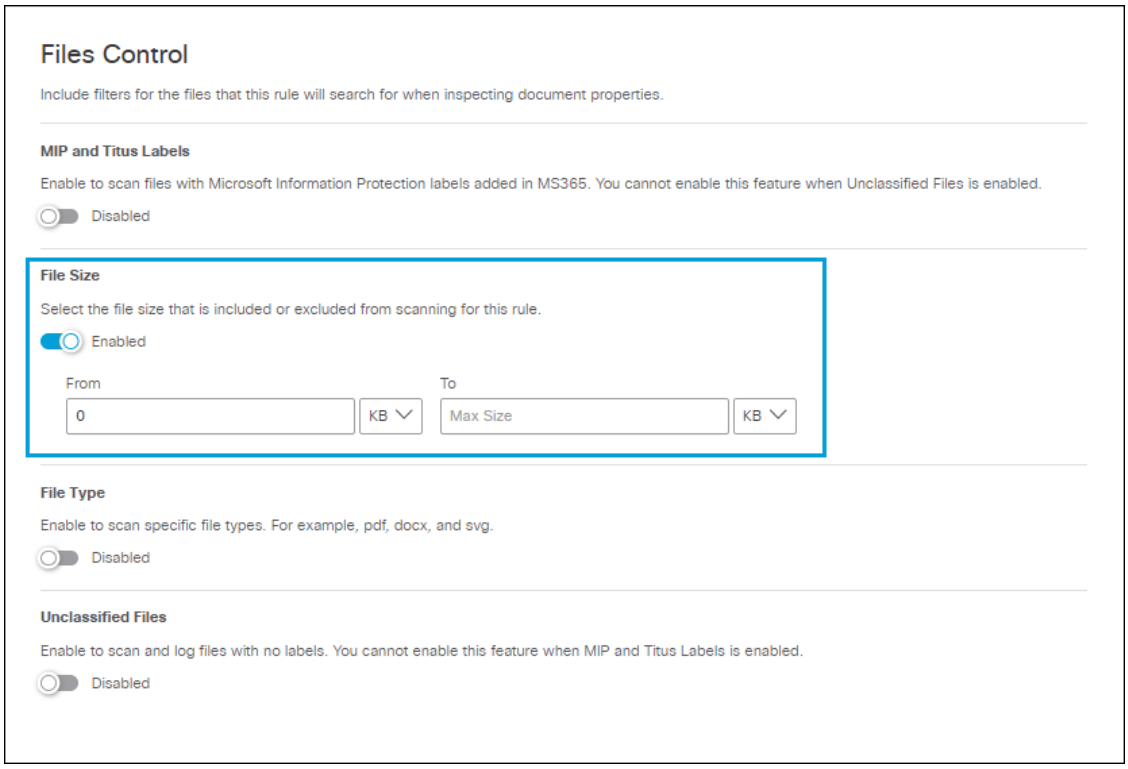
   The **File Size** area has two use cases:

   - In a rule with only custom file size criteria, DLP applies the rule action to files that match the file size criteria, regardless of content. (This may be useful in situations where you want to exclude certain low-risk files below a certain size from inspection, so as not to waste processing time on insignificant events.)
   - In a rule that specifies a custom file size along with other criteria such as Data Classification, the DLP applies the rule action to files that match the other criteria within the file size specified up to the first 50 MB of plain text. (Secure Access does not scan file content beyond the first 50 MB regardless of the file size specified here.)

   In the **File Size** area choose from two options:

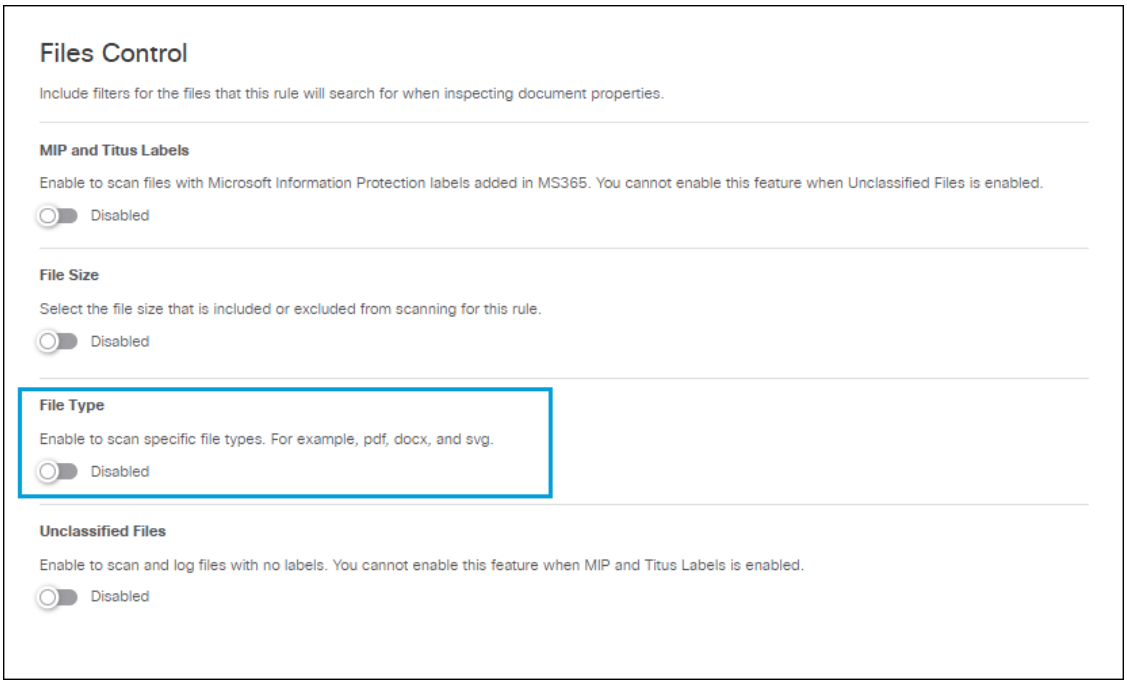
   - To scan up to the first 50 MB of plain text of all files that meet other criteria defined by this rule, enable the **File Size** toggle and do not select custom sizes. (A rule that uses this option must also specify Data Classifications.)
   - To specify the minimum and maximum size limits the system will scan for files that meet other inclusion criteria defined by this rule, if there are any, enable the **File Size** toggle and select custom size values. If the file size exceeds the first 50 MB of the file, Secure Access scans only up to the first 50 MB of plain text in the file. (I.e., if you specify a minimum file size greater than 50 MB, Secure Access will not scan for other criteria specified in the rule.)

You can choose to apply the rule action only to files that are greater than a minimum size you specify, or to files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB.

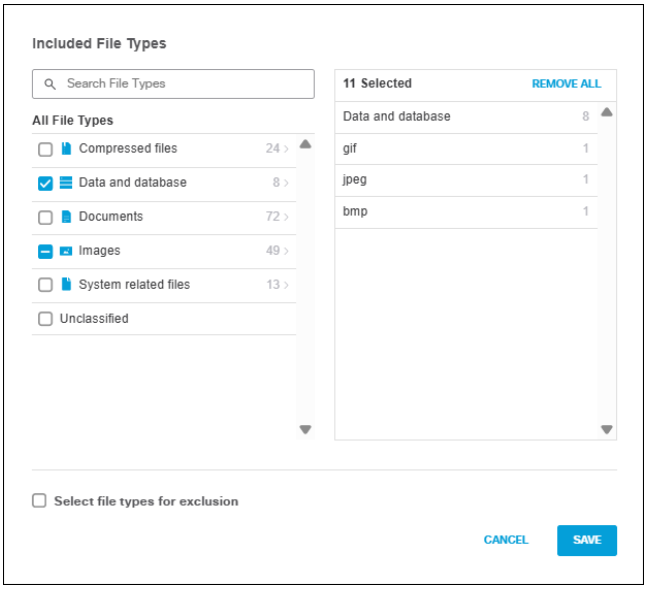


3. You can select the **File Type** filter, which causes DLP to apply the action to emails that match the other rule criteria as well as having file attachments that match file type inclusions or exclusions that you select.

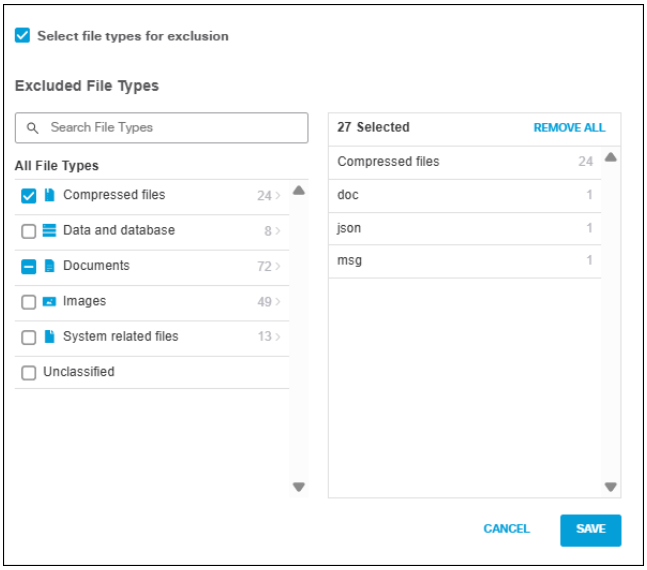
   a. Click the toggle to enable file type filtering.



   b. To include file types, use the search box to search for file types or browse within the the lists for file types. Check the boxes for the file types to include--individually or by group. Selected file types appear on the right.



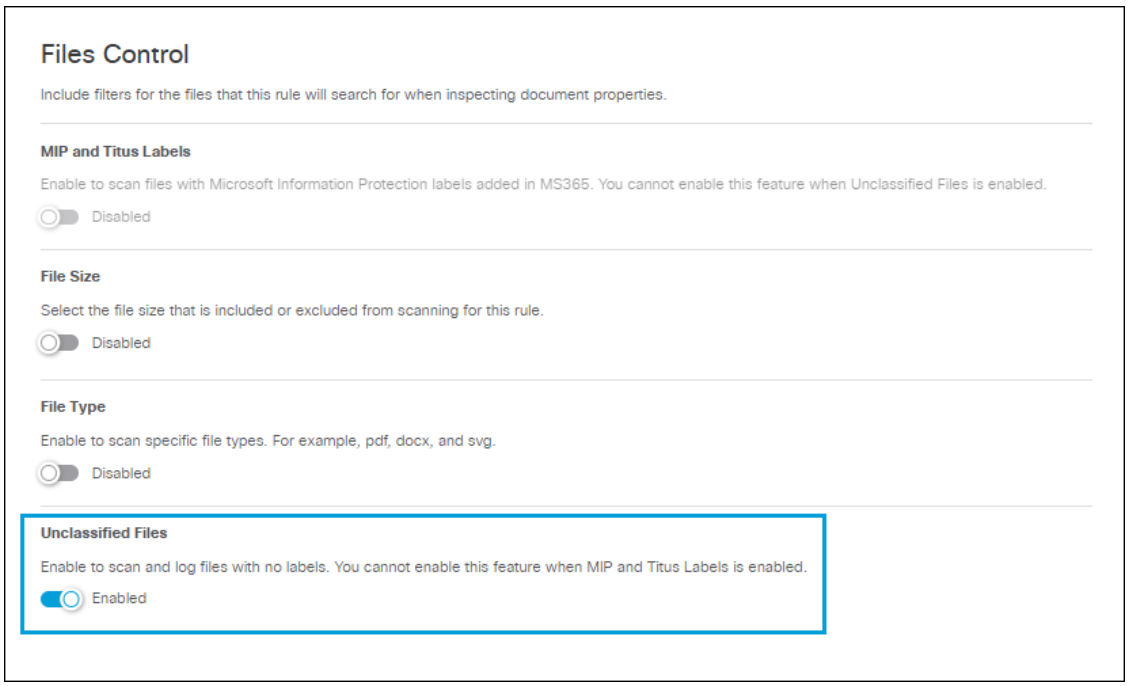
c. To exclude file types, check **Select file types for exclusion**. Under **Excluded File Types**, use the search box to search for file types or browse within the lists for file types. Check the boxes for file types to exclude--individually or by group. Selected file types appear on the right.



4. In the **Unclassified Files** area, click the toggle to include that have no labels associated with them.

This includes Microsoft Office Sensitivity Labels and Adobe PDF Document Properties. For Microsoft Office Document Properties (or Titus labels) , this includes only the Label Value field in the custom document properties.

Secure Access can scan for file labels on the following file types: .doc, .pdf, .rtf, .xls, .ppt, .odp, .ods, .odt, .pptx, .xlsx, .docx, and .eml.



Create a DLP Email Rule Step 4 — Select the Senders

Provides instructions for completing the Create a DLP Email Rule Step 4 – Select the Senders workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the fourth step in the process to add an email rule to a DLP policy, in which you select the senders whose emails would be included or excluded from scanning this rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 3 – Select Files Controls
- For the next step in the process, see Create a DLP Email Rule Step 4 – Select the Recipients

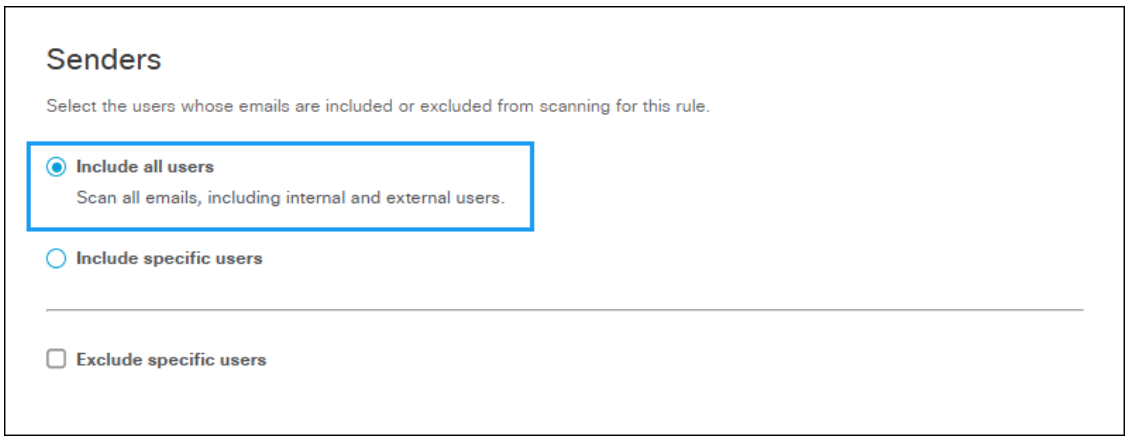
Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

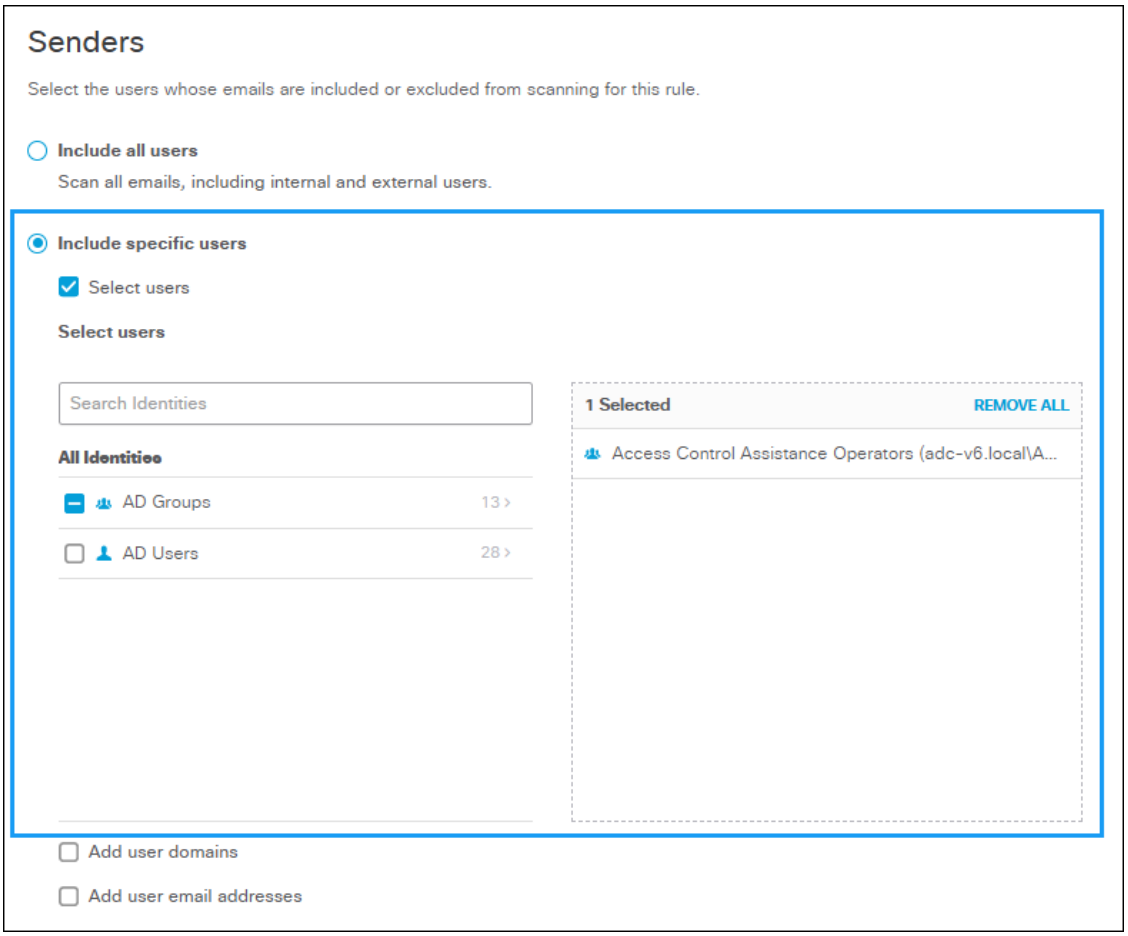
In the **Senders** area, choose to include all users, include specific users, or exclude specific users.

- To scan all emails from all senders, select **Include all users**.



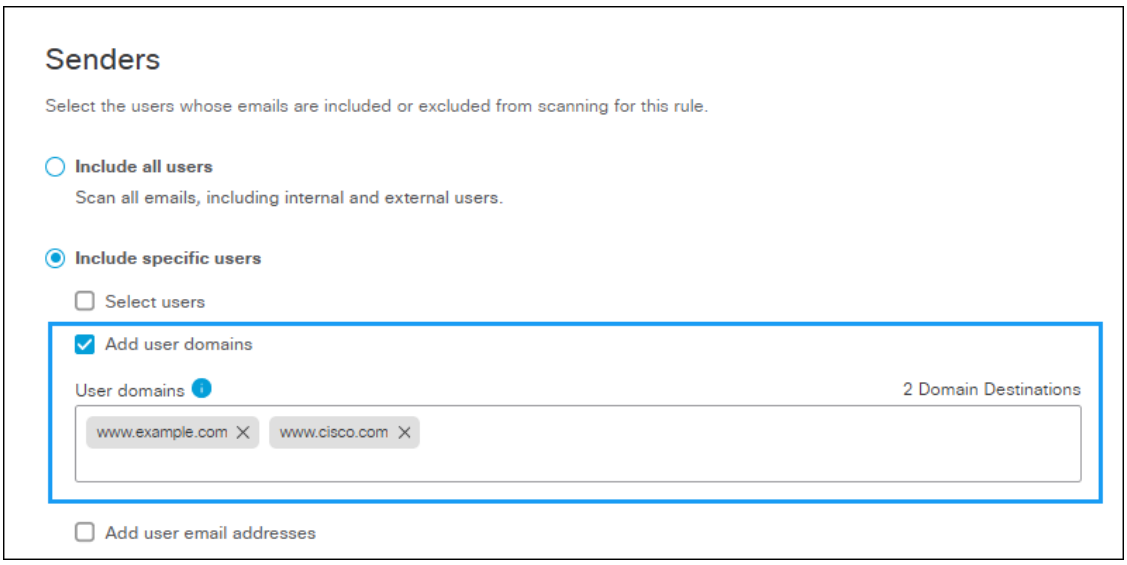
- To scan emails from specific users, select **Include specific users**. You can choose one or more of the following options:
  - **Select users**

    Use the search box to search for Identities within your environment, or browse within the the lists for AD Groups and AD users. Check the boxes for the users to include--individually or by group. Selected users appear on the right.



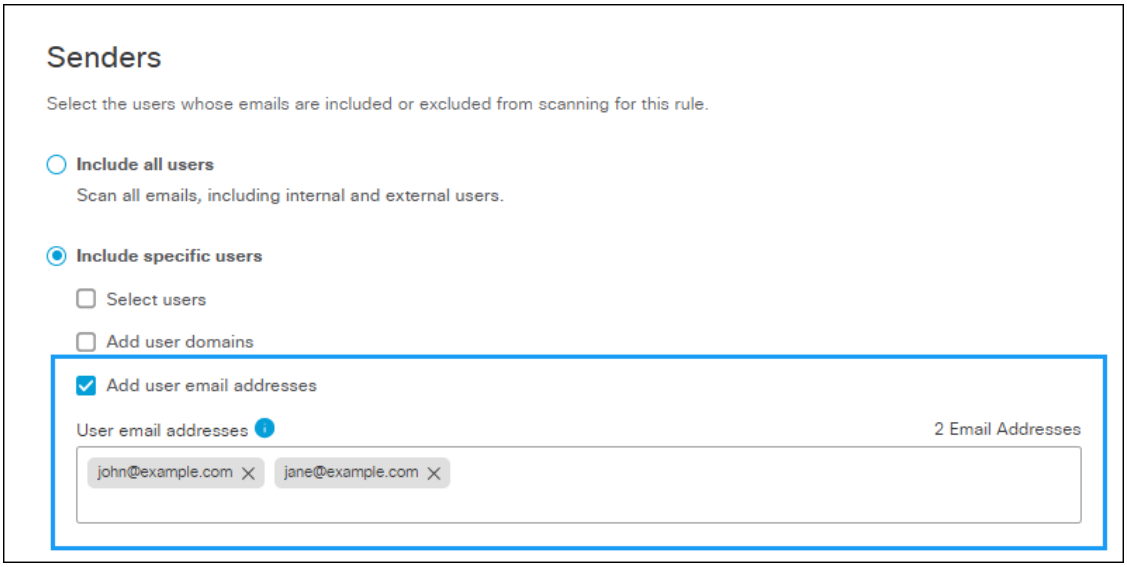
  - **Add user domains**

    Enter one or more unique web site addresses from which email may be sent.



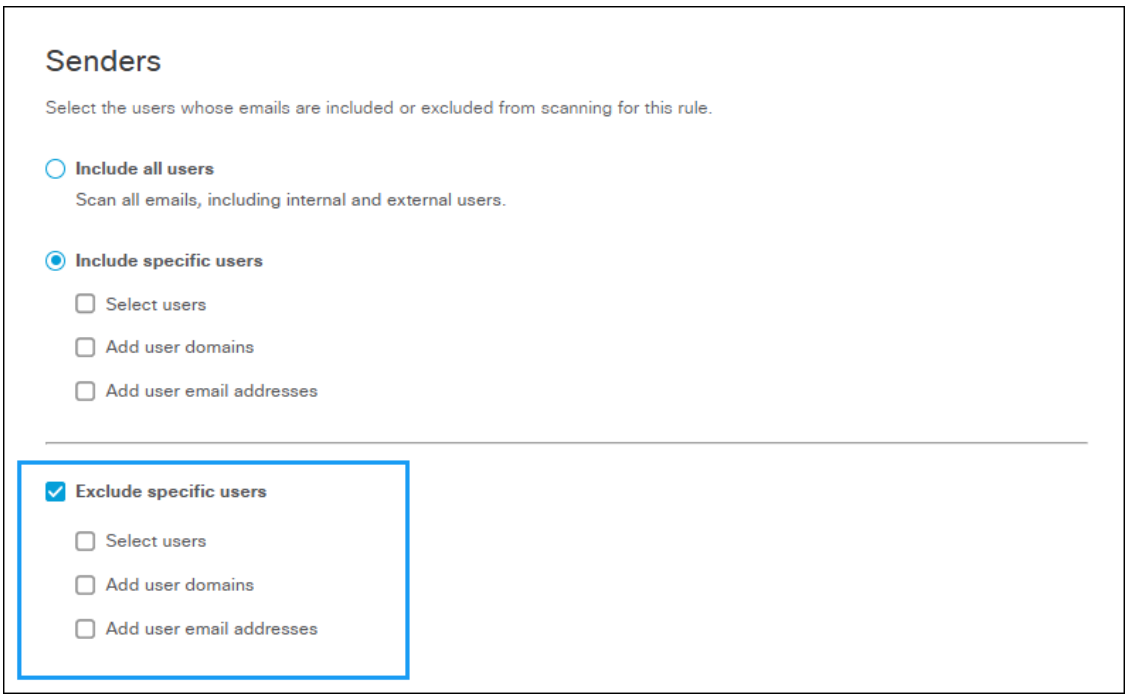
- **Add user email addresses**

  Enter one or more valid email addresses from which email may be sent.



- You can choose to exclude selected users from the lists of senders you have included:

  a. Select **Exclude specific users**.



b. Choose one or more of the following options to select users to exclude:

- **Select users**
- **Add user domains**
- **Add user email addresses**

These options present the same mechanisms for selecting users as described for including users, above.

Create a DLP Email Rule Step 5 — Select the Recipients

Provides instructions for completing the Create a DLP Email Rule Step 5 – Select the Recipients workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the fifth step in the process to add an email rule to a DLP policy, in which you select the recipients whose emails would be included or excluded from scanning this rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 4 – Select the Senders
- For the next step in the process, see Create a DLP Email Rule Step 6 – Select the Rule Action

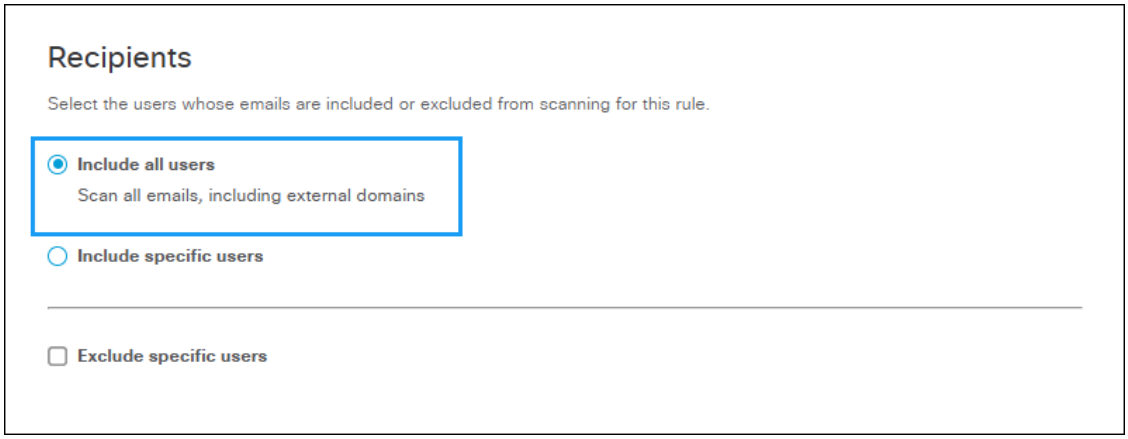
Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

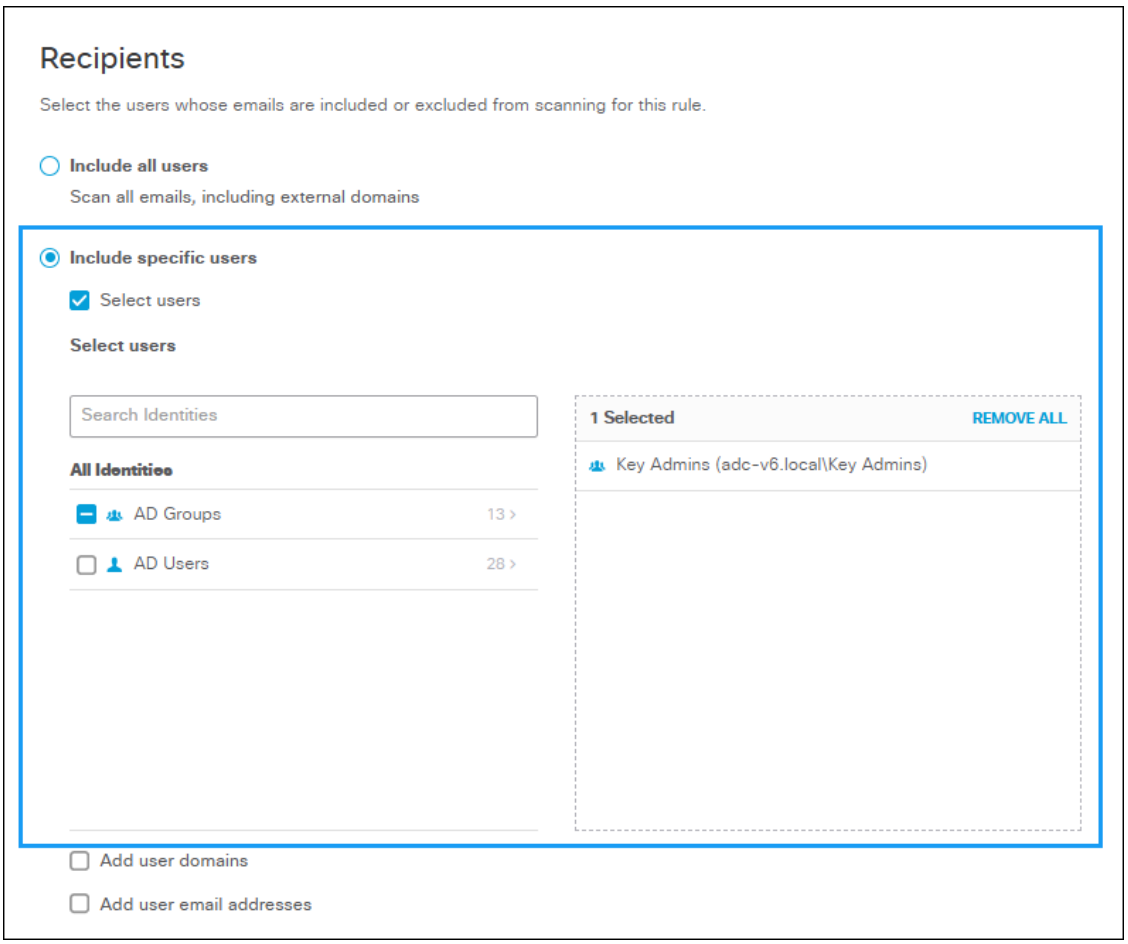
In the **Recipients** area, choose to include all users, include specific users, or exclude specific users.

- To scan all emails from all recipients, select **Include all users**.



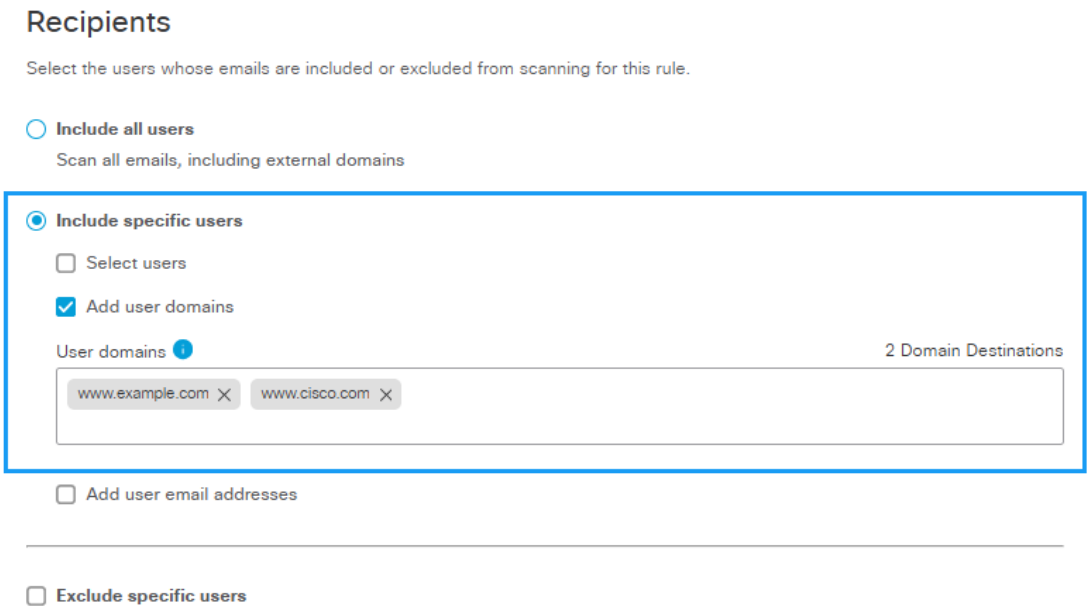
- To scan emails from selected recipients, you can choose one or more of the following options:
  - **Select users**

    Use the search box to search for Identities within your environment, or browse within the the lists for AD Groups and AD users. Check the boxes for the users to include--individually or by group. Selected users appear on the right.



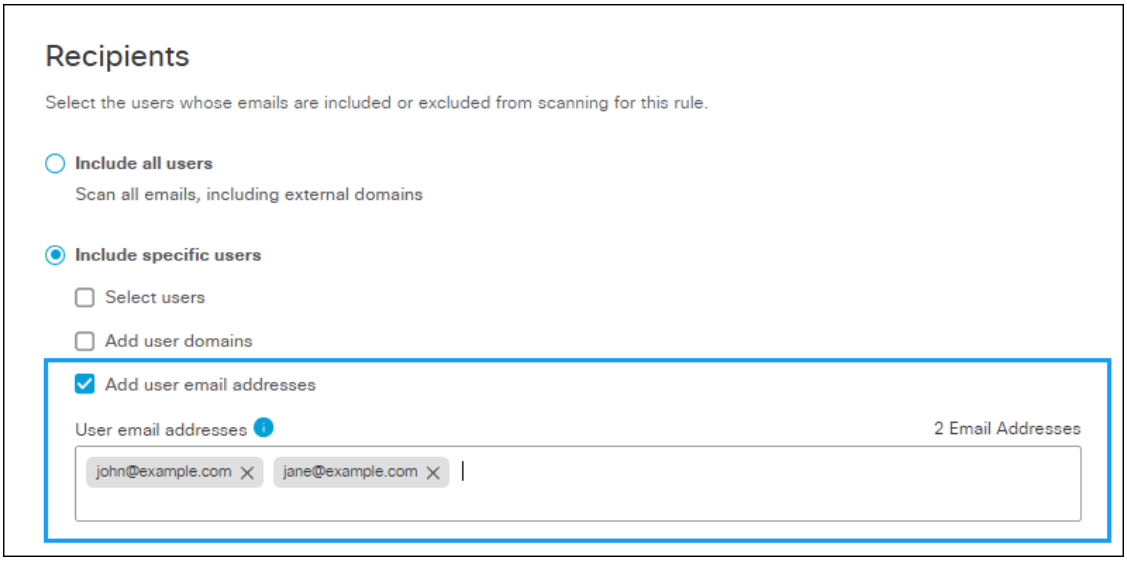
  - **Add user domains**

Enter one or more unique web site addresses to which email may be sent.



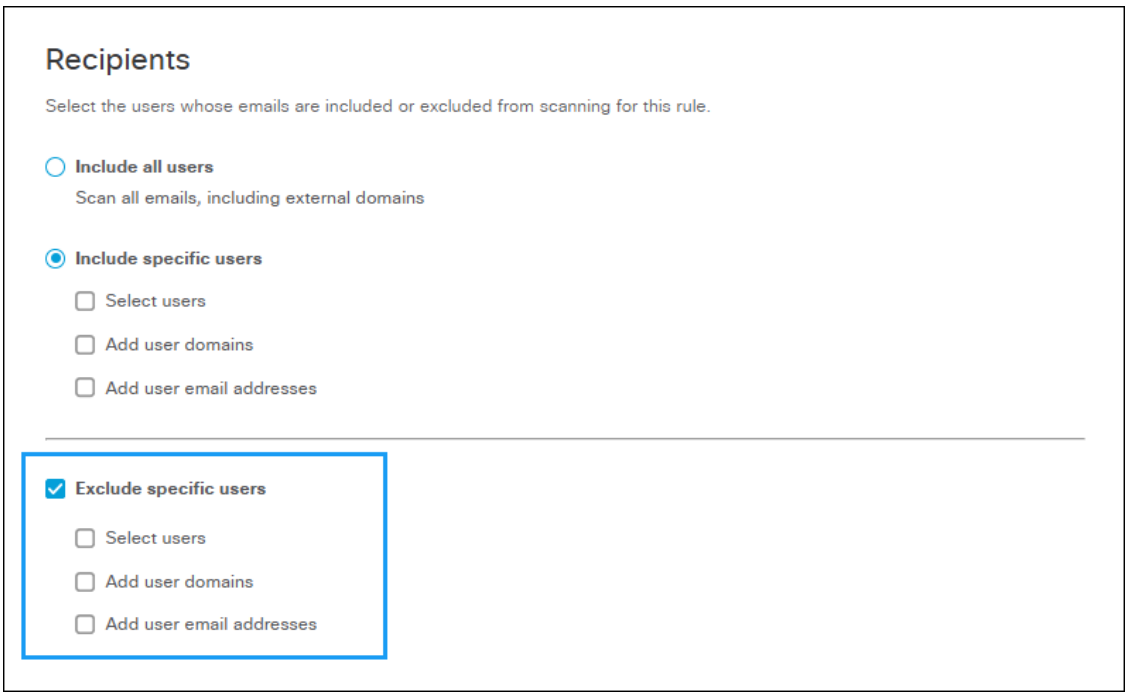
- **Add user email addresses**

  Enter one or more valid email addresses to which email may be sent.



- You can choose to exclude selected users from the lists of recipients you have included:

  a. Select **Exclude specific users**.



b. Choose one or more of the following options to select users to exclude:

- **Select users**
- **Add user domains**
- **Add user email addresses**

These options present the same mechanisms for selecting users as described for including users, above.

Create a DLP Email Rule Step 6 — Select the Rule Action

Provides instructions for completing the Create a DLP Email Rule Step 6 – Select the Rule Action workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the sixth step in the process to add an email rule to a DLP policy, in which you select an **Action** to be performed when data matches the rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 5 – Select the Recipients
- For the next step in the process, see Create a DLP Email Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations

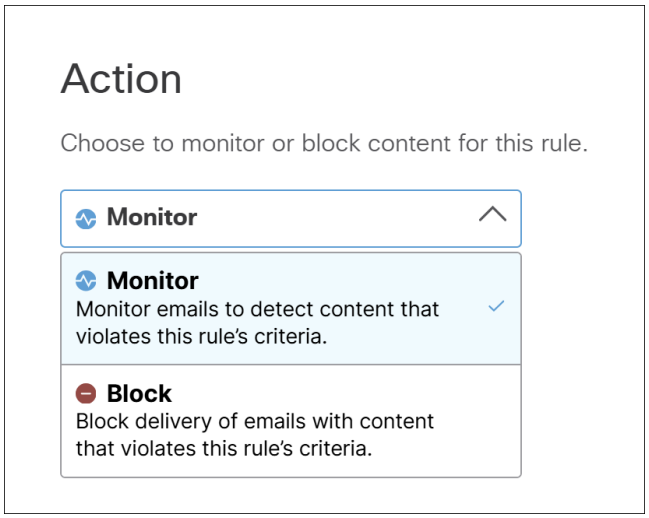
Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

From the **Action** drop-down list, choose **Monitor** or **Block**.

- **Monitor**- Detects and logs a DLP event for every email violating this rule's criteria
- **Block**- Blocks delivery of every email violating this rule's criteria, and logs a DLP event.



Create a DLP Email Rule Step 7 — Enable and Configure Pop-Up Notifications for Violations

Provides instructions for completing the Create a DLP Email Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the seventh step in the process to add an email rule to a DLP policy, in which you may optionally select to display a pop-up notification to the end user when data matches the rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy.
- For the previous step in the process, see Create a DLP Email Rule Step 6 – Select the Rule Action.
- For the next step in the process, see Create a DLP Email Rule Step 8 – Enable and Configure Email Notifications for Violations.

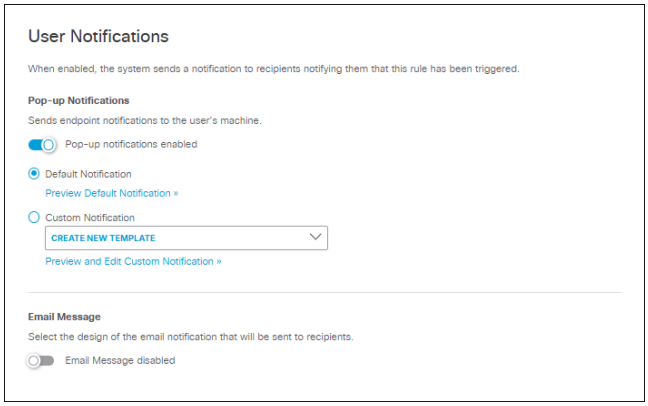
Before you begin

- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

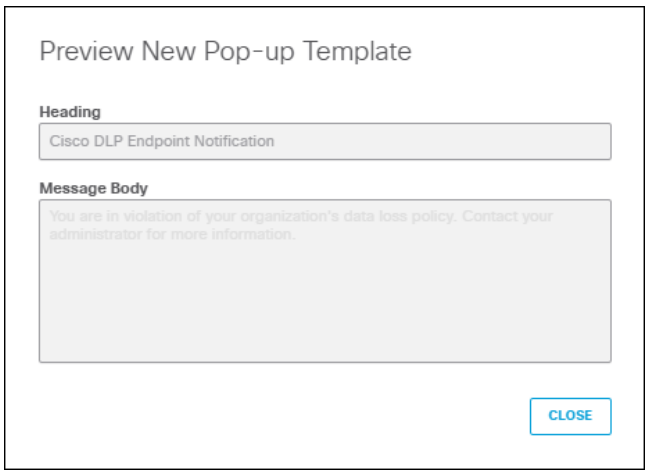
Procedure

1. Under **User Notifications**, you can enable the **Pop up Notifications** option to display pop-up notifications of violations to the end user.

> **Note**
>
> If you have no real time rules with at least one endpoint channel selected under Destinations, the **Pop up Notification** option remains disabled.

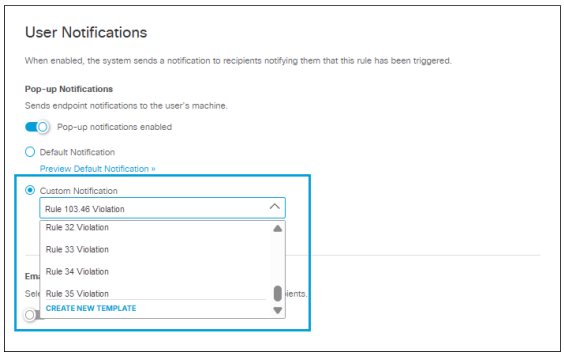


2. Define the message to appear in the pop up dialog when files match a rule.
   - **To use the default Pop Up Template:**
     a. Click **Default Notification**.
     b. To preview the content of the pop up text, click on **Preview Default Notification**. You can review the text, but you cannot change it.

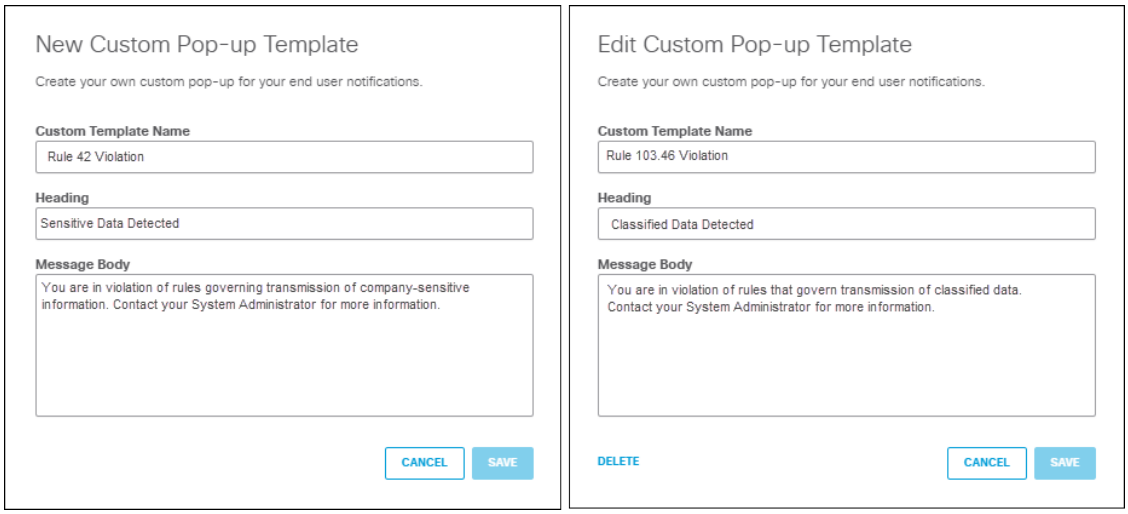


     c. Click **CLOSE** to close the preview.

   - **To use a Custom Pop Up Template:**
     a. Click **Custom Notification**.
     b. From the drop-down list, select an existing custom template, or choose **CREATE NEW TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Notification** to review and change the template.



c. When you choose to create or edit a custom template for pop up text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Pop-up Template** dialog includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the heading text for the pop up in the **Heading** text box.
3. Enter the message text for the pop up in the **Message Body** text box.
4. Click **SAVE** to complete the changes.

Create a DLP Email Rule Step 8 — Enable and Configure Email Notifications for Violations

Provides instructions for completing the Create a DLP Email Rule Step 8 – Enable and Configure Email Notifications for Violations workflow in Cisco Secure Access. You must have full Admin user permission in Secure Access.

This is the seventh and final step in the process to add an email rule to a DLP policy, in which you may optionally select to configure and enable email notifications to send users when data matches the rule.

- For an overview of the entire process, see Add an Email Rule to the Data Loss Prevention Policy
- For the previous step in the process, see Create a DLP Email Rule Step 7 – Enable and Configure Pop-Up Notifications for Violations

Before you begin

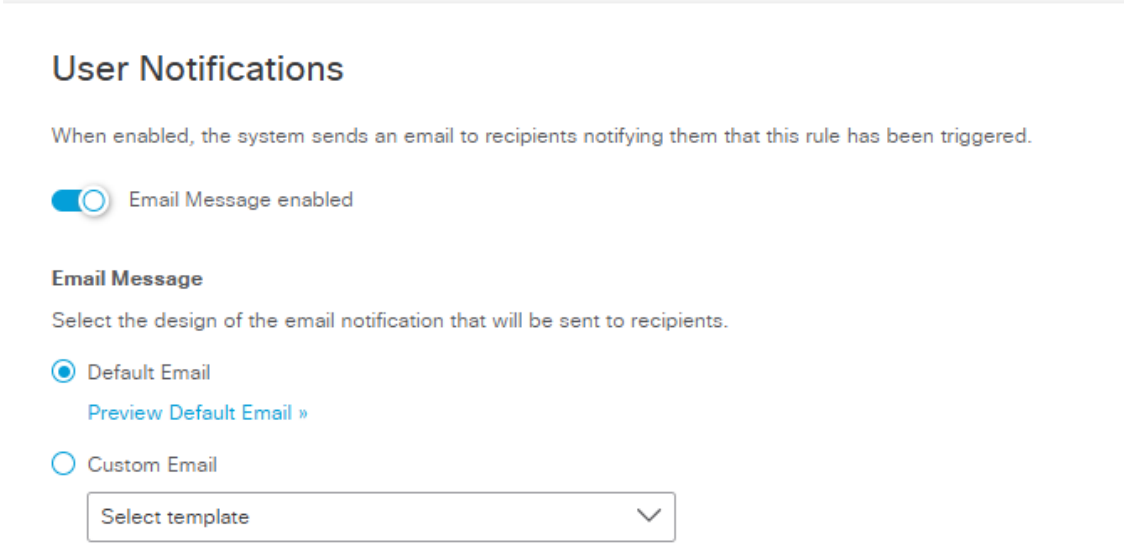
- You must have full Admin user permission in Secure Access. For more information, see Manage Accounts.
- You must install Cisco Secure Email Threat Defense.
- You must Integrate Email Threat Defense with Secure Access DLP.

Procedure

1. Under **User Notifications** you can enable and configure an email notification to be sent to a user who triggers a violation of the rule. You can use a default email template provided by the system, or create your own custom template.

> **Note**
>
> The system gets the "send to" address for the notification email from UPN field in the authenticated active directory. Some identity configurations may not be able to provide the end user's email address, in which case the system will be unable to send the email. These cases include:
>
> - The user uses network or tunnel identities, in which case the user's IP address will be available to the system, but not the email address.
> - The user did not authenticate through active directory, so the system has no information about the user.
> - The user's email address is not stored in the UPN field in the authenticated active directory.

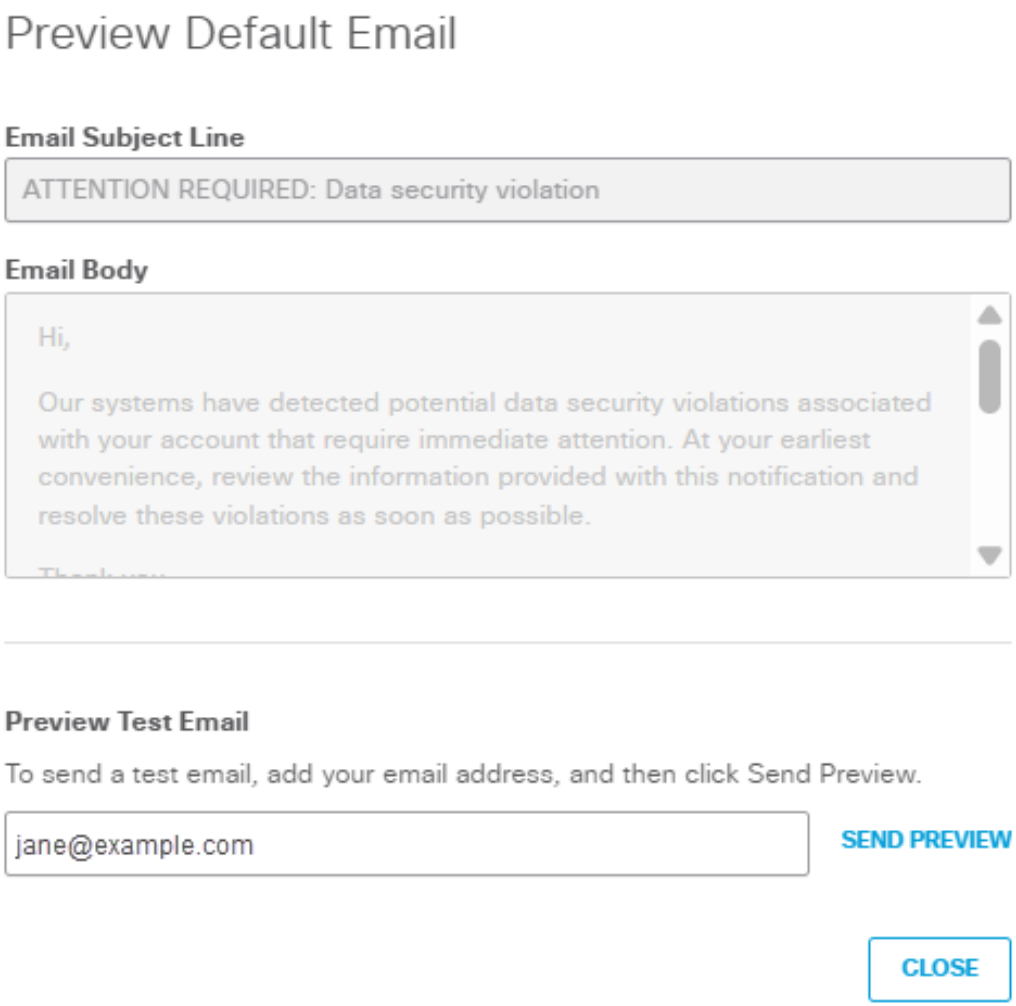
   a. Enable Email messages.



   b. Choose the email template:

   To Use the Default Email Template:

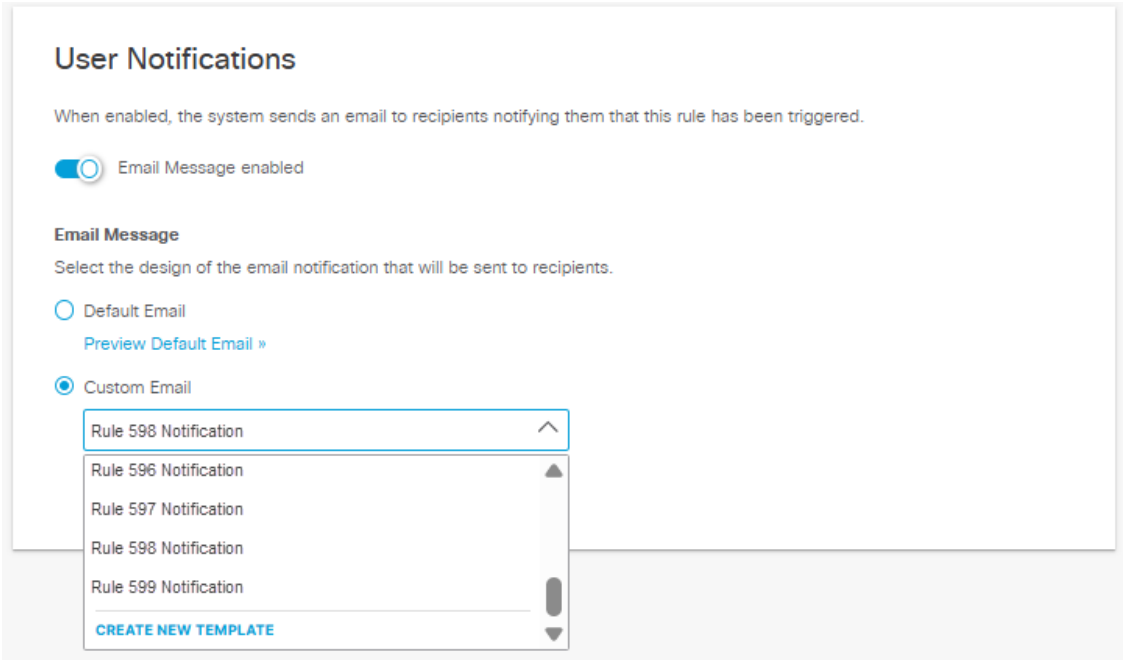
   1. Click **Default Email**.
   2. To preview the content of the email that will be send to users, click on **Preview Default Email**. You can review the email subject line and text, but you cannot change it.



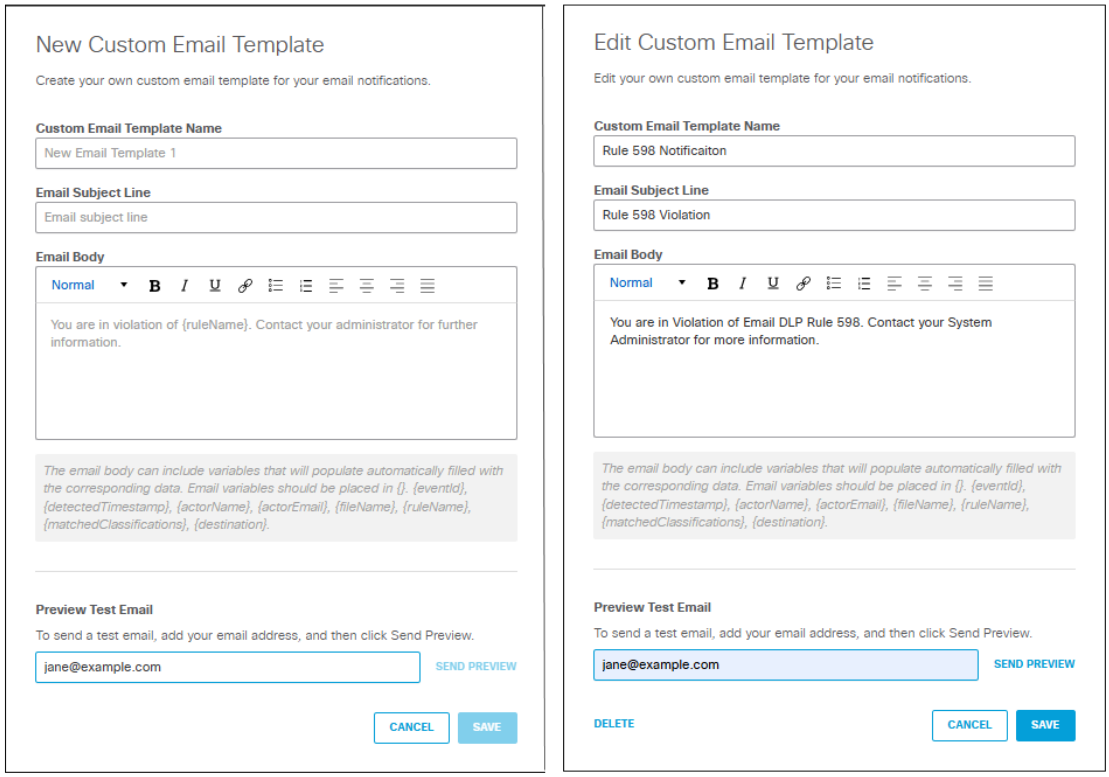
3. (Optional) To send a test copy of the email to an address of your choosing, enter an address in **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)
4. Click **CLOSE** to return to the Data Loss Prevention Policy page.

To Use a Custom Email Template:

1. Click **Custom Email**.
2. From the drop down menu, select an existing custom template, or choose **CREATE NEW TEMPLATE**. If you select an existing custom template, you can click **Preview and Edit Custom Email** to review and change the template.



3. When you choose to create or edit a custom template for email notifications of policy violations you will see one of these two dialogs, which are almost identical:



The **Edit Custom Email Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You may not delete a template that is in use by any rule.

To create a new template or change an existing template:

a. Enter a unique **Custom Email Template Name**.

b. Enter an **Email Subject Line**.

c. Enter the text of the email in the **Email Body** text box.

The email text can include the following variables, which you must enclose in braces (**{}**):

- **{eventId}** - The unique identifier the system generates for the policy violation event.
- **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
- **{actorName}** - Name of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{actorEmail}** - Email address of the user whose action triggered the violation. (Secure Access gets this information from the authenticated Active Directory.)
- **{fileName}** - Name of the data file that triggered the violation.
- **{ruleName}** - Name of the rule that was triggered.
- **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
- **{destination}** - URL or IP address of the intended destination for the monitored request.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

d. (Optional) To send a test copy of the email to an address of your choosing, enter an address inHere is my first draft of sd **Preview Test Email** and click **SEND PREVIEW** to send the message. (By default the system uses the email address of the logged in user.)

e. Click **SAVE**.

2. Click **Save**. All fields must have options selected to save.

Discovery Scan

Describes Discovery Scan in Cisco Secure Access. Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range.

Discovery Scan inspects the content of all files in the tenant that are modified over the selected date range. As files in the selected tenant are scanned upon content change and context (sharing) change, Secure Access assesses the file. If Secure Access detects a violation, the offending file is listed in the Data Loss Prevention Report.

This topic walks you through how to initiate a scan and how to cancel an ongoing scan.

> **Note**
>
> A discovery scan must be triggered around 24 hours after tenant authorization as the system evaluates and enumerates the users in the organization. Any triggering beforehand might not include all users. Secure Access performs discovery scans on files of up to 50 MB. For each file, the scan extracts up to the first 5 MB of plain text from the file, and scans that data for violations.

Prerequisites

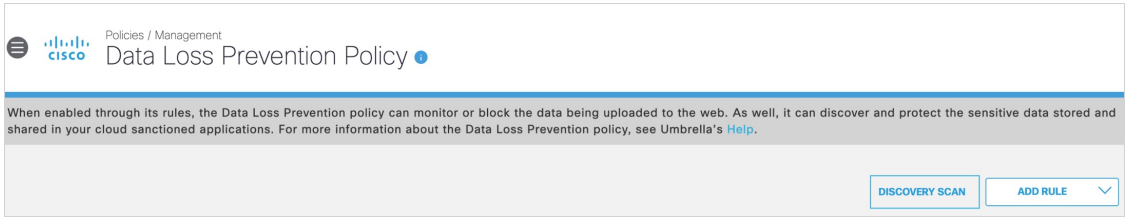
- You must authenticate a tenant for at least one of the platforms Secure Access supports for SaaS API Data Loss Prevention. For more information, see Manage SaaS API Data Loss Prevention.

Initiate a Discovery Scan

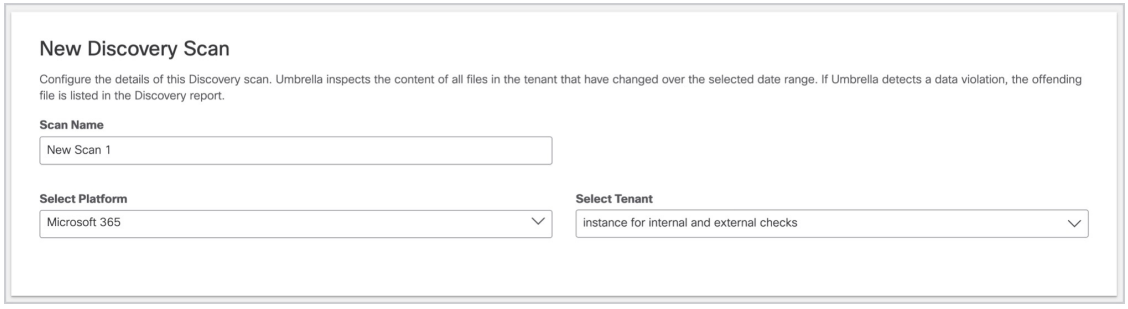
Provides instructions for completing the Initiate a Discovery Scan workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click **Discovery Scan**.



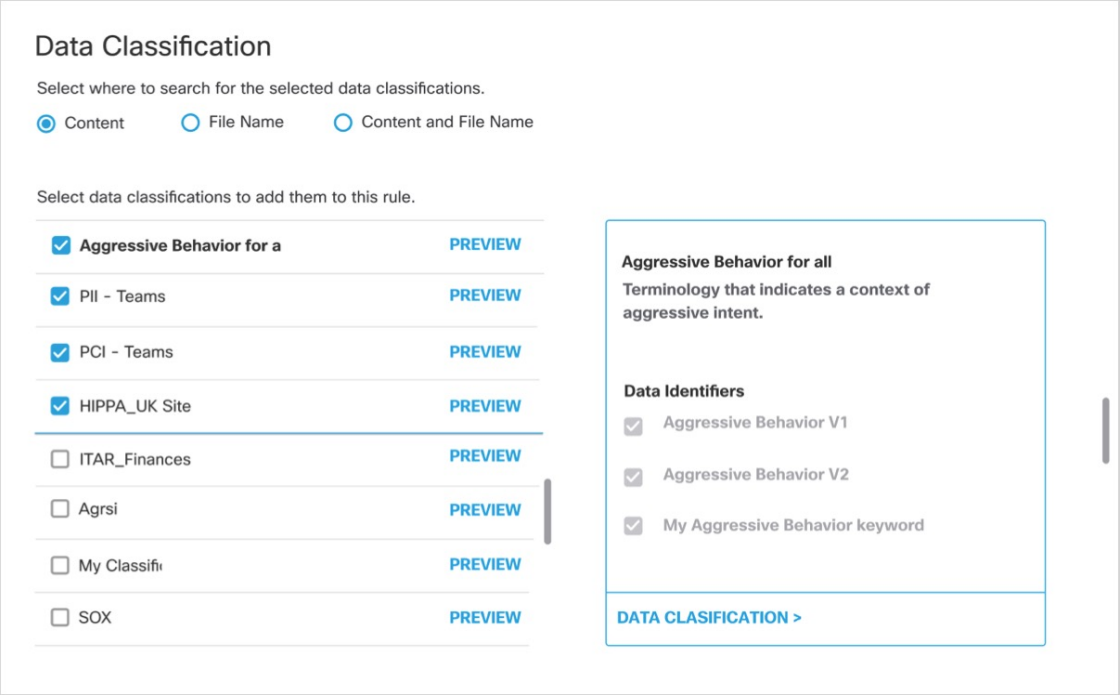
3. Enter the **Scan Details**. Choose a platform and tenant of the platform from the drop-down lists.



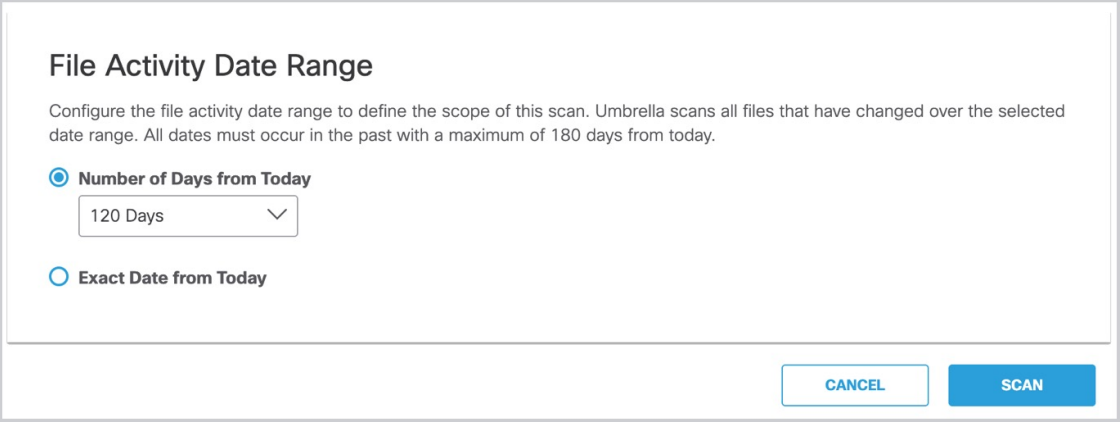
4. Select where in uploaded files you would like the scan to search for the data classifications that you choose.
   - **Content**–(Default) Searches only the content of files for the selected data classifications.
   - **File Name**–Searches only file names for the selected data classifications.
   - **Content and File Name**–Searches content and file names for the selected data classifications. Both content and file name do not need to match for the scan to apply, only one or the other.

> **Note**
>
> Choosing Content, File Name, or Content and File Name refers to scanning file uploads for the selected data classifications and configured file labels.

5. Select the required **Data Classification** of your choice. You can select multiple tenants.

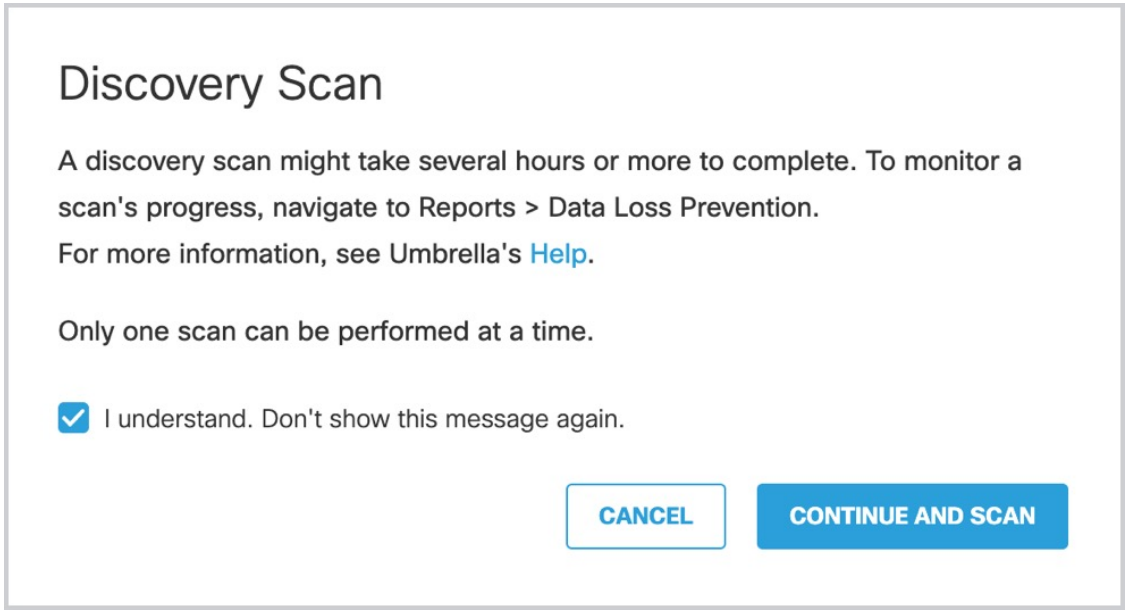


6. Enter the Date Range to define the scanning scope. Note that only files modified in the selected date range are scanned.



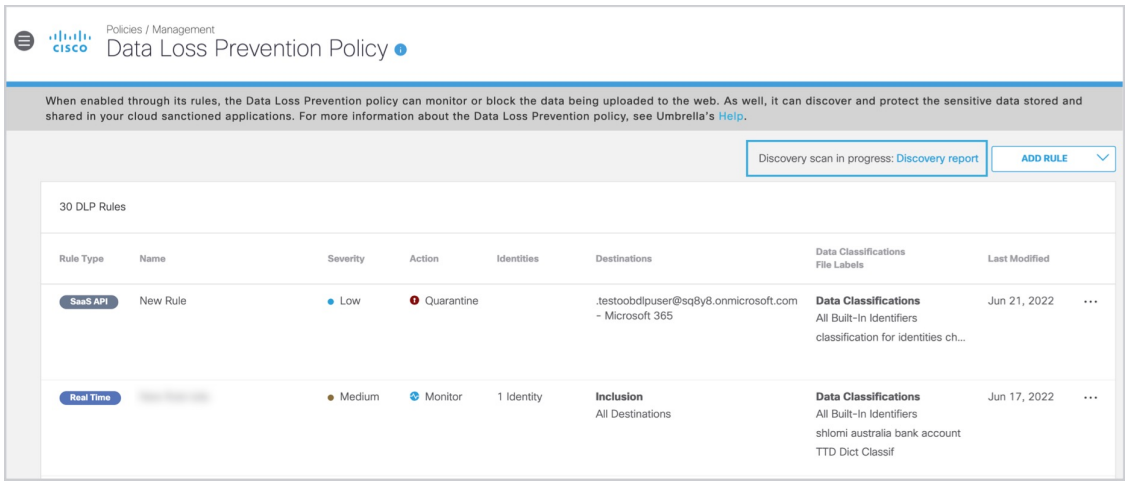
7. Click **Scan** to initiate.
8. Click **Continue and Scan**.

> **Note**
>
> Only one scan executes at a time. The scan might take a while. Once completed, you can initiate another scan.



9. Click **Discovery Report** to view the progress of the scan results.

   For more information on DLP reports, refer to DLP Report.



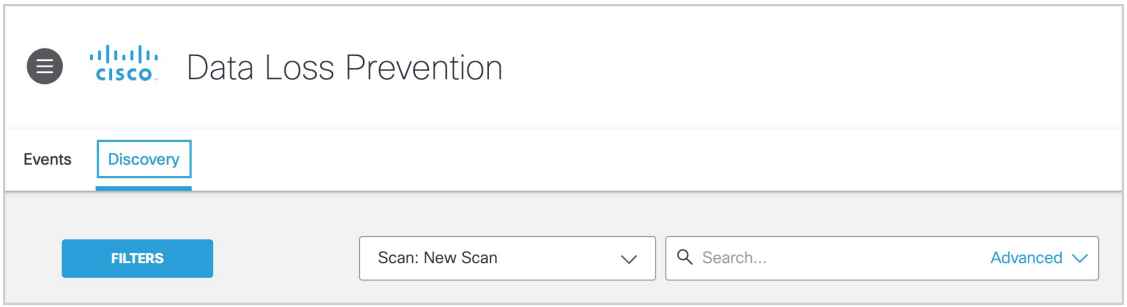
Cancel a Discovery Scan

Provides instructions for completing the Cancel a Discovery Scan workflow in Cisco Secure Access. Navigate to Reporting Additional Reports Data Loss Prevention .

Procedure

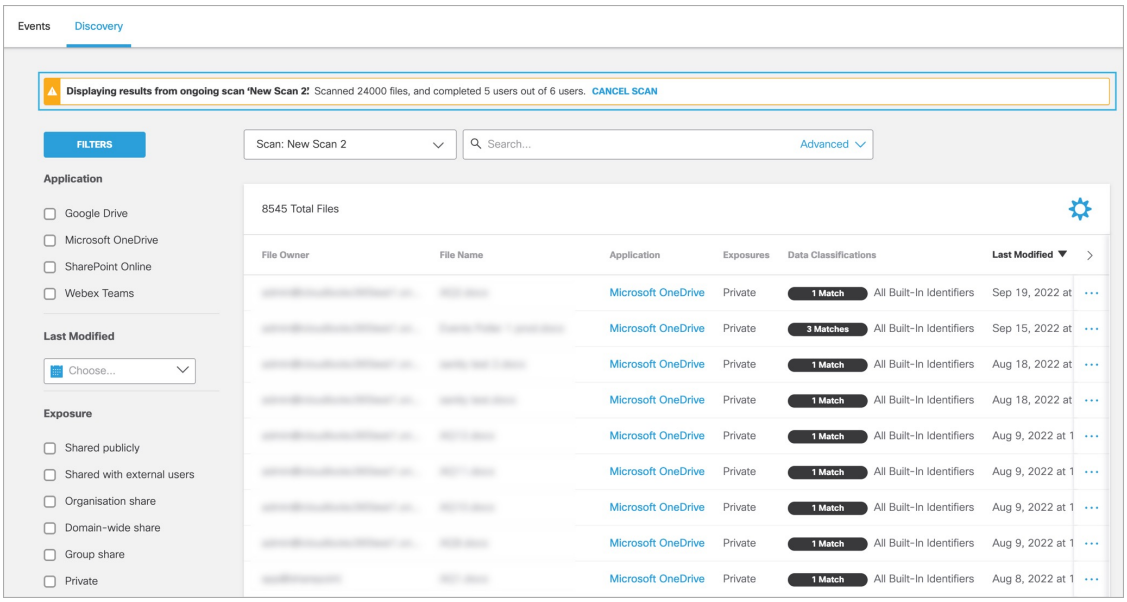
1. Navigate to **Reporting** > **Additional Reports** > **Data Loss Prevention**.

2. Switch to the **Discovery** tab.

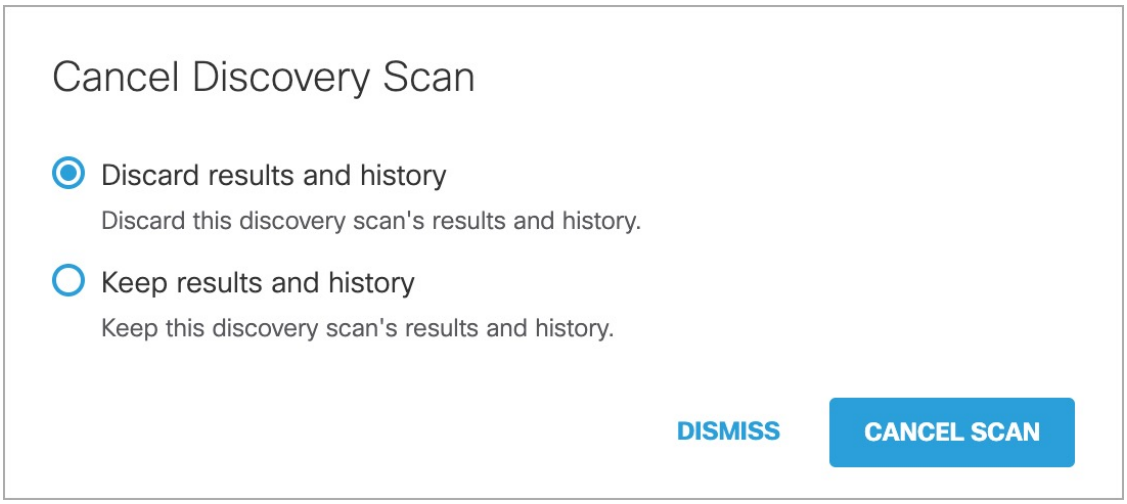


3. Click **Cancel Scan**. Results of the ongoing scan are displayed in the ribbon.

   Note that the cancellation of a scan might take a few minutes.



4. You can choose to either discard or keep the scan results and history. Click **Cancel Scan**.



Edit a Data Loss Prevention Rule

Provides instructions for completing the Edit a Data Loss Prevention Rule workflow in Cisco Secure Access. Full admin access to the Secure Access dashboard.

After adding a Real Time or SaaS API rule, you can edit it to change what traffic it monitors (identities and destinations) or what cloud tenant is applicable to, the data classifications and file labels that represent the data violation criteria, and the action to be enforced upon detecting data violations in the scanned content.

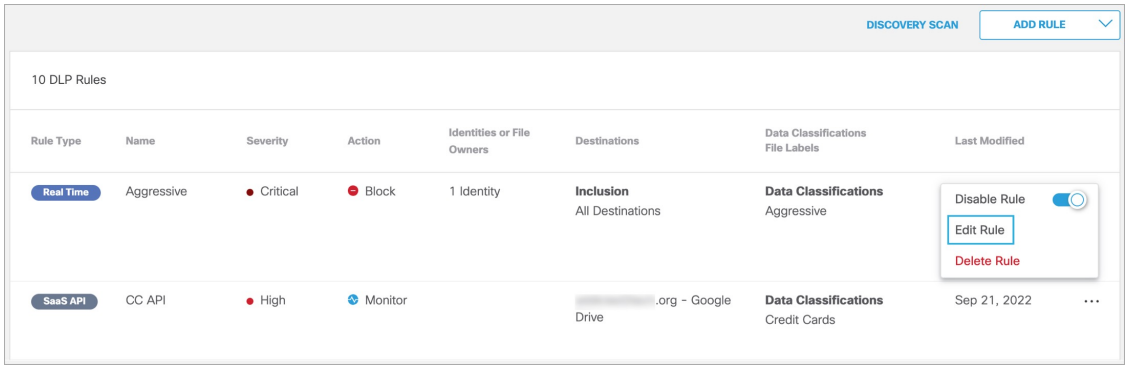
> **Note**
>
> Editing a rule does not impact any running Discovery Scan, it only impacts incoming events for the scan.

Before you begin

- Full admin access to the Secure Access dashboard. See Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and select **Edit Rule**.



3. Make the changes and click **Save**.

Delete a Data Loss Prevention Rule

Provides instructions for completing the Delete a Data Loss Prevention Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can delete a Data Loss Prevention rule at any time. To edit a rule, see Edit a Data Loss Prevention Rule.

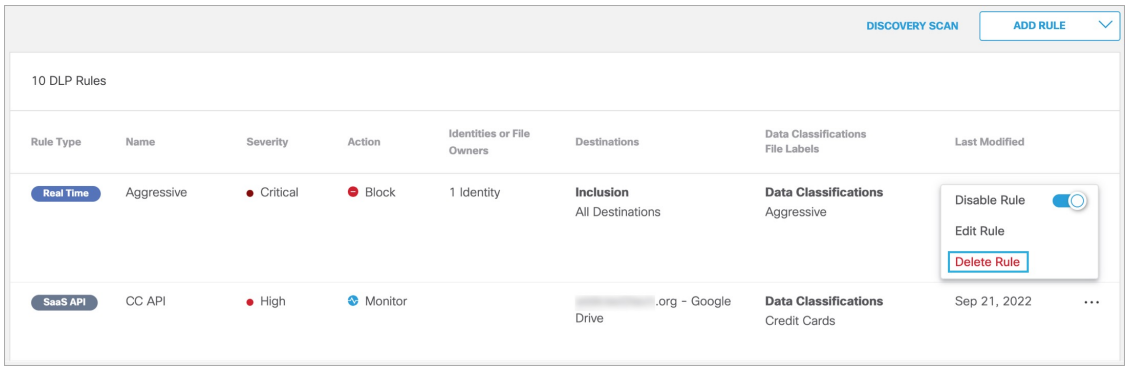
Deleting a rule does not impact a running Discovery Scan, it only impacts incoming events for the scan.

Before you begin

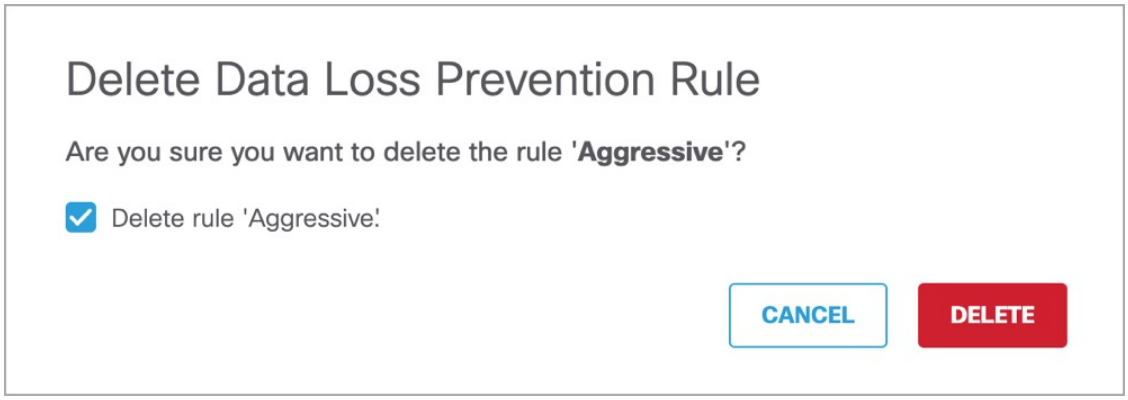
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and click **Delete Rule**.



3. Confirm deleting the rule and then click **Delete**.



Enable or Disable a Data Loss Prevention Rule

Describes Enable or Disable a Data Loss Prevention Rule in Cisco Secure Access. Newly added rules are automatically enabled for the Data Loss Prevention policy.

Newly added rules are automatically enabled for the Data Loss Prevention policy. When you navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**, disabled rules appear faded. Note that enabling or disabling a rule does not impact any running Discovery Scan, it only impacts incoming events for the scan.

Prerequisites

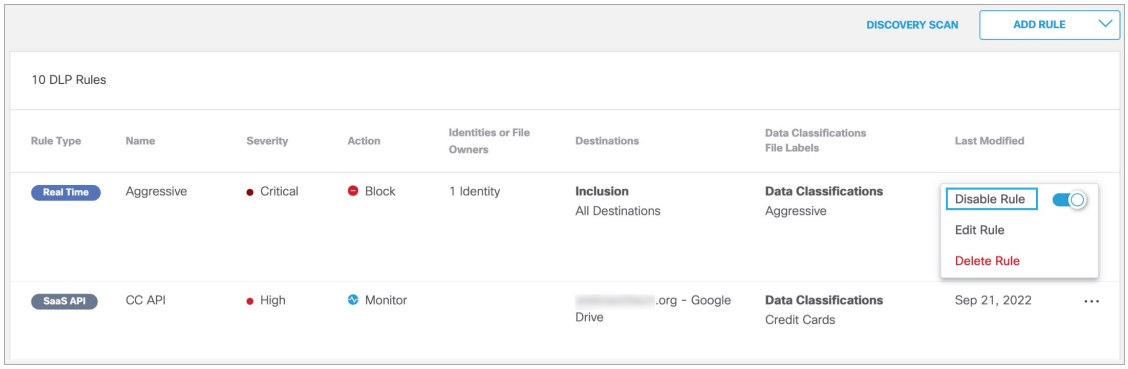
- Full Admin user role. For more information, see Manage Accounts.
- For Real Time DLP rules, HTTPS Inspection must be enabled either on the Web Default Policy, or at least one web policy ruleset where the same identity is configured in a DLP rule. For example, if the identity "Network A" is configured for a DLP rule, it must also be configured for a web policy ruleset where HTTPS is enabled. For more information, see Manage Traffic Decryption and Manage Web Profiles.

Disable a Rule

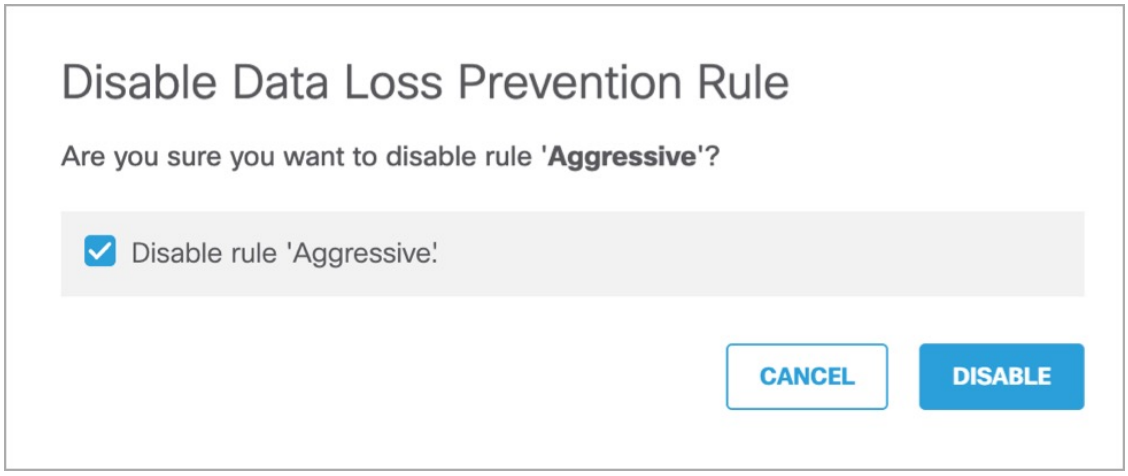
Provides instructions for completing the Disable a Rule workflow in Cisco Secure Access. Navigate to Secure Policy Data Loss Prevention Policy .

Procedure

1. Navigate to **Secure** > **Policy** > **Data Loss Prevention Policy**.
2. Click the **More Actions** menu, and click **Disable Rule**.



3. Confirm disabling the rule and then click **Disable**.

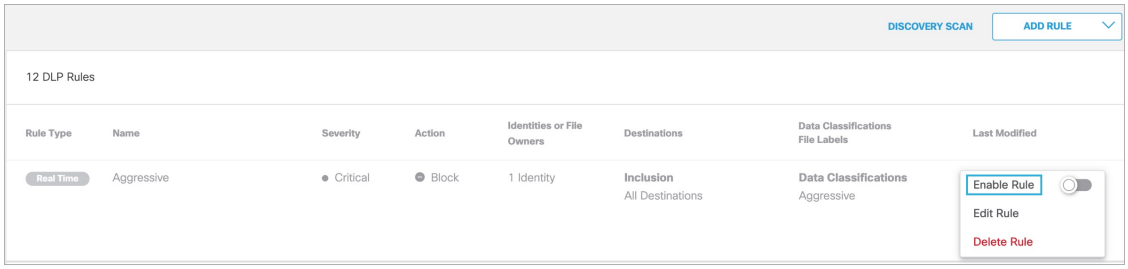


Enable a Rule

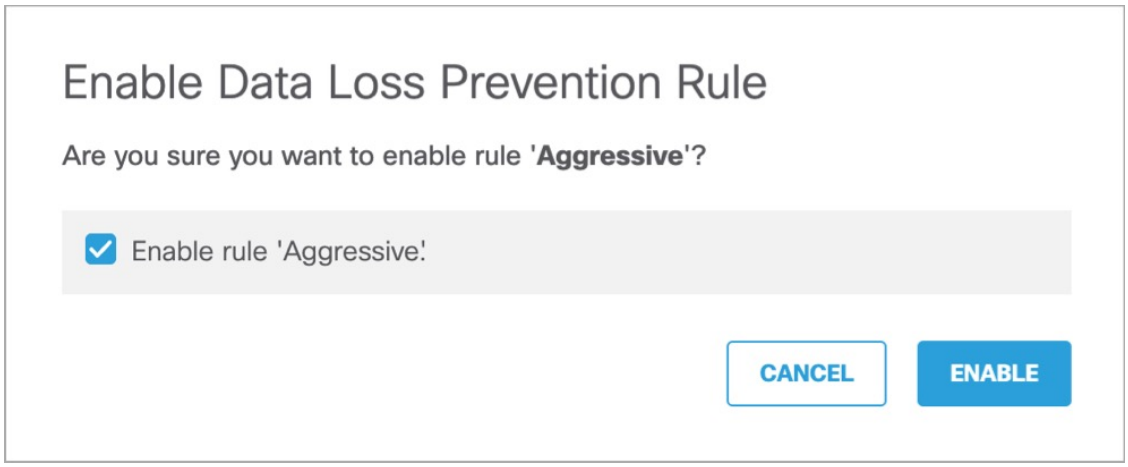
Provides instructions for completing the Enable a Rule workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Policy** > **Data Protection Policy**.
2. Click the **More Actions** menu, and click **Enable Rule**.



3. Confirm enabling the rule and then click **Enable**.



Manage Global Settings

This concept explains how to configure common or specific settings for Endpoint channels to manage data exfiltration policies.

When the Endpoint Data Loss Prevention (DLP) module operates in error mode, choose an action using Global Settings:

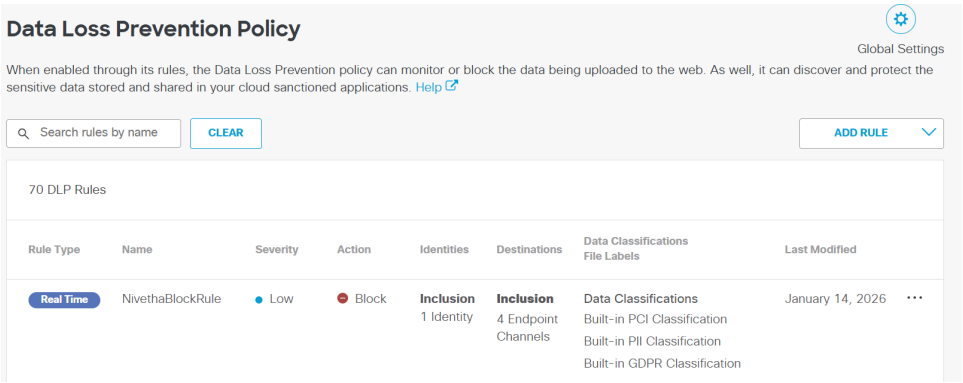
- Fail-close–Blocks data exfiltration
- Fail-open–Allows data exfiltration

The Endpoint DLP module may also decide locally to apply fail-open or fail-close in certain cases, such as:

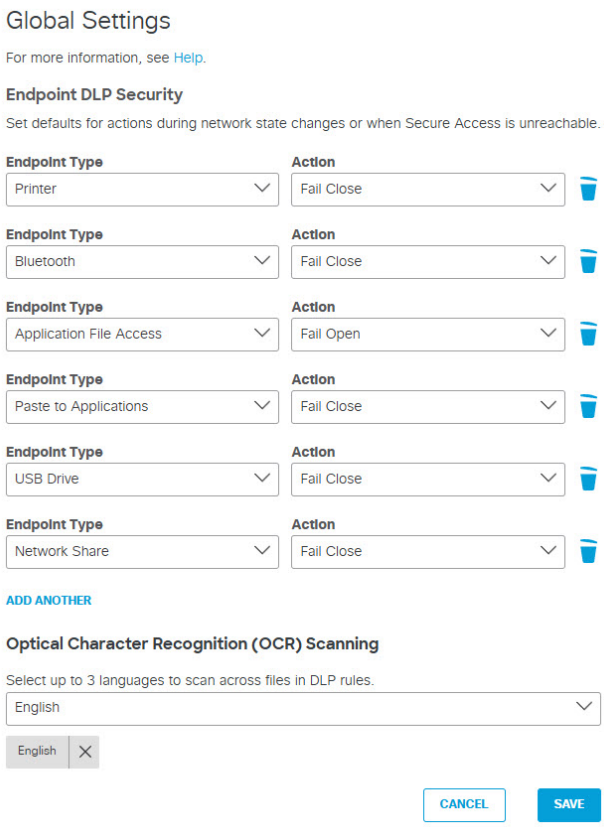
- **Internet connection failure**–When you try to copy files from a device to a destination such as a USB drive, the Endpoint DLP module can block the transfer by default if the internet connection is unavailable.
- **Cloud response failure**–When DLP scan calls to the cloud fail because of connection timeouts, request timeouts, or rate limiting, the Endpoint DLP module applies the configuration chosen by the administrator.

Procedure

1. Navigate to **Secure** > **Data Loss Prevention Policy**, and click **Global Settings**.



2. Make the required configuration changes.



3. To detect sensitive content in images, under **Optical Character Recognition (OCR) Scanning**, select up to three languages.

   Secure Access uses the selected languages to extract text from supported images and then evaluates the extracted text against configured data classifications and DLP rules. For more information on supported OCR file types and limitations, see Supported File and Form Types.

   Configuring OCR Scanning enables text extraction from supported image content. To use OCR-based detection in a policy, complete the following additional tasks:

   a. Use built-in identifiers or create custom identifiers for the terms or patterns that you want to detect in OCR-extracted text. For more information, see Create a Custom Identifier.

   b. Create a data classification and add the identifiers that you want Secure Access to match in OCR-extracted text. For more information, see Procedure for Creating a Data Classification.

c. Apply the classification in a DLP rule. When you configure the rule, choose Content or Content and File Name so the rule evaluates OCR-extracted text in files. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.

4. Click **Save**.

You can set a common configuration for all channels or apply a specific configuration for each channel.

> **Note**
>
> The latest configuration may take approximately 30 minutes to sync to the client.

44 Secure Browser Extension

Topics:

- Secure Browser Extension

Secure Browser Extension

Cisco Secure Enterprise Browser extends Cisco Secure Access protections directly into managed browsers. It combines **Secure Enterprise Browser** controls with **Browser Detection and Response** capabilities to govern SaaS, GenAI, private application, and web workflows at the point where users interact with enterprise data.

Manage the Secure Browser Extension

About the Secure Browser Extension

The Cisco Secure Browser Extension is the browser security client for Cisco Secure Access. It installs as a lightweight extension that enforces security policy and collects telemetry directly within managed browsers.

The extension connects browser activity to Secure Access policy and broker services, Secure Web Gateway (SWG) proxy decisions, DLP verdicts, private access policy, and enterprise-managed configuration.

Content-agnostic browser protection is included with Cisco Secure Access packages. Content-aware protection requires the applicable DLP entitlement and is configured through a Real Time DLP rule in the Secure Access Data Loss Prevention Policy.

Install the Cisco Secure Browser Extension

Prerequisites and steps to install Cisco Secure Browser Extension

Cisco Secure Browser Extension supports managed and unmanaged installation. The exact steps depend on the browser, operating system, and selected device-management or MDM platform.

> **Note**
>
> Secure Browser Extension is not supported in incognito mode.

The supported installation methods include:

- Chrome Web Store installation in Chrome, Microsoft Edge and Brave,
- Enterprise force-install through supported browser policy,
- Device-management or MDM deployment,
- Browser-native managed package installation where the browser supports it,
- Administrator-distributed CRX or package from a customer-managed site; and
- Administrator-owned unpacked package with approved manifest configuration.

> **Note**
>
> Microsoft Edge Add-ons, other Chromium extension stores, and developer-mode unpacked installation for customer development or evaluation are not supported.

Before you begin

- Full admin access. For more information, see Manage Accounts.
- Confirm the following:
  - the supported browser and desktop operating system selected for the deployment;
  - the approved installation source and, for managed deployment, the applicable browser or MDM policy;
  - whether organization, user, device identifier, update source, and automatic-enrollment settings will be supplied through management; and
  - that Secure Access SAML prerequisites are complete before you activate the extension.

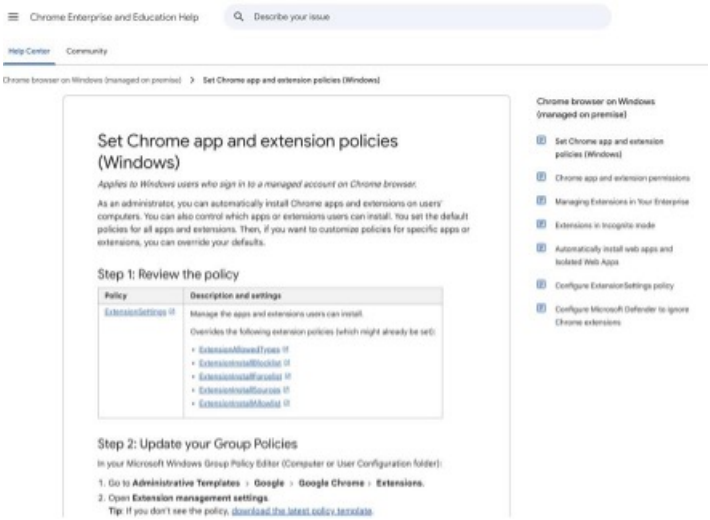
Procedure

1. Choose from the following to deploy the Cisco Secure Browser Extension:
   - **Managed deployment**:

     A managed installation can supply optional organization, user, device identifier, update source, and automatic-enrollment settings when the management platform supports them. Organization and user settings can restrict enrollment to an approved organization or user set. A device identifier helps correlate installed Secure Access modules in the dashboard.

     Force-installed users cannot disable or uninstall the extension through normal browser controls. User control for an optional managed assignment follows the browser-management policy. Administrators are responsible for resolving browser, MDM, allowlist, blocklist, update, or security-policy conflicts.

     For example, read more about Set Chrome app and extension policies (Windows):



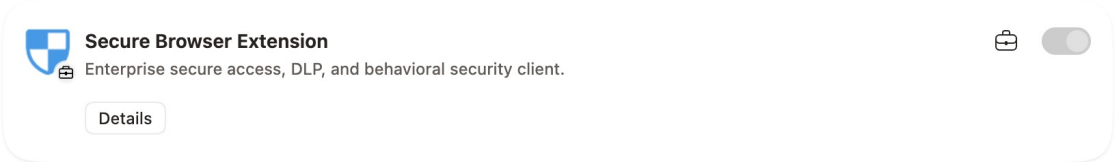
> **Note**
>
> The extension-supported attributes include: **orgId**, **emails**, **autoEnroll**, and **allowAdminControls**.

- **Unmanaged and administrator-owned packages**:

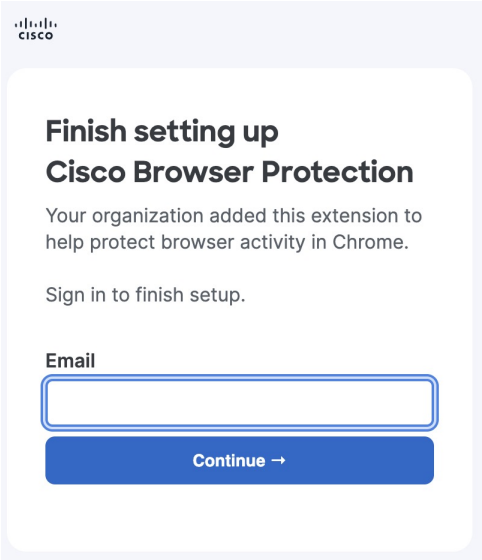
  A store-installed user can uninstall the extension. Administrators who host or modify a package own its hosting, configuration, identity, integrity, distribution, and updates.

  When organization or user hints are not supplied, you can enter an email address and continue through organization discovery and SAML authentication.

2. Download the extension via this link or by using this extension ID: ***lejnccmfdieebndebgkdckcbabbnnndm*.**
3. Confirm the installation:
   a) Open the browser's extension-management page and confirm Cisco Secure Browser Extension is present and enabled.



   b) Pin or open the extension from the browser toolbar.
   c) Confirm the setup screen opens.



> **Note**
>
> This proves that the extension is installed, but it does not prove that registration or policy synchronization has completed.

   d) Complete your SAML registration.

> **Note**
>
> For a managed installation, also confirm that the browser reports the extension as managed and that a standard user cannot remove it when force-install is intended. Exact management labels vary by browser and MDM.

Onboarding and Activation

When organization, user, and automatic-enrollment settings are available, the extension opens the configured identity provider at launch. You are still required to enter credentials, complete multifactor authentication, grant conditional access, or authorize any other identity-provider interaction when required. If a valid identity-provider session already exists, another credentials prompt may not be needed.

When automatic enrollment is disabled, you can start the setup journey before SAML authentication. If automatic enrollment is cancelled or fails, the extension falls back to the applicable user-initiated journey instead of repeatedly forcing the automatic flow:

- With valid organization and user hints, the setup journey retains those hints and lets you restart the configured organization's SAML flow.
- Without complete hints, the setup journey asks for email and performs organization discovery.

When organization and user hints are unavailable, you can enter an email address. Secure Access discovers eligible organizations:

- One eligible organization continues to its identity provider.
- Multiple eligible organizations display an organization selector and require the user to choose one before authentication. Cancelling the selector returns to the user-initiated setup journey so selection can be retried.
- Registration fails if no eligible organization is found or the user details are incomplete.

After successful authentication and registration, the extension receives the tokens and configuration required for its enrolled state.

Before you begin

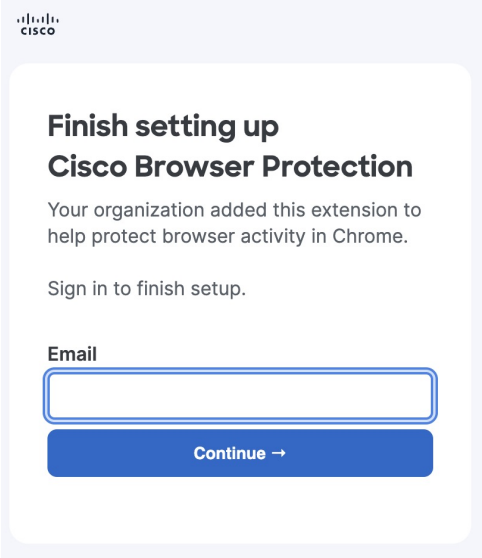
1. You must configure the organization's SAML identity provider and assign it to the applicable Secure Access configuration.
2. See Cisco Secure Access Prerequisites for SAML Authentication.
3. You should have:
   - the extension installed and enabled;
   - an organization-managed identity that can complete the configured SAML flow; and
   - organization or email details when they are not supplied through managed browser settings.
4. For more information about downloading and installing the certification, see Download the Cisco Secure Access Root Certificate.

Procedure

1. Open Cisco Secure Browser Extension from the browser toolbar.

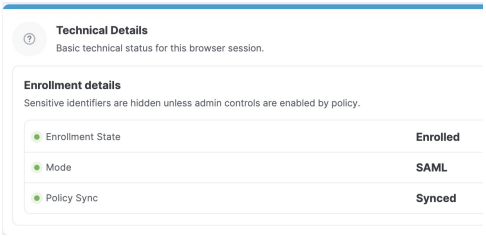


2. On the setup screen, select the available sign-in or setup action. If managed automatic enrollment is configured, this step may begin automatically.



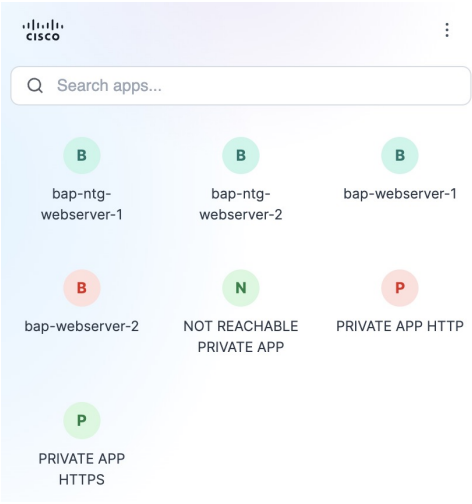
> **Note**
>
> You need to re-enrol every time you close and re-open the browser.

3. Enter the requested email or select an eligible organization when the extension cannot determine it from managed settings.
4. Complete the organization's SAML flow in the identity-provider window. The identity provider controls credentials, multifactor authentication, and conditional-access prompts.
5. Return to the extension. A waiting state can appear while authentication and registration finish.

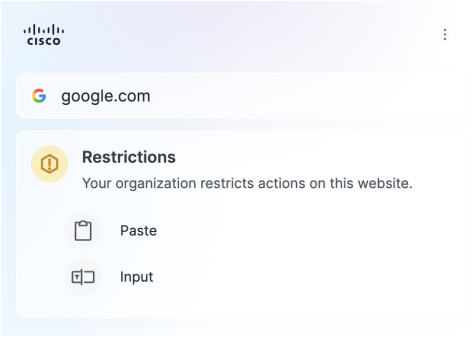


6. You will see the page below in the extension, with a list of the private resources you can access or the restrictions provided on an Internet page.

   Private Applications:



Internet Applications:



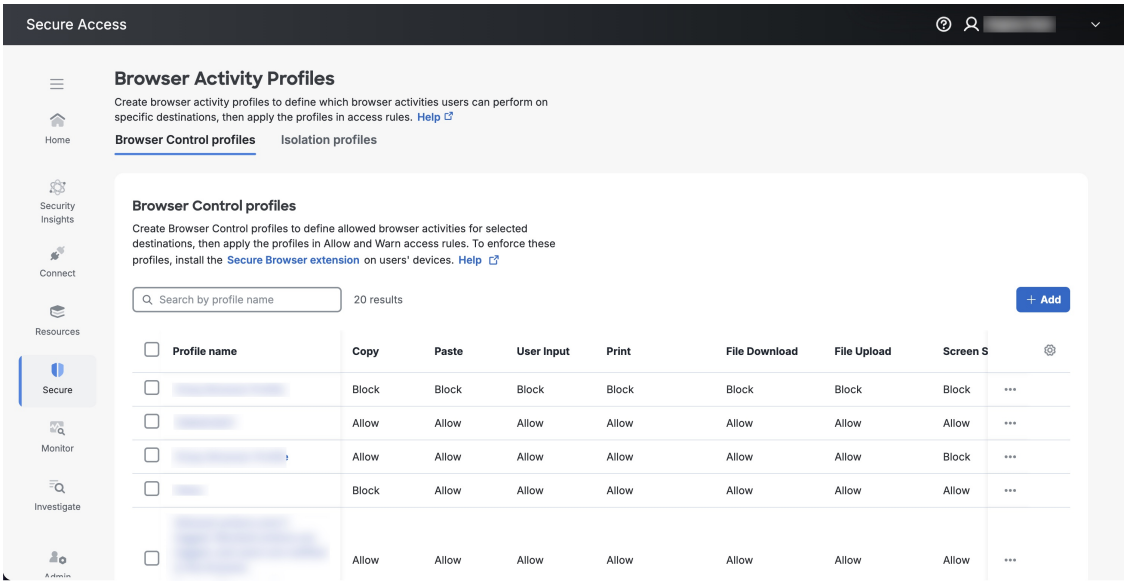
Configure Browser Policy

Before you begin

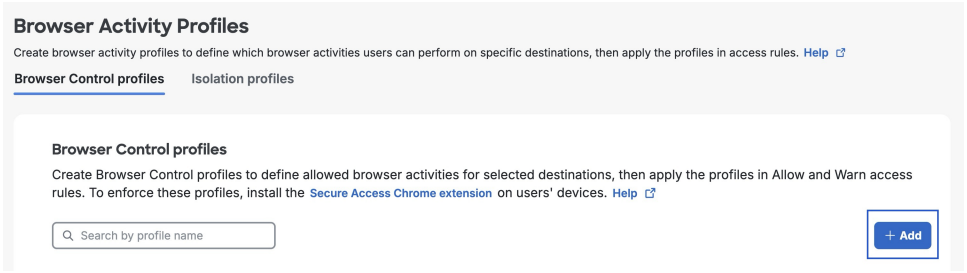
Full Admin user role. For more information, see Manage Accounts.

Procedure

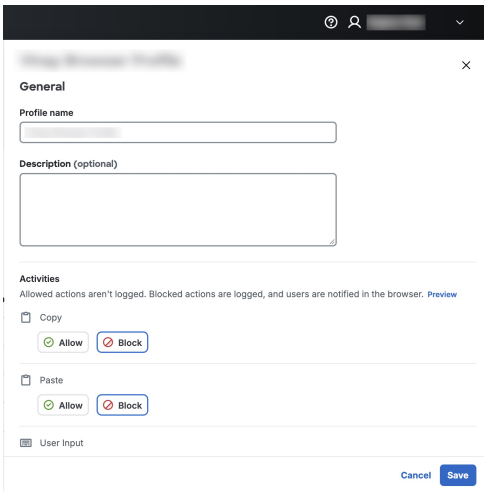
1. Create a Browser Control Profile:
   a) Navigate to **Secure** > **Profiles** > **Browser Activity Profiles**.



b) In the Browser Control profiles tab, click the **+ Add** button.



c) Enter a profile name and optional description, then choose Allow or Block for each browser activity.

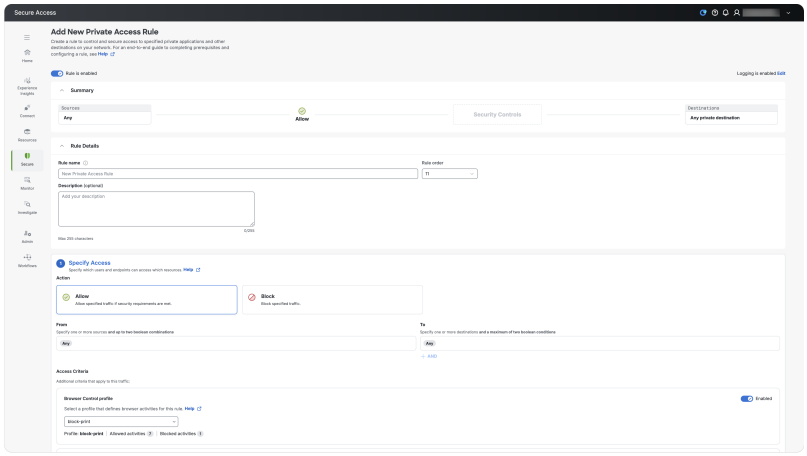


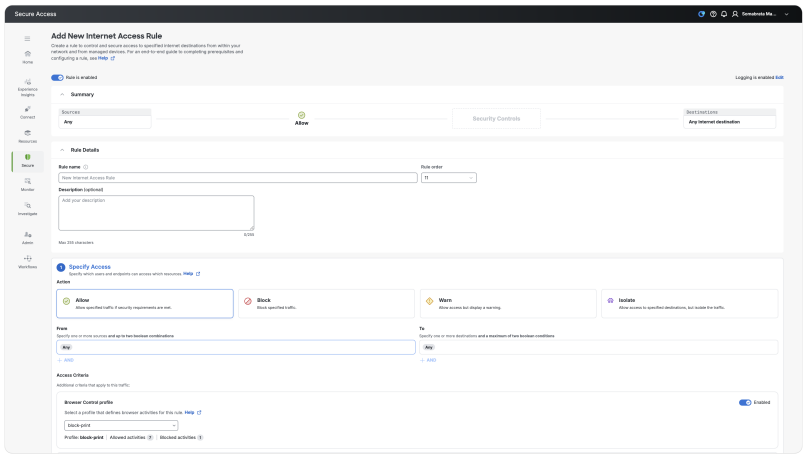
> **Note**
>
> For applicable activities, the editor also provides an option to **Add a mask** on each page.

d) **Save** the profile.

2. Attach the profile to an access rule:

a) Create an Access Rule. For more information, see Add an Internet Access Rule, Add a Private Access Rule and Manage the Access Policy.
b) Configure the applicable identities and destinations, choose an Allow or Warn access action, and attach the newly created Browser Control profile.





Note

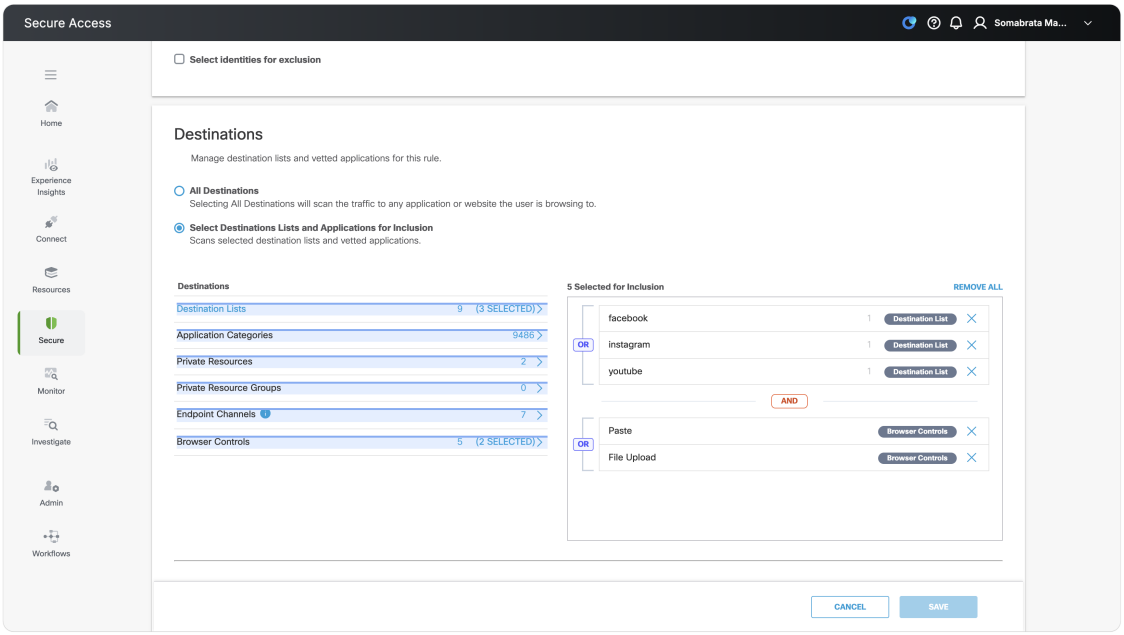
A Browser Control profile is not attached to a Block rule because the destination does not load. It is also not attached to an Isolate rule, which uses a separate proxy-based Remote Browser Isolation profile.

3. Configure content-aware Real Time DLP:
   a) Add a Real Time Rule to the Data Loss Prevention Policy. For more information, see Add a Real Time Rule to the Data Loss Prevention Policy.
   b) Provide a rule name and keep severity as Critical.
   c) Under **Destinations** > **Endpoint Channels**, select the browser channels for Cisco Secure Browser Extension that are available in your tenant.
   d) Under **Action**, select **Block** or **Monitor**.
   e) **Save** the rule.

Content Agnostic Browser Control Profile

About Content-agnostic Browser Control Profile

An administrator creates a reusable Browser Control profile and chooses the website-based outcome for each protection feature. The Browser Control profile is attached to an applicable Secure Access access policy for Internet or private-app access.



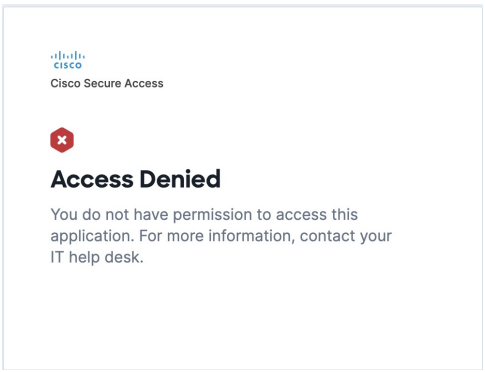
The access policy supplies source and destination matching, such as user, website, category, or app. The Browser Control profile supplies the additional browser action protection. Browser Control profiles can be attached to access policies whose action is Allow or Warn. They are not attached to Block policies, where the page does not load, or Isolate policies, which use separate proxy-based Remote Browser Isolation.

See Cisco Secure Access Manage the Access Policy for the shared access-policy workflow.

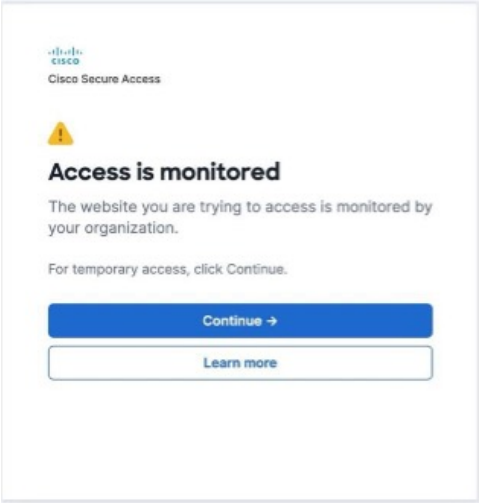
Content-Aware Real Time DLP rule

The applicable DLP entitlement is required. In the Data Loss Prevention Policy, an administrator selects supported browser endpoint channels in the existing Real Time DLP rule destinations configuration. The rest of this guide uses Real Time DLP as the short name. Supported content-aware outcomes are:

- **Block**: stop the protected action.



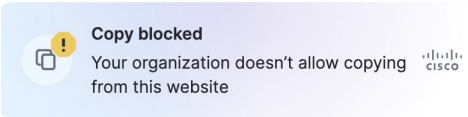
- **Monitor**: allow the action, display a non-blocking warning and record the activity for administrator preview. The toast does not require acknowledgement.



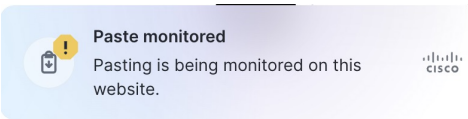
Browser Action Protection Enforcements

The Browser Action Protection Enforcements include:

- **Copy Block**

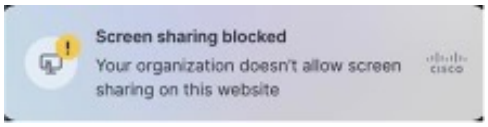


- **Paste Block**



> **Note**
>
> Paste and input enforcements are excluded and won't be intercepted/blocked for credential like fields e.g. e-mail and password, to allow you to authenticate websites.

- **Screenshare Block**



Note

Print and screenshot actions are Operating System-dependent. The system monitors pre-defined key combinations for these:

For macOS:

- Print: Cmd+P
- Screenshot: Cmd+Shift+3 / +4 / +5, Cmd+Shift+S, plus the Cmd+Shift prefix chord

For Windows:

- Print: Ctrl+P
- Screenshot: PrintScreen, Win+Shift, Ctrl+Shift+S

View Reports

View Reports for Secure Browser Extension using Access Policy or DLP Policy

Procedure

1. For Access Policy Reporting, navigate to **Monitor** > **Reports** > **Events**.

   Note

   - For more information, see Events Reports.
   - Private access is part of ZTA client-less; Internet access is part of proxy/SWG.

2. For DLP Policy Reporting, navigate to **Monitor** > **Reports** > **Data Loss Prevention**.

   For more information, see Data Loss Prevention Report.

45 Data Classifications

Topics:

- Manage Data Classifications
- Create a Data Classification
- Copy and Customize a Built-In Data Classification
- Delete or Edit a Classification
- Exact Data Match Identifiers
- Indexed Document Match Identifiers
- Built-In Data Classifications

Provides an overview of Data Classifications in Cisco Secure Access, including Manage Data Classifications, Create a Data Classification, and Copy and Customize a Built-In Data Classification. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Data Classifications

Describes Manage Data Classifications in Cisco Secure Access. The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy.

The Data Loss Prevention (DLP) policy monitors or blocks content based on the rules configured for the policy. The rules use *data identifiers* and *data classifications*, which describe the type of data to be monitored or blocked. The file and form types supported by the DLP policy are listed here.

Data identifiers describe the content the Data Loss Prevention Policy monitors or blocks. Data identifiers can describe Personal Information Identifiers (PII) that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. Data identifiers can also describe certain content an organization may wish to monitor or block within its network traffic, such as discriminatory or aggressive content. Secure Access provides a collection of built-in data identifiers (see Built-in Data Identifiers and Individual Data Identifiers), and you can create custom identifiers based on the built-in data identifiers (see Copy and Customize a Data Identifier).

Data classifications are groups of data identifiers combined for the purpose of monitoring or blocking closely related content. For example, you can create a data classification that encompasses medically related content by including the built-in identifiers for ICD codes, drug names, prescription names, health conditions, and national drug code names. The classification, when applied to a rule in the Data Loss Prevention Policy, will monitor or block content matching those identifiers.

Using the inclusion and exclusion options on the Data Classification page, you can fine-tune your classification to be more precise and reduce false positives. You can exclude specific terms and regular expression (regex) patterns by creating a custom identifier in the exclusion area, or by excluding a pre-existing built-in identifier.

The exclusion applies only to the content that's been matched, not to every document that meets the exclusion criteria.

For example, consider a data classification that targets the built-in identifier Health Condition and Person Name (US). You want to block instances of "John Smith cancer" while allowing instances of "John Smith cancer fundraising." To achieve this, you can craft a custom data identifier for "cancer fundraising" and set up an exclusion for this identifier within your data classification. As a result, matches for the Health Condition and Person Name (US) identifier will be flagged, except when the phrase "cancer fundraising" is present.

The system compares data identifiers selected for exclusion against both the keywords and the proximity terms of included data identifiers. If the Data Loss Prevention Report reveals that a particular rule or identifier is generating false positives, consider using terms and identifiers exclusion to remedy the situation.

> **Note**
>
> If you select a data identifier for both inclusion and exclusion, exclusion will take precedence.

There are three ways to establish a data classification to apply to a data loss prevention rule:

- You can create a custom data classification entirely of your own design. (See Create a Data Classification.)
- You can create a custom data classification based on a built-in data classification provided by Secure Access. (See Copy and Customize a Built-In Data Classification).
- You can apply a built-in data classification provided by the system.

Secure Access provides four different built-in data classifications. You can apply these directly to your DLP rules or copy them and customize the copies to create your own data classifications. Each of the built-in data classifications has a different set of built-in data identifiers associated with it. The four pre-defined data classifications are described in Built-In Data Classifications.

Create a Data Classification

Describes Create a Data Classification in Cisco Secure Access. You can create a data classification to help you monitor content with specific characteristics.

You can create a data classification to help you monitor content with specific characteristics. Custom data classifications can be used in real time rules, SaaS API rules and discovery scans.

The building blocks for data classifications are data identifiers. The data identifiers that you choose for a data classification determine the type of data for which rules using that data classification will scan.

Using the inclusion and exclusion options on the Data Classification page, you can fine-tune your classification to be more precise and reduce false positives. You can exclude specific terms and regular expression (regex) patterns by creating a custom identifier in the exclusion area, or by excluding a pre-existing built-in identifier.

The exclusion applies only to the content that's been matched, not to every document that meets the exclusion criteria.

For example, consider a data classification that targets the built-in identifier Health Condition and Person Name (US). You want to block instances of "John Smith cancer" while allowing instances of "John Smith cancer fundraising." To achieve this, you can craft a custom data identifier for "cancer fundraising" and set up an exclusion for this identifier within your data classification. As a result, matches for the Health Condition and Person Name (US) identifier will be flagged, except when the phrase "cancer fundraising" is present.

The system compares data identifiers selected for exclusion against both the keywords and the proximity terms of included data identifiers. If the Data Loss Prevention Report reveals that a particular rule or identifier is generating false positives, consider using terms and identifiers exclusion to remedy the situation.

> **Note**
>
> If you select a data identifier for both inclusion and exclusion, exclusion will take precedence.

The system offers two types of built-in data identifiers you can choose from:

Built-In Identifiers

These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

Machine Learning Identifiers

These identify data based on AI analysis of example documents. For example, the identifier for Patent Files has been trained to recognize documents that are likely patent applications. For more information, see Built-In Data Identifiers.

The system offers three types of data identifiers you can create yourself applying different methods of data analysis:

Custom Identifiers

You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier .

Exact Data Match Identifiers

Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

Indexed Document Match Identifiers

Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

To delete or edit a data classification, see Delete or Edit a Classification.

Procedure for Creating a Data Classification

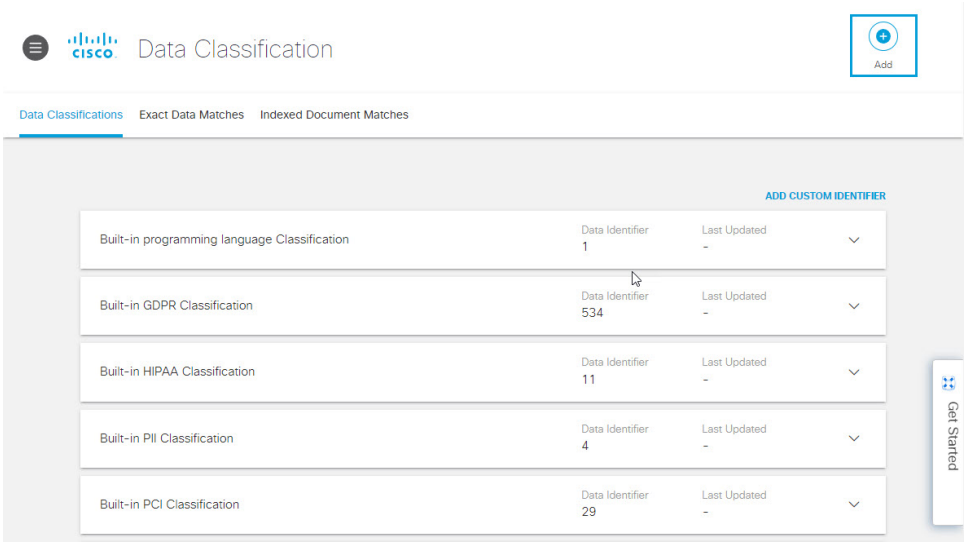
Provides instructions for completing the Procedure for Creating a Data Classification workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

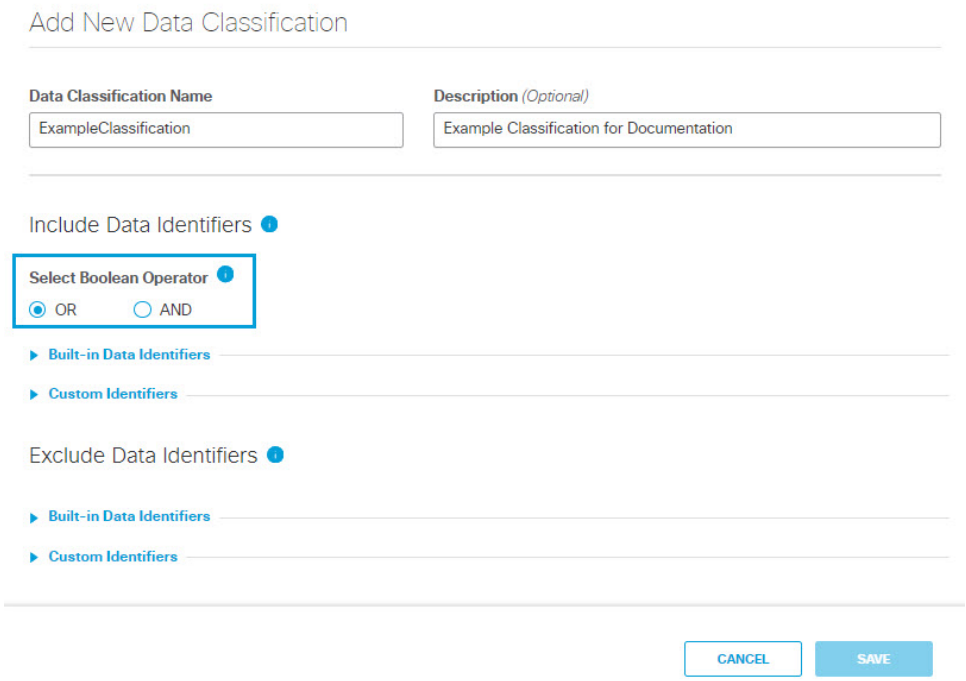
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Data Loss Prevention Classifications** > **Data Classification** and click **Add**.



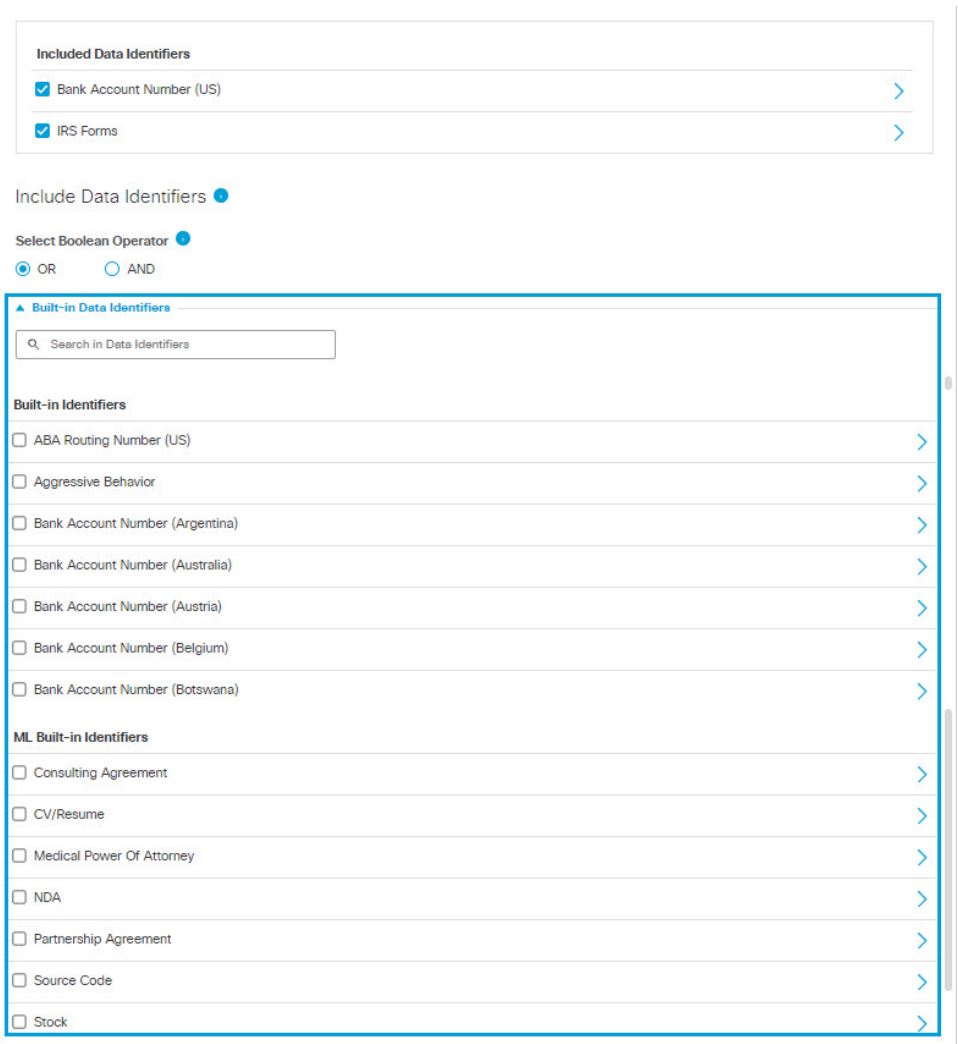
2. Give your classification a meaningful name and description.
3. Under **Include Data Identifiers**, select a Boolean operator to separate the identifiers included in the classification.
   - **OR**–At least one of the data identifiers included must match during rule evaluation.
   - **AND**–All of the data identifiers included must match during rule evaluation.



4. Under **Include Data Identifiers**, expand **Built-in Data Identifiers** and select data identifiers to include in the data classification.

   Choose from:

   - Built-In Identifiers
   - ML (Machine Learning) Built-In Identifiers



5. Under **Include Data Identifiers**, expand **Custom Identifiers** and select custom identifiers to include in the data classification.

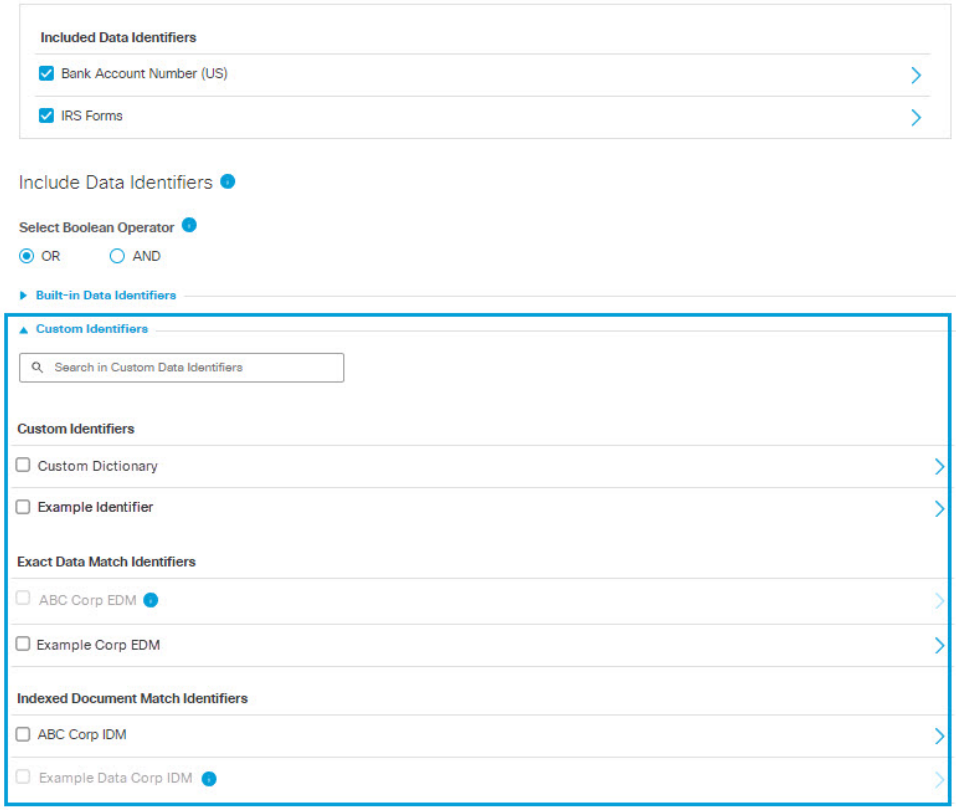
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

   > **Note**
   >
   > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)

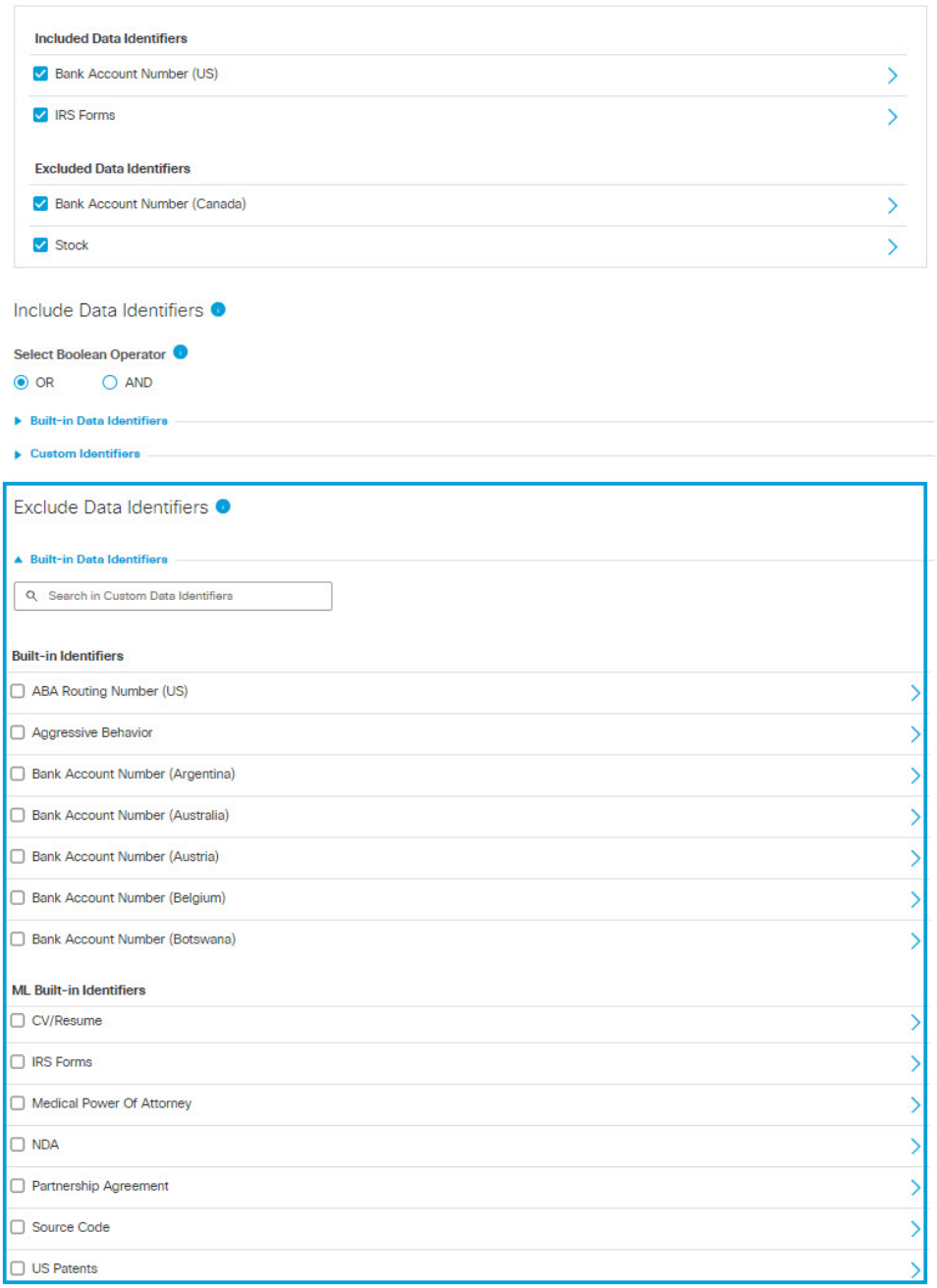


For OCR-related use cases, select the custom identifiers created for the languages or terms you want DLP to detect in image content.

6. Under **Exclude Data Identifiers**, expand**Built-in Data Identifiers** and choose data identifiers to exclude from the data classification.

   Choose from:

   - Built-In Identifiers
   - ML (Machine Learning) Built-In Identifiers



7. Under **Exclude Data Identifiers**, expand **Custom Identifiers** and choose custom data identifiers to exclude from the data classification.

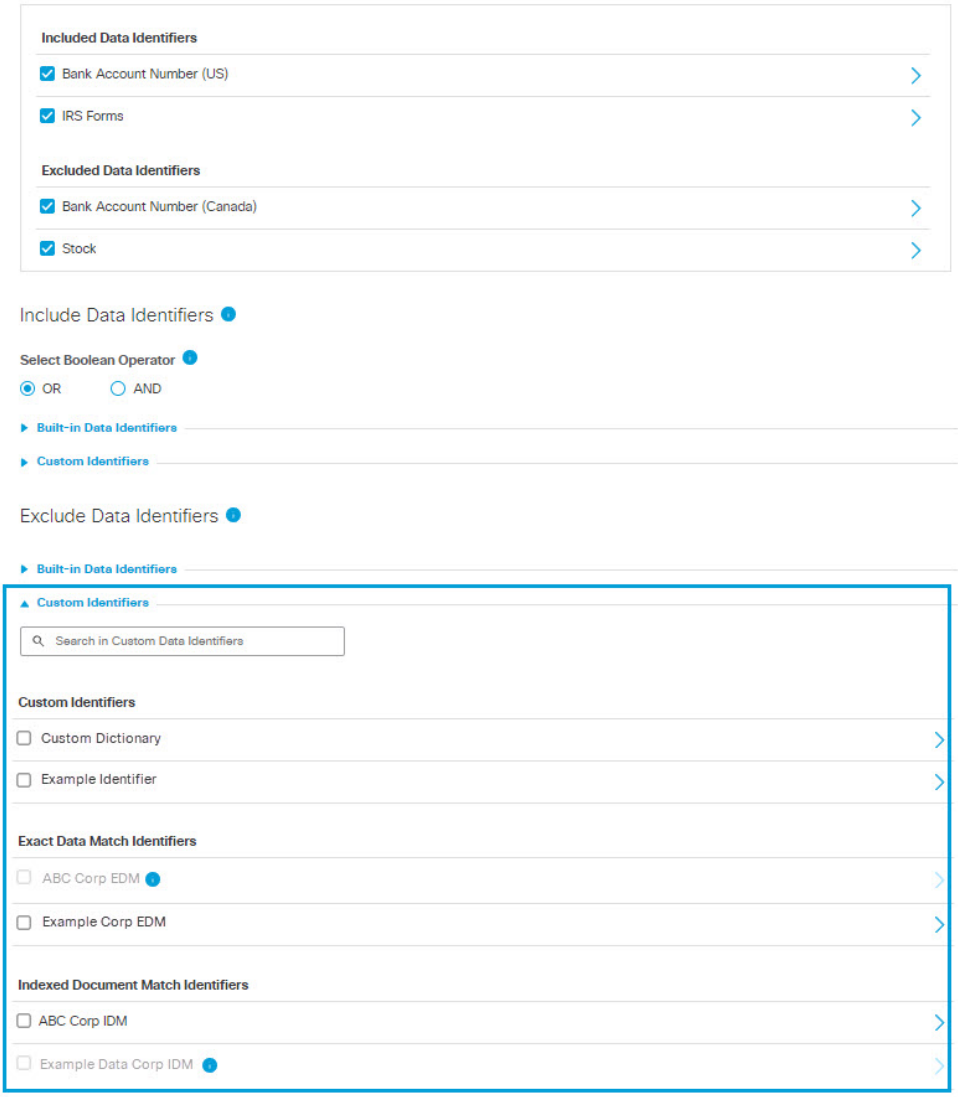
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

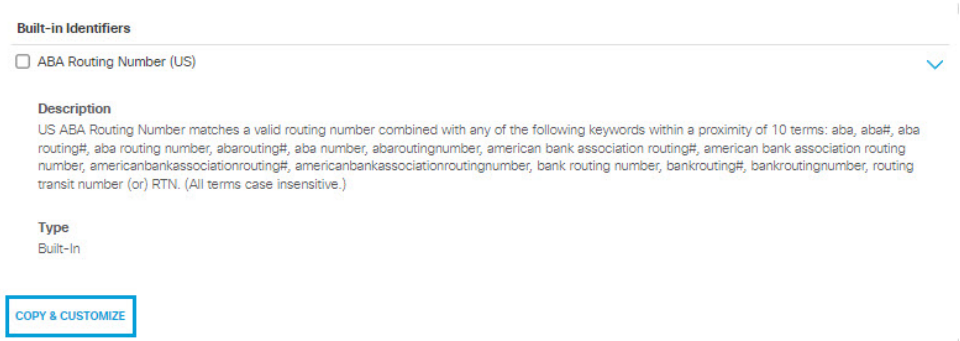
> **Note**
>
> Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

- Indexed Document Match Identifiers

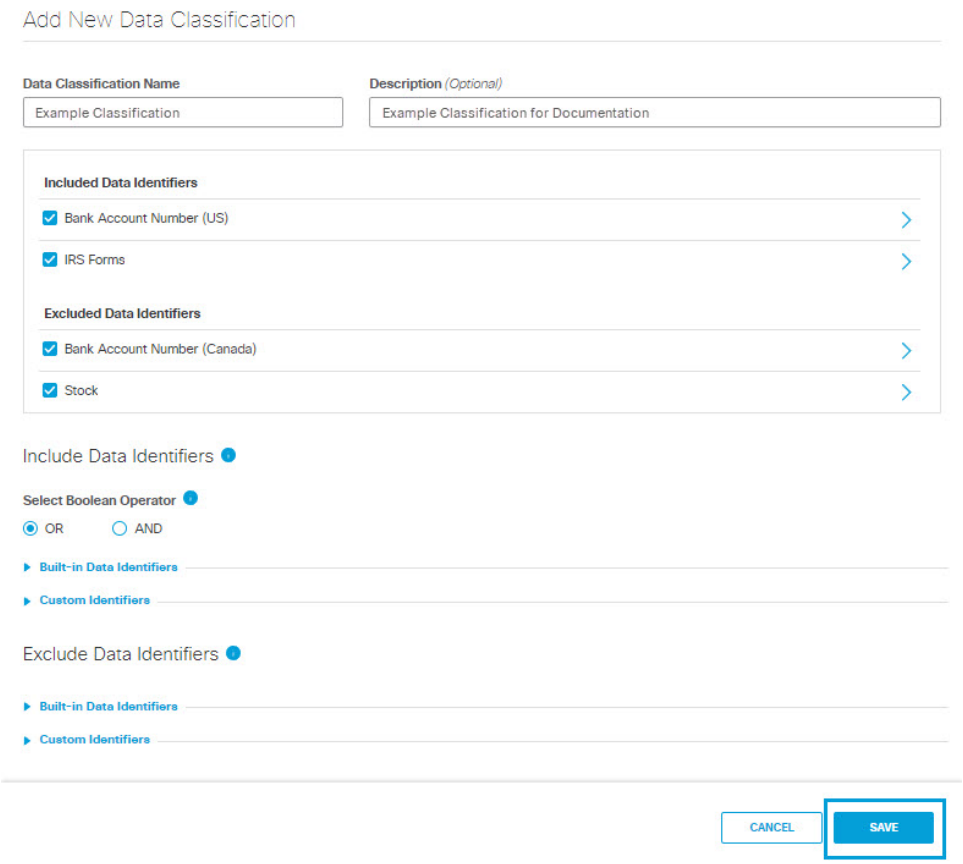
> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



8. You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.

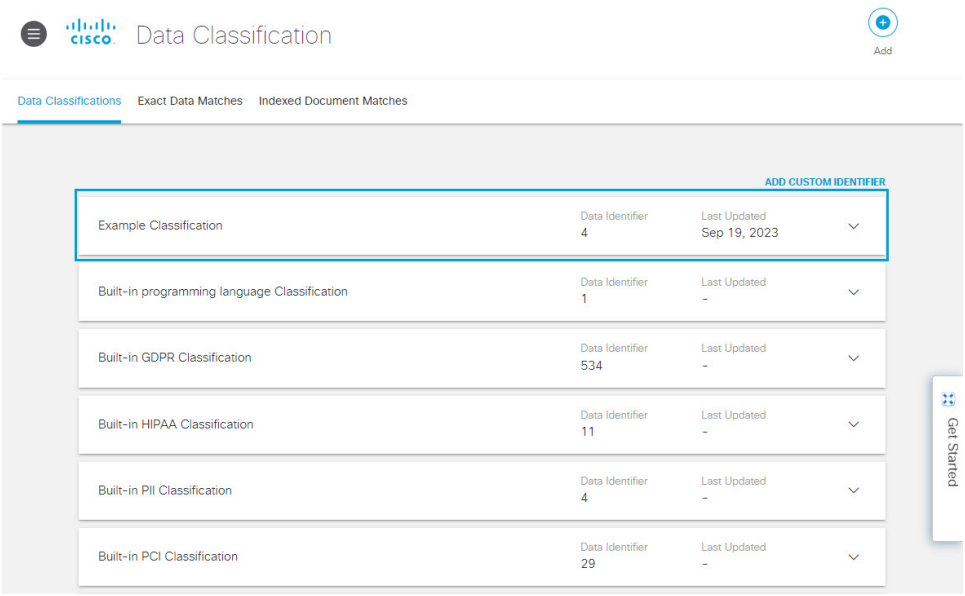


9. Click **Save**.



What to do next

Your new classification is listed on the Data Classification page, and will be available to you when you Add a Real Time Rule to the Data Loss Prevention Policy, Add a SaaS API Rule to the Data Loss Prevention Policy, or initiate a new Discovery Scan.



For multilingual OCR use cases, you can create separate classifications for each language or combine multiple language-specific identifiers into a single classification, depending on how you want the policy to be applied.

Copy and Customize a Built-In Data Classification

Describes Copy and Customize a Built-In Data Classification in Cisco Secure Access. The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans.

The system provides four different built-in data classifications you can use in real time rules, SaaS API rules, and discovery scans. These are:

PII Data Classification

Personal Information Identifiers; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers.

PCI Data Classification

Data related to the Payment Card Industry.

GDPR Data Classification

Common personal data associated with the European Union's General Data Protection Regulation. Customers can use these identifiers to support GDPR compliance within their organizations.

HIPAA Data Classification

Describes HIPAA Data Classification in Cisco Secure Access. Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act.

Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act. Customers can use these identifiers to support HIPAA compliance within their organizations.

For more details on each of these built-in data classifications, see Built-In Data Classifications. You can create custom data classifications based on any of these built-in data classifications. Simply copy the desired built-in classification, make changes to the copy, and save it as a custom data classification.

The building blocks for data classifications are data identifiers. The data identifiers selected for a data classification determine the type of data for which rules using that data classification will scan. Built-in data classifications have data identifiers already selected for them; you can produce your own customized versions of these classifications by removing selected identifiers or adding other identifiers.

Using the inclusion and exclusion options on the Data Classification page, you can fine-tune your classification to be more precise and reduce false positives. You can exclude specific terms and regular expression (regex) patterns by creating a custom identifier in the exclusion area, or by excluding a pre-existing built-in identifier.

The exclusion applies only to the content that's been matched, not to every document that meets the exclusion criteria.

For example, consider a data classification that targets the built-in identifier Health Condition and Person Name (US). You want to block instances of "John Smith cancer" while allowing instances of "John Smith cancer fundraising." To achieve this, you can craft a custom data identifier for "cancer fundraising" and set up an exclusion for this identifier within your data classification. As a result, matches for the Health Condition and Person Name (US) identifier will be flagged, except when the phrase "cancer fundraising" is present.

The system compares data identifiers selected for exclusion against both the keywords and the proximity terms of included data identifiers. If the Data Loss Prevention Report reveals that a particular rule or identifier is generating false positives, consider using terms and identifiers exclusion to remedy the situation.

Note

If you select a data identifier for both inclusion and exclusion, exclusion will take precedence.

The system offers two types of built-in data identifiers you can choose to remove from or add to your customized version of a built-in data classification:

- Built-In Identifiers

  These identify data using pattern matching and dictionary lookups. The descriptions shown in the GUI provide details about the type of data they match. For more information, see Built-In Data Identifiers.

- Machine Learning Identifiers

  These identify data based on AI analysis of example documents. For example, the identifier for Patent Files has been trained to recognize documents that are likely patent applications. For more information, see Built-In Data Identifiers.

The system offers three types of data identifiers you can create yourself applying different methods of data analysis. You can add these to your customized version of a built-in data classification:

- Custom Identifiers

  You can create custom identifiers to match specific terms and pattern expressions of your choosing. See Create a Custom Identifier .

- Exact Data Match Identifiers

  Exact Data Match Identifiers use fingerprinting to identify data in structured documents that match criteria you define. (See Create an Exact Data Match Identifier for more information.)

- Indexed Document Match Identifiers

  Indexed Document Match Identifiers use fingerprinting to identify data in unstructured documents that match criteria you define. See Create an Indexed Document Match Identifier for more information.

To delete or edit a data classification, see Delete or Edit a Classification.

Procedure for Copy and Customize a Built-In Data Classification

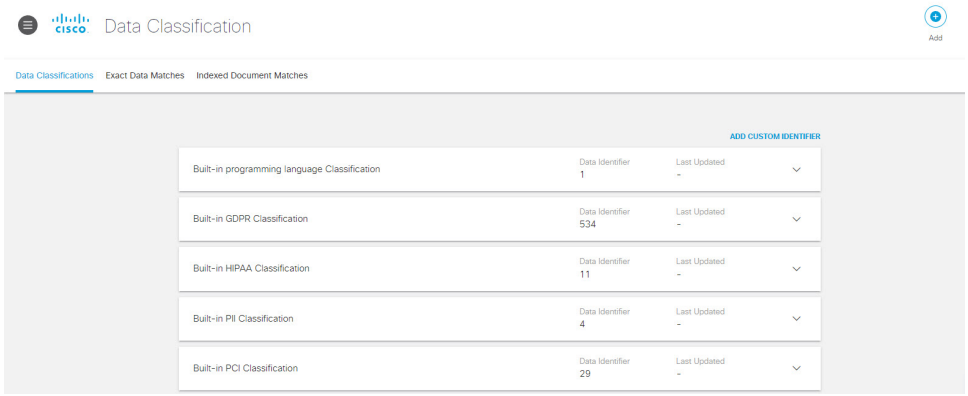
Provides instructions for completing the Procedure for Copy and Customize a Built-In Data Classification workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

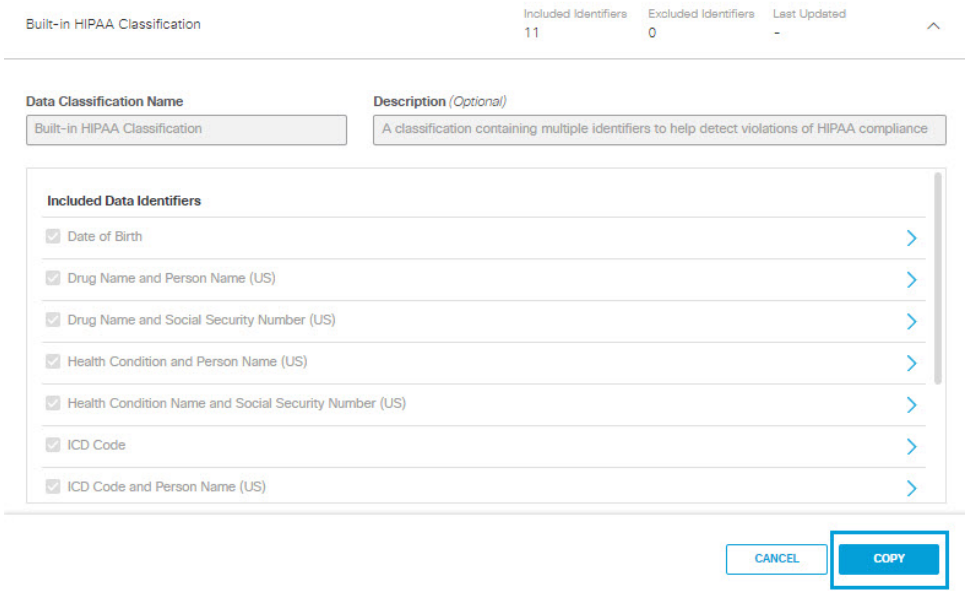
- Full Admin user role. For more information, see Manage Accounts.

Procedure

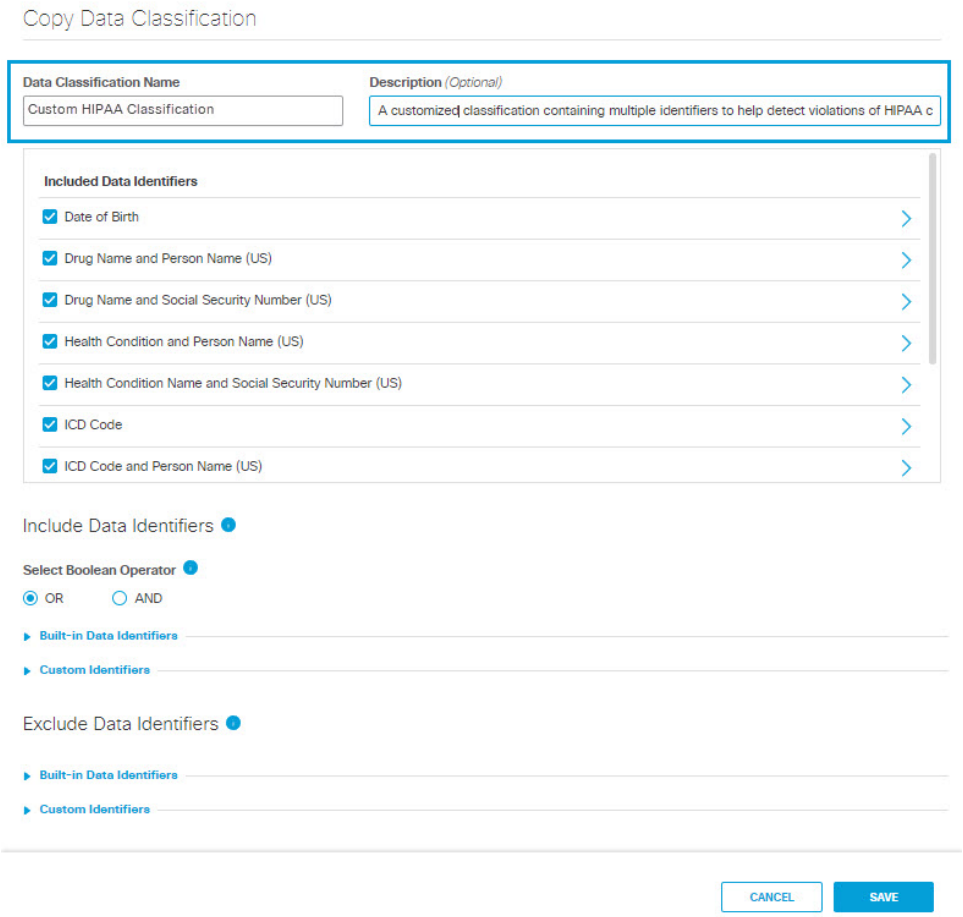
1. Navigate to **Secure** > **Settings** > **Data Loss Prevention Classifications** > **Data Classification**.



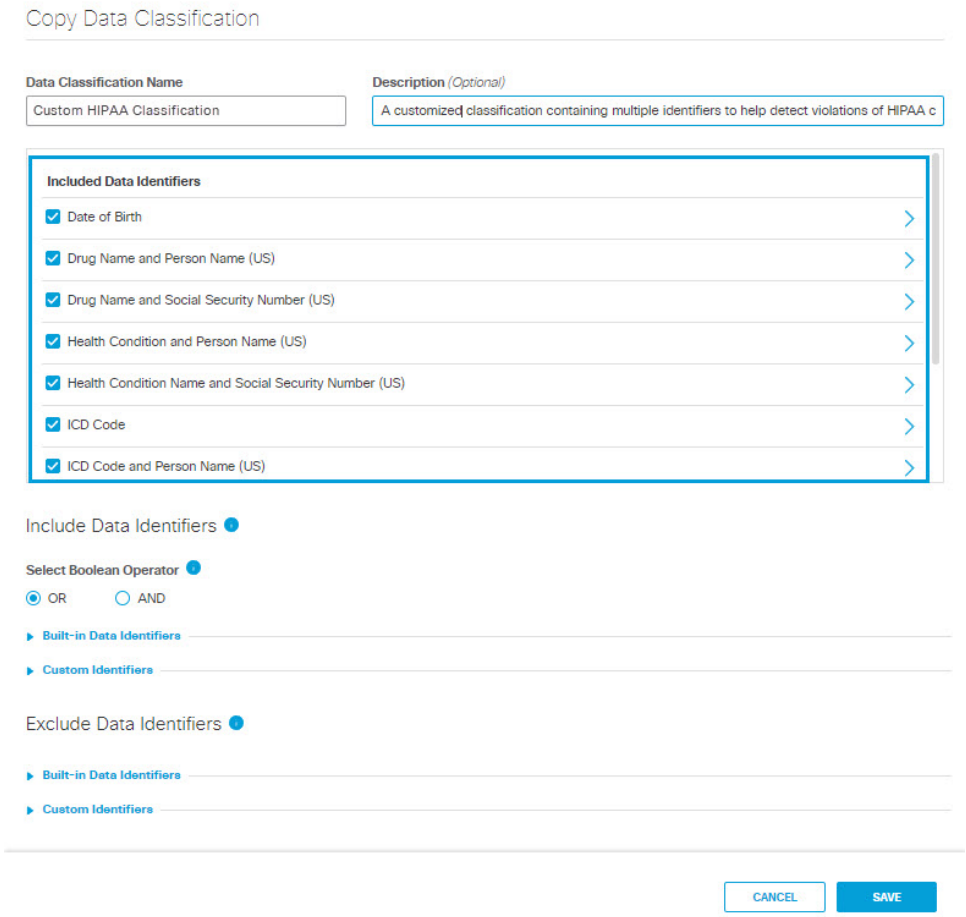
2. Expand one of the built-in data classifications and click **Copy**.



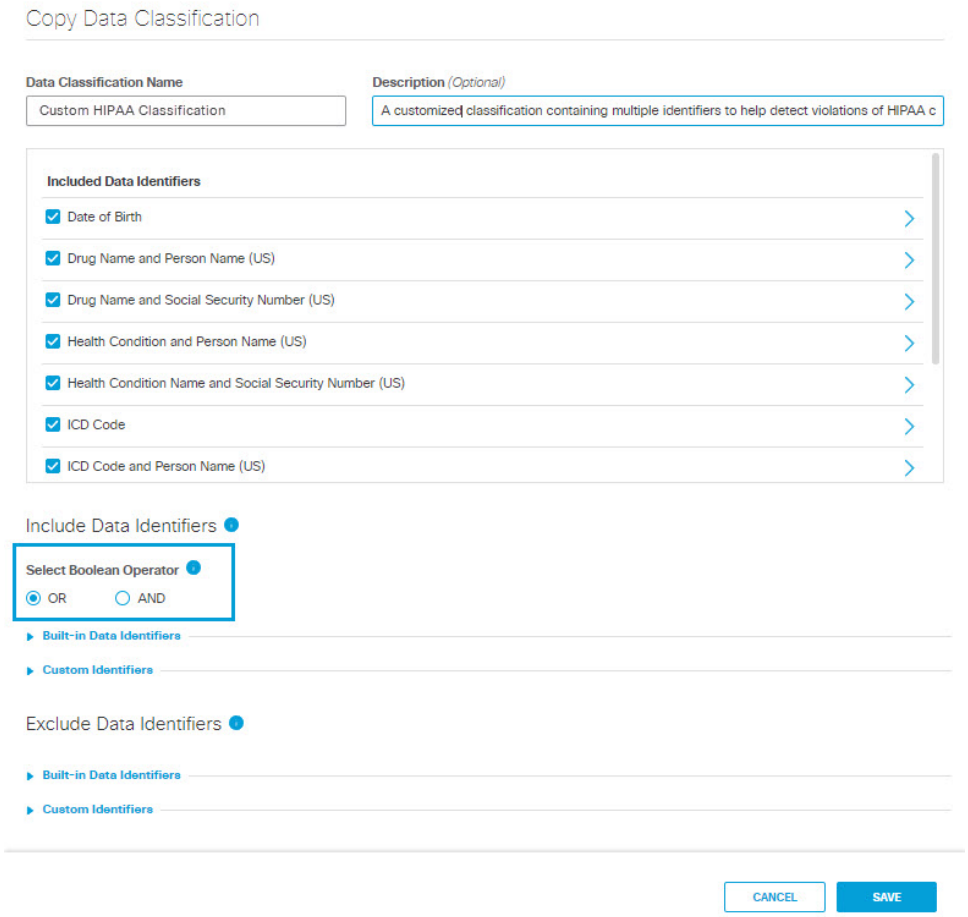
3. Give the new data classification a meaningful name and description.



4. Under **Included Data Identifiers** deselect pre-selected data identifiers as needed.



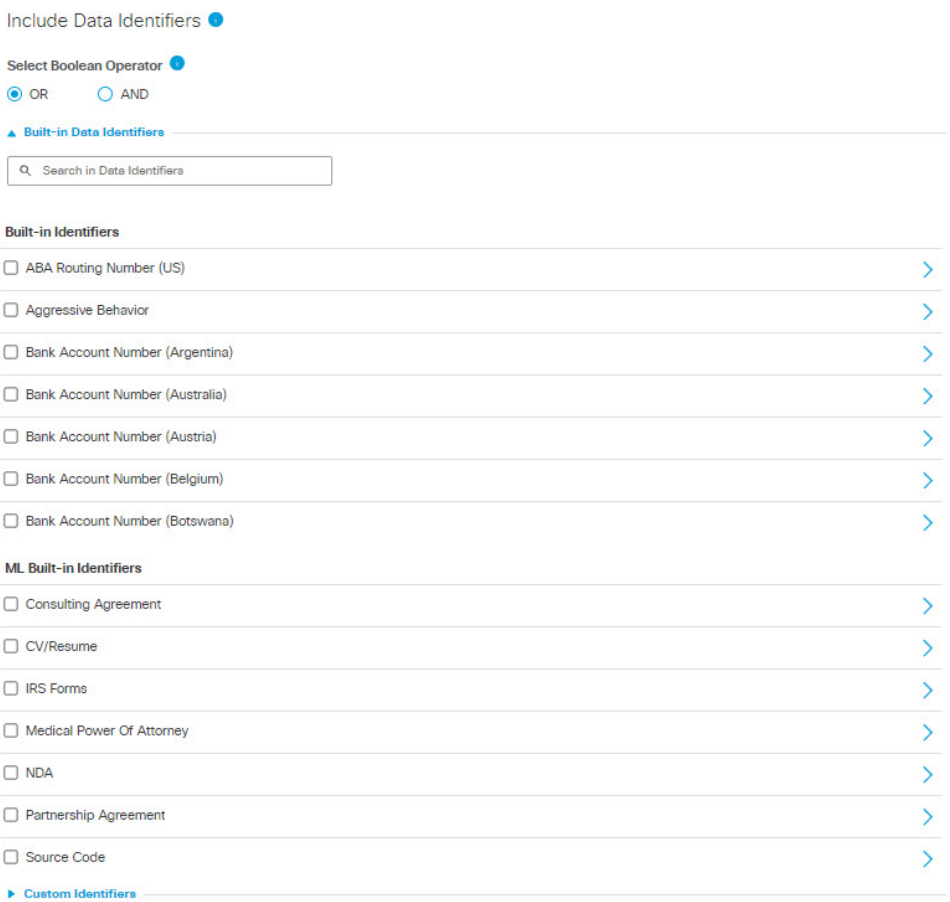
5. Under **Include Data Identifiers**, you may change the Boolean operator to separate the identifiers included in the classification:
   - **OR**–At least one of the data identifiers selected must match during rule evaluation.
   - **AND**–All of the data identifiers selected must match during rule evaluation.



6. Under **Include Data Identifiers**expand **Built-in Data Identifiers** and select additional data identifiers to include in the data classification.

   Choose from:

   - Built-In Identifiers
   - ML (Machine Learning) Built-In Identifiers



7. Under **Include Data Identifiers** expand **Custom Identifiers** and select custom data identifiers to include in the data classification.

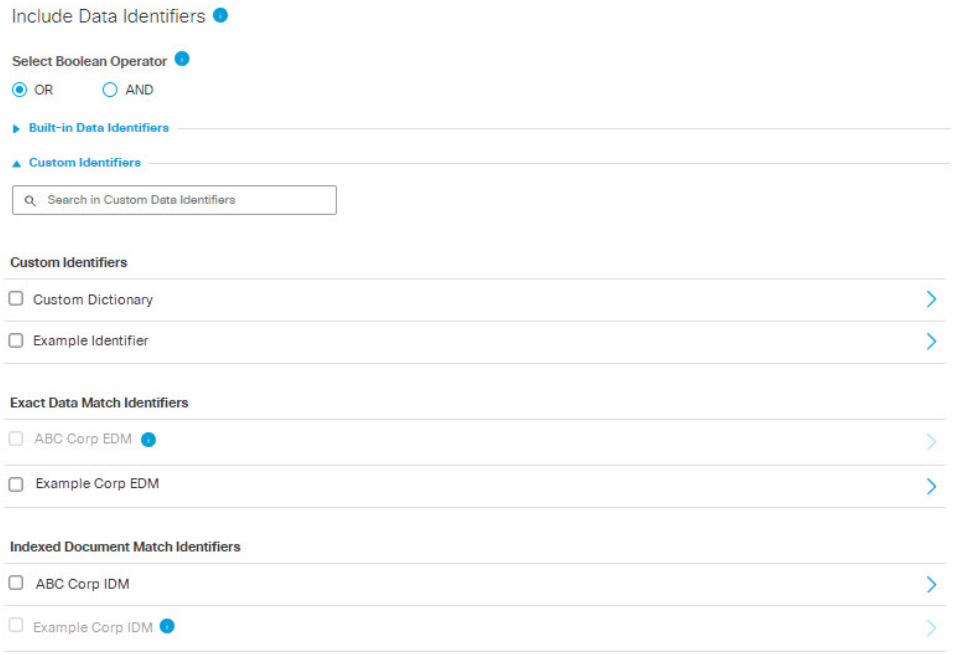
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

     > **Note**
     >
     > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

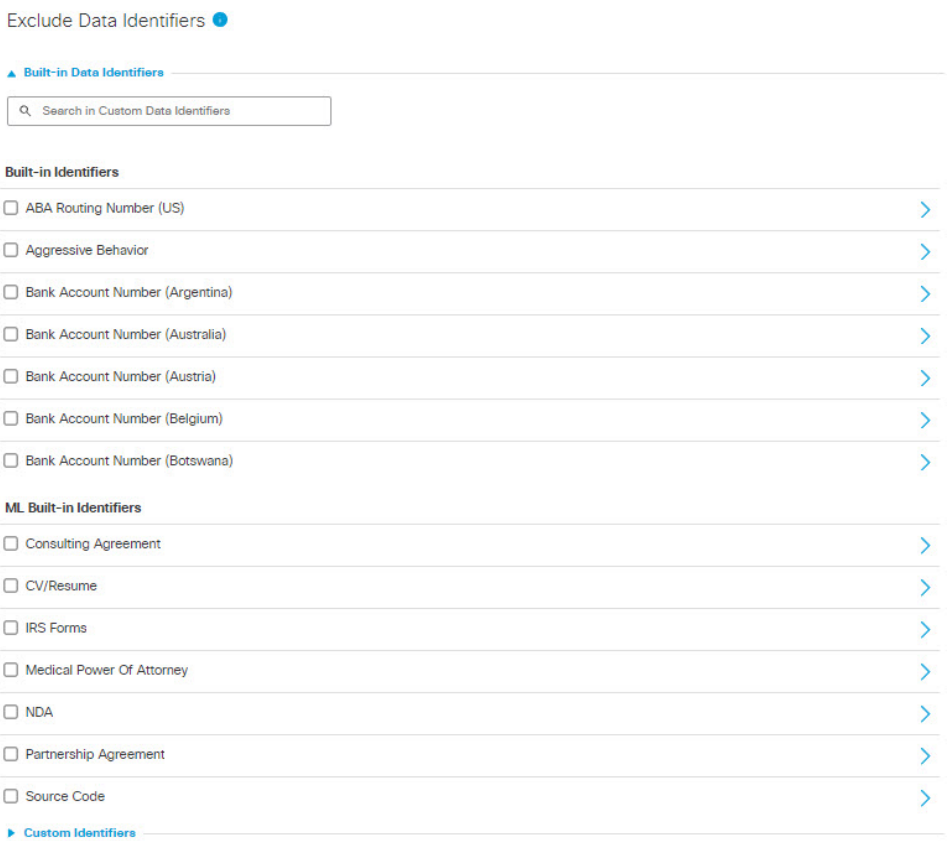
> **Note**
>
> Index Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



8. Under **Exclude Data Identifiers**, expand **Built-in Data Identifiers** and choose data identifiers to exclude from the data classification.

   Choose from:

   - Built-In Identifiers
   - ML (Machine Learning) Built-In Identifiers



9. Under **Exclude Data Identifiers**, expand **Custom Identifiers** and choose custom data identifiers to exclude from the data classification.

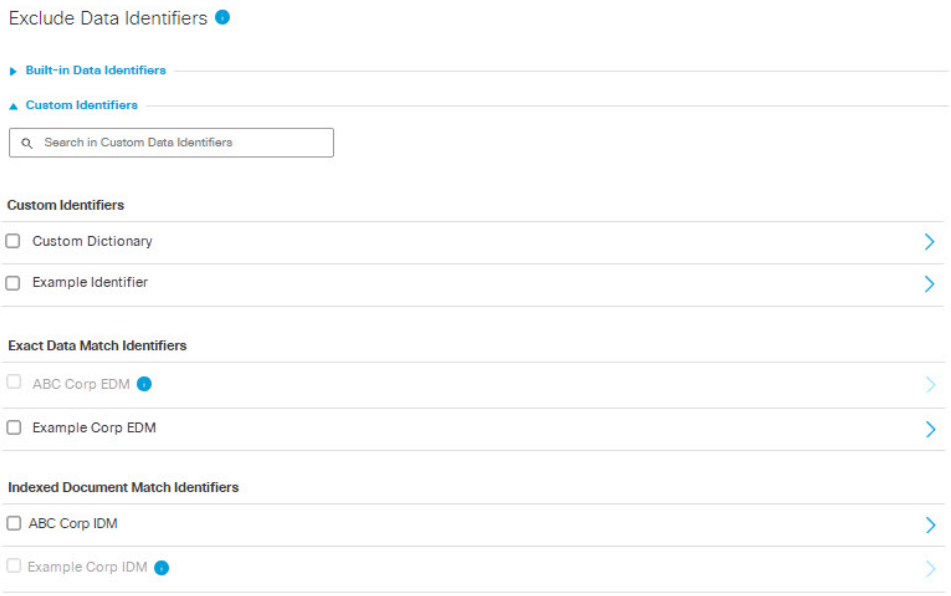
   Choose from:

   - Custom Identifiers
   - Exact Data Match Identifiers

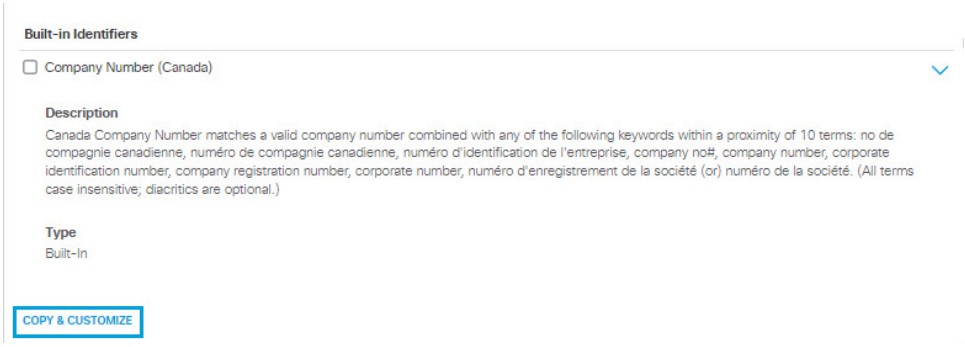
   > **Note**
   >
   > Exact Data Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Exact Data Match Identifier for more information.)

   - Indexed Document Match Identifiers

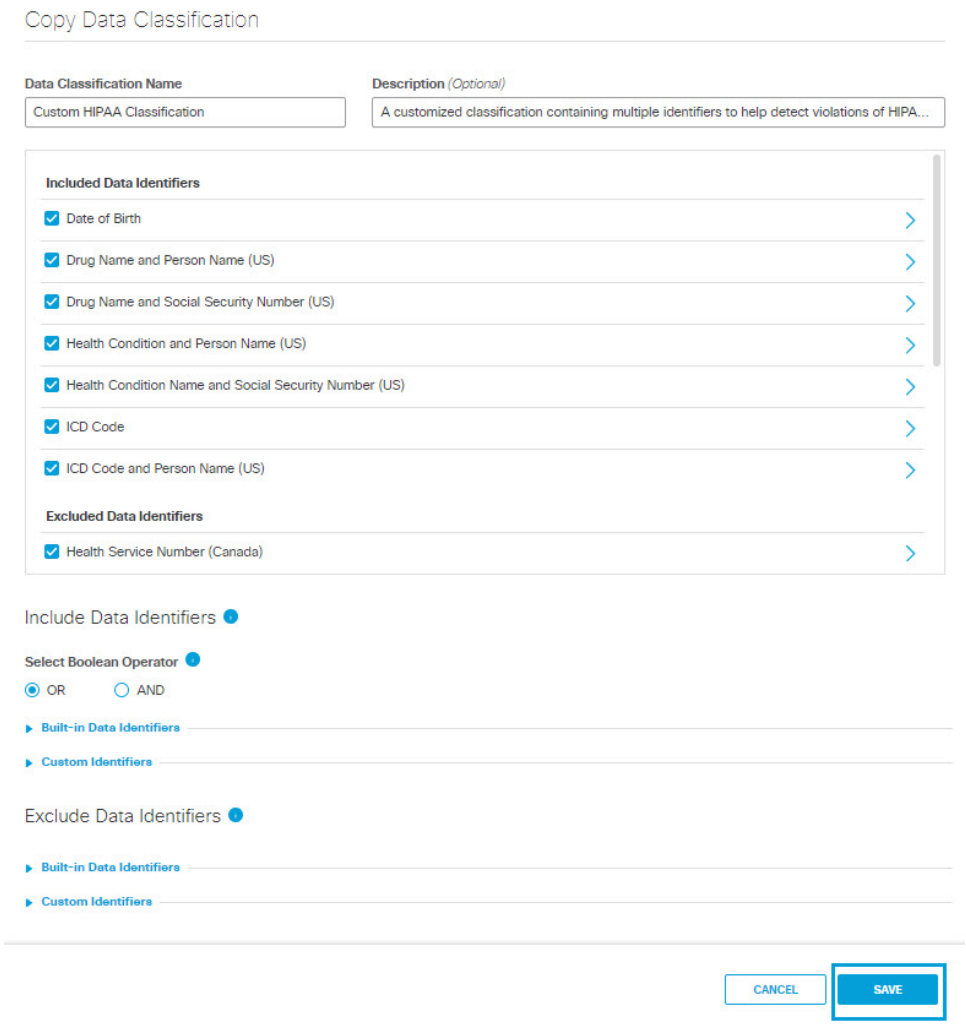
> **Note**
>
> Indexed Document Match Identifiers that are greyed out have not yet been indexed and may not be selected. (See Create an Indexed Document Match Identifier for more information.)



10. You may expand any built-in data identifier and click **COPY & CUSTOMIZE** to create a new customized data identifier. See Copy and Customize a Data Identifier.

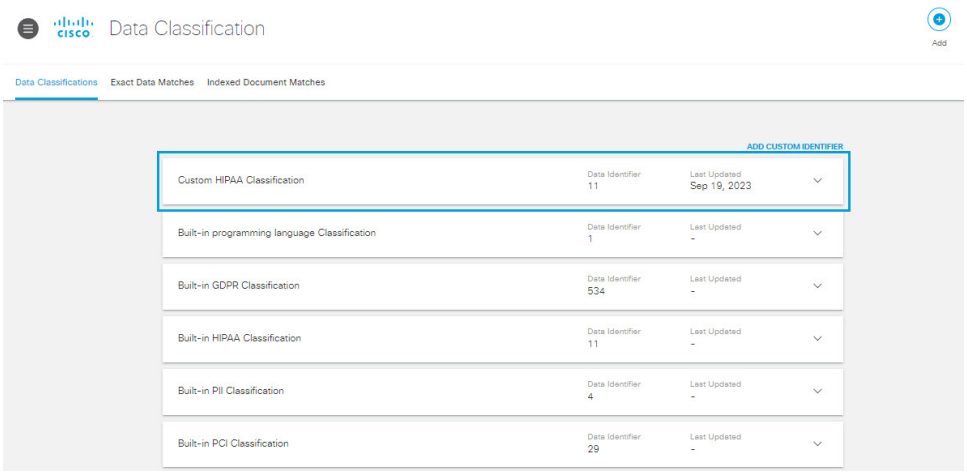


11. Click **Save**.



What to do next

Your new classification is listed on the Data Classification page, and will be available to you when you Add a Real Time Rule to the Data Loss Prevention Policy, Add a SaaS API Rule to the Data Loss Prevention Policy, or initiate a new Discovery Scan.



Delete or Edit a Classification

Describes Delete or Edit a Classification in Cisco Secure Access. After adding a data classification, you can delete or edit it at any time.

After adding a data classification, you can delete or edit it at any time. To add a data classification, see Add a Data Classification or Copy and Customize a Built-In Data Classification.

> **Note**
>
> You cannot edit or delete a built-in data classification.

Prerequisites

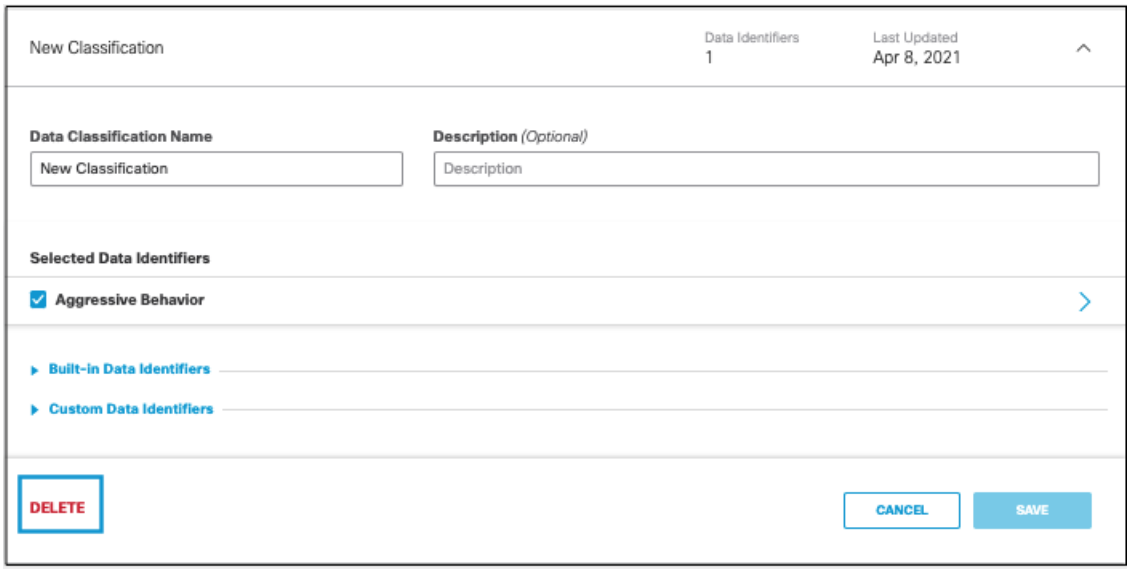
- Full Admin user role. For more information, see Manage Accounts.

Delete a Classification

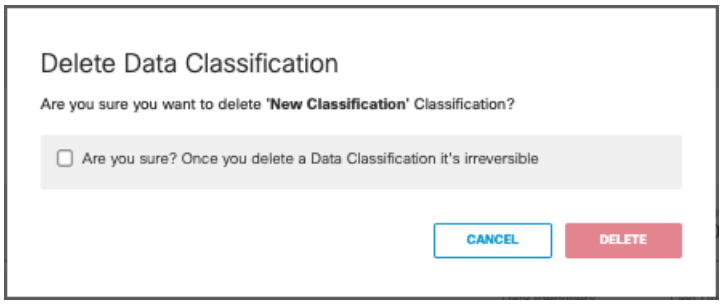
Provides instructions for completing the Delete a Classification workflow in Cisco Secure Access. Navigate to Secure Settings Data Loss Prevention Classifications .

Procedure

1. Navigate to **Secure** > **Settings** > **Data Loss Prevention Classifications**.
2. Expand a data classification and click **Delete**.



3. Confirm deleting the classification and then click **Delete**.



Edit a Classification

Provides instructions for completing the Edit a Classification workflow in Cisco Secure Access. You may not edit a built-in data classification.

> **Note**
>
> You may not edit a built-in data classification.

Procedure

1. Navigate to **Secure** > **Settings** > **Data Loss Prevention** > **Classifications**.
2. Expand a data classification.
3. Edit the data classification as needed and click **Save**.

Exact Data Match Identifiers

Provides instructions for completing the Exact Data Match Identifiers workflow in Cisco Secure Access. Exact Data Matching (EDM) is a data classification and matching technique that effectively detects data loss incidents involving sensitive records maintained and stored in a structured data format.

Exact Data Matching (EDM) is a data classification and matching technique that effectively detects data loss incidents involving sensitive records maintained and stored in a structured data format. EDM is designed to help protect sensitive data by fingerprinting data instead of leveraging pattern matching techniques.

Secure Access performs Exact Data Matching using an EDM template, which you create by uploading a plain text CSV file that describes the fields to be matched, and choosing an EDM type for each field described in the CSV file. You must also specify which fields are required for a match, and their priority. Once the EDM template is created, you will obtain an ID for it from Secure Access.

You must then download the DLP indexer and run the indexer against your data records using the EDM template. The DLP indexer validates records against the template and generates hash fingerprints for those records, creating an EDM.

Once you have run the indexer, you will have an Exact Data Match Identifier associated with the documents. You will then be able to:

Procedure

1. Create a Data Classification that uses the EDM as a custom data identifier (as described in Create a Data Classification or Copy and Customize a Built-In Data Classification).
2. Create a DLP rule that uses the Data Classification including that EDM Identifier. (For more information on DLP rules, see Manage the Data Loss Prevention Policy.)

What to do next

With these configurations in place, Secure Access can monitor and/or block transmission of structured files containing records that match your indexed data. Matching records meet the criteria you establish when you create the EDM template.

Prerequisites for Exact Data Match Identifiers

Describes Prerequisites for Exact Data Match Identifiers in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- The template CSV you upload must meet the following requirements:
  - The file can not be larger than 10 KB.
  - The second and ensuing rows may contain sample data; be aware, however, that this data will not be indexed unless it also appears in the source data CSV file.
- The DLP indexer supports data files with up to 55 million records. The exact records limit is determined by the total number of columns and the number of those are of Alphanumeric type. The indexer displays the exact limit when attempting to load a file that exceeds it. If your dataset is larger than the limit, you need to split the records into multiple files. For errors received when indexing a large file, see Memory Tuning for DLP Exact Data Matching Indexer.
- Both the template and source data CSV files must meet the following requirements:
  - A multi-term (multi-word) field can contain a maximum of 6 space-separated words.

- The data file must contain only 1 byte or 2 byte UTF-8 encoded characters.
- The first row of data must have between 1 and 50 fields and each row must have the same number of fields.
- The first row of data must specify the name of each field, and each value must be unique.
- Data in the second and ensuing rows must comply with the EDM field types and supported formats (see Exact Data Match Field Types).
- The field names in the sample data template must match the field names in the actual data source file. The field names must appear in the same order in both files.

Caution

Do *not* create, edit, or view the template or source data CSV file using Microsoft Excel, as this may corrupt the file. Use a text editor.

Note

If any of the values provided in the source file to the DLP indexer fail to be validated as per the supported format, then the DLP indexer will skip that record and proceed with indexing the remaining records. The indexer also behaves in this manner for any records that may exceed the template-defined fields, and for empty rows or records with empty primary values. The position of the skipped records in the file will be provided as part of the output of the DLP indexer.

The following procedure uses the following example CSV file for both the template and indexed source data:

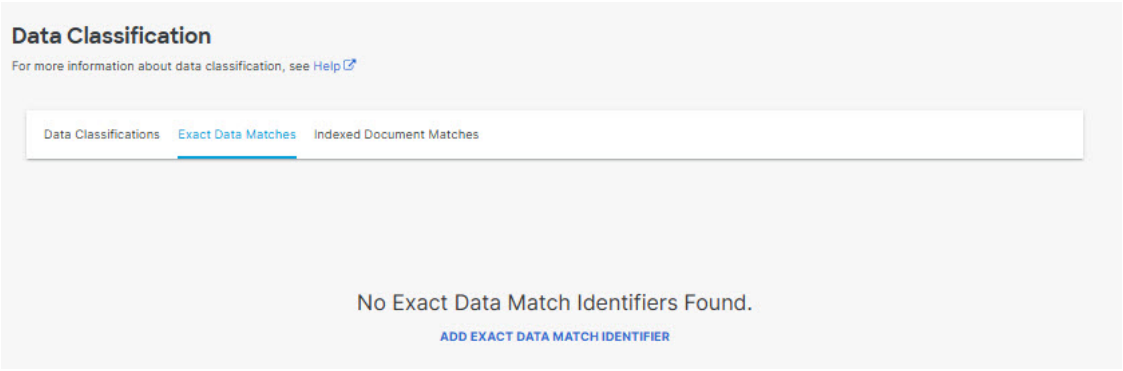
```
Email,SSN,Passport number - US,Credit card number
r_t@gmail.com, 113011111,123456789USA1234567U1234567, 5205105105105109
r_ppp@gmail.com, 248257990,123456789USA1234567U1234567, 4532237384050172
r_opop@gmail.com, 363265019,123456789USA1234567U1234567, 4532549977031249
ppo_t@gmail.com, 417279936,123456789USA1234567U1234567, 4539157470627290
```

Create an Exact Data Match Identifier

Provides instructions for completing the Create an Exact Data Match Identifier workflow in Cisco Secure Access. Navigate to Secure Settings Data Classification Exact Data Matches and click ADD EXACT DATA MATCH IDENTIFIER.

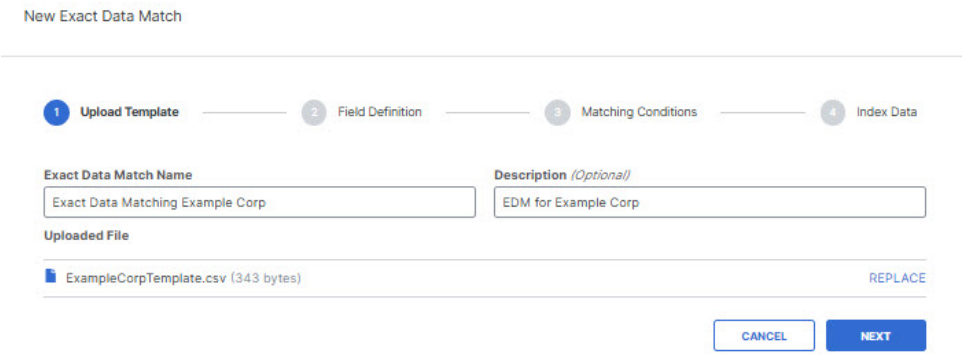
Procedure

1. Navigate to **Secure** > **Settings** > **Data Classification** > **Exact Data Matches** and click **ADD EXACT DATA MATCH IDENTIFIER**.



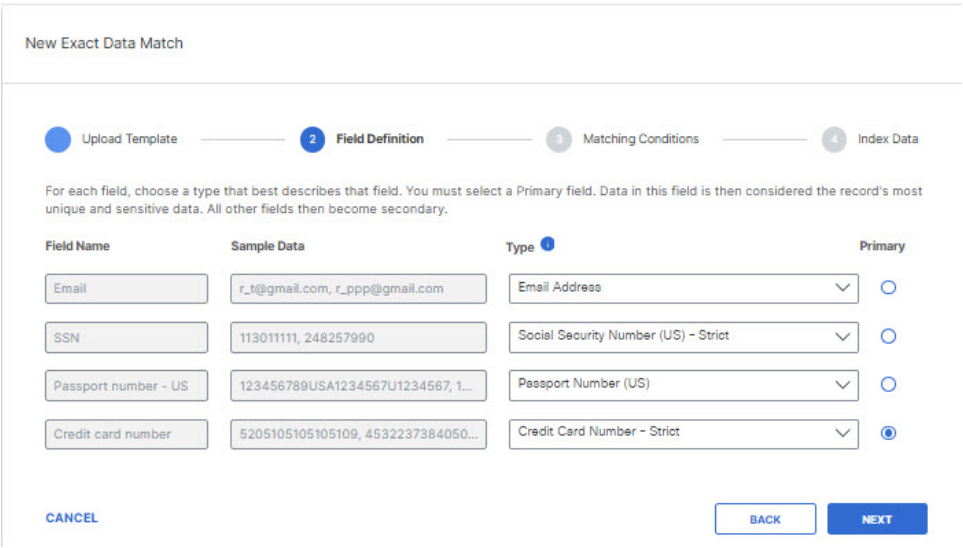
2. Provide a name and description for the exact data match, then upload sample data and click **Next**.

> **Note**
>
> Do not upload any real data in the CSV. Use only sample data for the template.



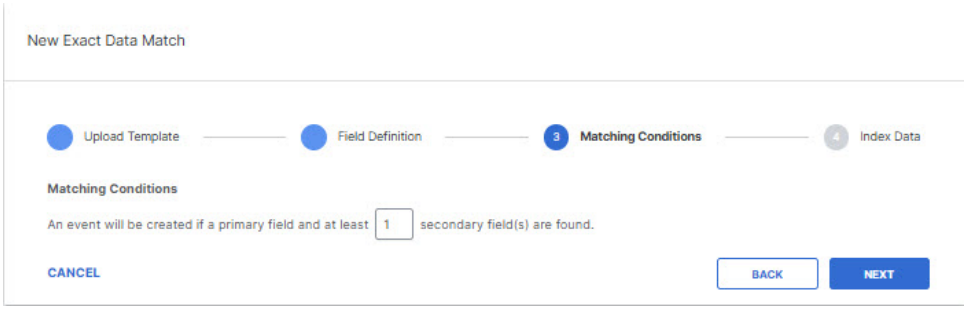
3. From the drop-down menu, choose the type of data of each field.

   The available field types are described in Exact Data Match Field Types:



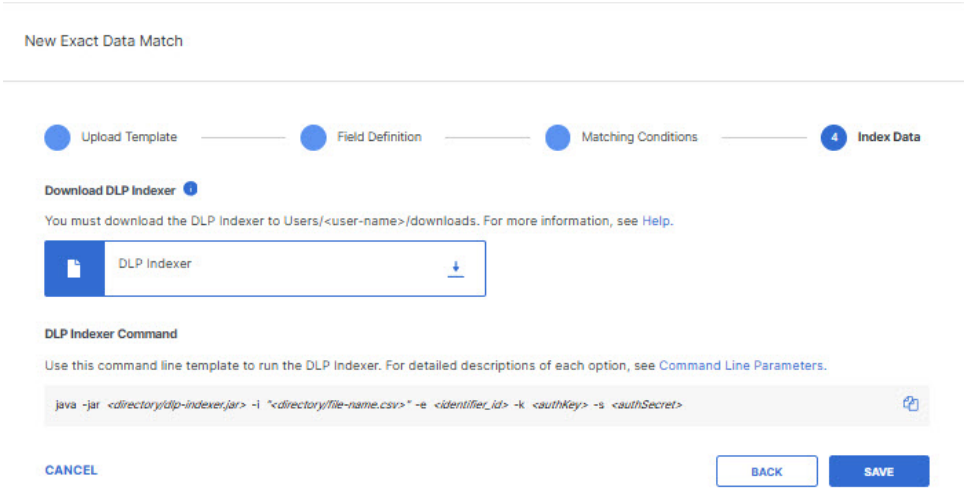
4. Select the Primary field that must be found with other data fields for the identifier to match and click **Next**. The primary field should be the field in the record to always match. The secondary fields are the number of fields in the record that should be present with the primary field to match.
5. Enter the minimum number of secondary fields required to be found within 10 terms of the primary field for a match. You can have no secondary field, or up to as many fields in the record that are not the primary field. For example, if at least 3 secondary fields are required, then the identifier will trigger an event only when 3 or more additional fields are found with the primary field. If the .csv file has only 1 column, then the secondary option is greyed-out and automatically set to 0. Click **Next**.

> **Note**
>
> The secondary fields must each be a different identifier.



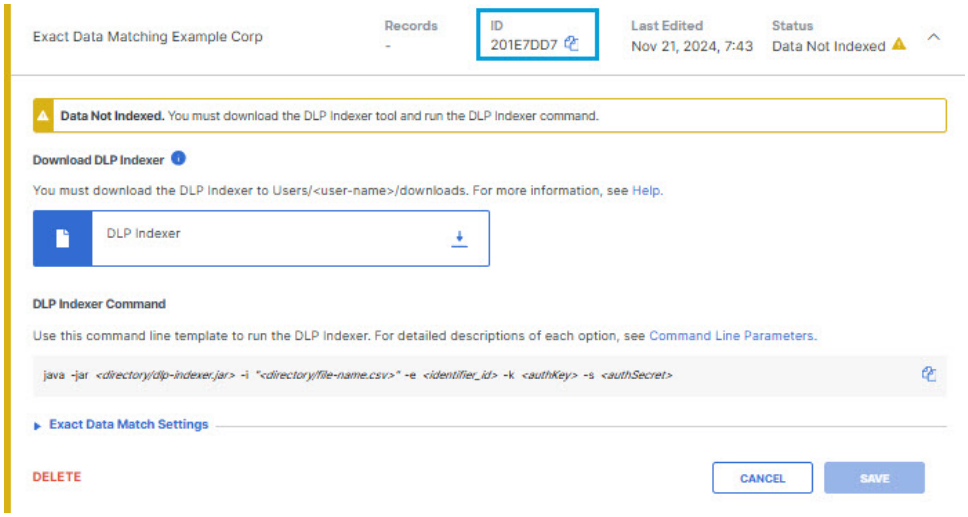
6. Click the download icon to download the DLP indexer. Then click **Save**.

> **Note**
>
> You can click on **Command Line Parameters** to view information about the command line arguments required to run the indexer.

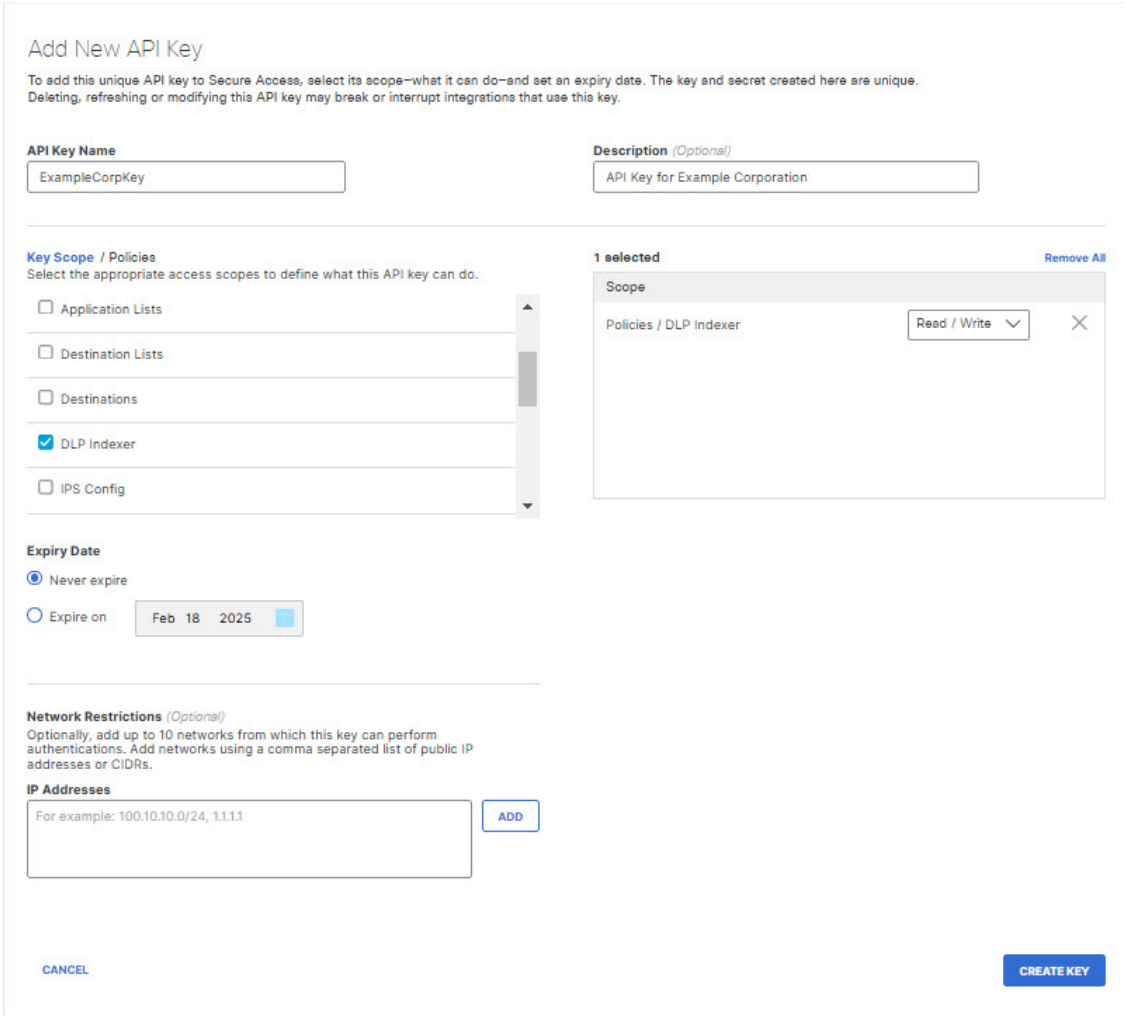


7. The EDM Identifier now has a status of **Data Not Indexed**. You can expand the listing to view the details about the EDM Identifier. When the EDM identifier status is **Data Not Indexed**, you can edit the field types, the primary field selection, and the matching conditions, but the EDM Identifier cannot be added to a data classification. Make note of the ID for th EDM Identifier; you will need it to run the DLP indexer.

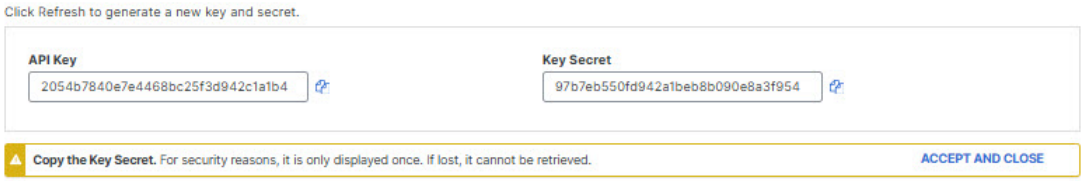
> **Note**
>
> The display page does not display the full EDM identifier ID; use the **Copy** icon to copy the ID



8. Create an API key and secret for the EDM data indexer.
   a) Navigate to **Admin** > **API Keys** and click **Open API Keys**.
   b) Click **Add** and provide an **API Key Name** and **Description** for the API Key.
   c) Select **Policies** > **DLP Indexer** for the scope and choose **Read/Write** for the permissions. Then click **Create Key**.



d) Copy and save the API Key and Secret somewhere safe, as you will need them to run the DLP Indexer.



9. Click **ACCEPT AND CLOSE**.
10. Use the Secure Access DLP Indexer to index your data records. For more information on the indexer, see Index Data for an EDM.
    a. Move the indexer from the Downloads folder to a convenient location, such as the folder where the data records are stored.
    b. Run the indexer in a terminal window with the following command:

    ```
    java -jar <directory_path>\dlp-indexer.jar -i
    "<directory_path>\<source_file>.csv"

    -e <edm_template-id> -k <authKey> -s <authSecret>
    ```

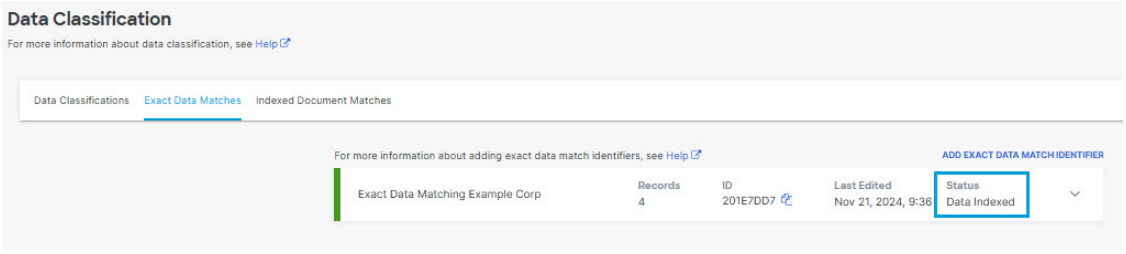
    where:

    - `<directory_path>\dlp-indexer.jar`–the relative path to the location of the DLP indexer

- "*<directory_path>**<source_file>*.csv"—the relative path to the csv spreadsheet with the actual data records
- *<edm_template-id>* —the ID of the EDM Identifier retrievable from the Umbrella UI (see Step 7)
- *<authKey>*—the API Key previously saved at Step 8d
- *<authSecret>*—the API Secret previously saved at Step 8d

What to do next

The EDM Identifier now has a status of **Data Indexed**.



The EDM Identifier now has a status of **Data Indexed**.

> **Note**
>
> When the EDM has a status of **Data Indexed**, you can add the EDM to a data classification but you can not edit the field types, primary field selection, or matching condition.

If you update your source file with new or changed records, you need to run the DLP indexer again on that file using the same EDM Identifier ID, API Key, and API Secret. This ensures that policies configured to use the EDM Identifier are updated to reflect the new data fingerprints. For more information, see Update the Indexed Data Set Periodically.

Index Data for an EDM

Describes Index Data for an EDM in Cisco Secure Access. The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom EDM Identifier.

The DLP indexer creates irreversible fingerprints of critical data structured in records with a consistent format and uploads them to Secure Access to establish a custom EDM Identifier. EDM Identifiers enable Secure Access to protect sensitive data by using data fingerprinting techniques as opposed to pattern matching techniques.

EDM Identifiers can be added to a Data Classification (see Manage Data Classifications) as custom identifiers; DLP rules that use these identifiers can monitor and/or block files that match the data you have indexed.

You need to run the DLP indexer in two different circumstances:

- When you initially create an EDM Identifier, you run the indexer on the data set you want to detect. This topic provides basic information for running the indexer, but for a description of the process to use the indexer within the context of creating an EDM Identifier, see Create an Exact Data Match Identifier. You cannot use the indexer to create an EDM Identifier without also performing the steps described in that topic.
- When the data set to be detected changes, you run the indexer to produce an updated version of the EDM Identifier. This process is described in Update the Indexed Data Set Periodically.

> **Note**
>
> To see a summary of the indexer options available, invoke the indexer with the **-h** option. (`java -jar <directory-path>\dlp-indexer.jar -h`.)

Prerequisites for Index Data for an EDM

Describes Prerequisites for Index Data for an EDM in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- You must download the indexer using the Secure Access GUI. See Step 6 in Create an Exact Data Match Identifier.
- Before running the DLP indexer you must generate an API Key and Secret using the Secure Access GUI. See Step 8 in Create an Exact Data Match Identifier.

> **Note**
>
> If you already have a key and secret generated for use with a previous run of the DLP indexer, you may use those.

- The indexer supports indexing source files with up to 55 million records. The exact records limit is determined by the total number of columns and how many of those are of alphanumeric type. The indexer will report the exact limit when attempting to load a file that exceeds it. If your dataset is larger than the limit, you need to split the records into multiple files. For errors received when indexing a large file, see Memory Tuning for DLP Exact Data Matching Indexer.
- The source data CSV file you index must meet the following requirements:
  - A multi-term (multi-word) field can contain a maximum of 6 space-separated words.
  - The data file must contain only 1 byte or 2 byte UTF-8 encoded characters.
  - The first row of data must have between 1 and 50 fields and each row must have the same number of fields.
  - The first row of data must specify the name of each field, and each value must be unique.
  - Data in the second and ensuing rows must comply with the EDM field types and supported formats (See Exact Data Match Field Types.)
  - The field names in the sample data template must match the field names in the actual data source file. The field names must appear in the same order in both files.

> **Caution**
>
> Do not create, edit, or view the source data CSV file using Microsoft Excel, as this may corrupt the file. Use a text editor.

> **Note**
>
> If any of the values provided in the source file to the DLP indexer fail to be validated as per the supported format, then the DLP indexer will skip that record and proceed with indexing the remaining records. The indexer also behaves in this manner for any records that may exceed the template-defined fields, and for empty rows or records with empty primary values. The DLP indexer generates messages reporting the position of any skipped records in the file.

Run the DLP Indexer to Create an EDM Identifier

Provides instructions for completing the Run the DLP Indexer to Create an EDM Identifier workflow in Cisco Secure Access. When you create a new EDM Identifier, you need to run the DLP indexer on the data set to upload the first set of data records.

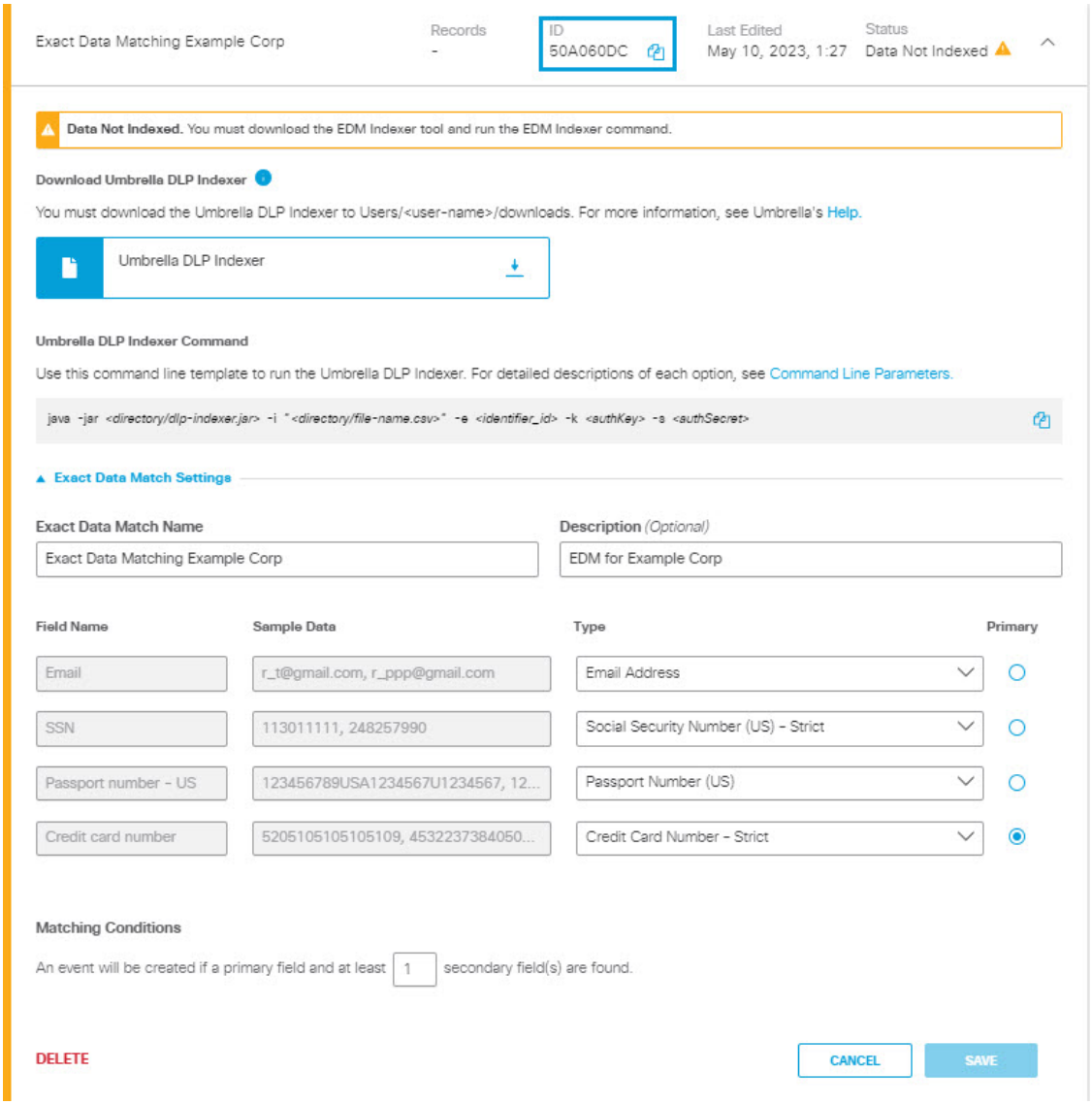
When you create a new EDM Identifier, you need to run the DLP indexer on the data set to upload the first set of data records. For the full procedure to create an EDM identifier, see Create an Exact Data Match Identifier.

Procedure

1. Review the Prerequisites, especially:
   - Be sure you have the API key and secret. (See Step 8 in Create an Exact Data Match Identifier.)
   - Be sure you have the EDM Identifier ID. (See Step 7 in Create an Exact Data Match Identifier.)
2. Run the indexer in a terminal window with the following command:

```
java -jar <directory_path>\dlp-indexer.jar -i
"<directory_path>\<source-file>.csv"-e <edm-template-id> -k <authKey> -s
<authSecret>
```

   Where:
   - `<directory_path>\dlp-indexer.jar` –the relative path to the location of the DLP indexer
   - "`<directory_path>\<source-file>.csv`" –the relative path to the csv spreadsheet with the actual data records
   - `<edm-template-id>`–the ID of the EDM Identifier retrievable from the Secure Access UI using the copy icon shown in the following screenshot. (See also Step 7 in Create an Exact Data Match Identifier.)



- <*authKey*> –the API Key previously saved at Step 8d of Create an Exact Data Match Identifier.
- <*authSecret*> –the API Secret previously saved at Step 8d of Create an Exact Data Match Identifier.

What to do next

If the indexer runs successfully, the exact data matcher will have a status of **Data Indexed**.

> **Note**
>
> When the EDM has a status of Data Indexed, you can add the EDM to a data classification but you can not edit the field types, primary field selection, or matching condition.

Update the Indexed Data Set Periodically

Provides instructions for completing the Update the Indexed Data Set Periodically workflow in Cisco Secure Access. When your source data changes, the existing EDM Identifier on your configured policy must be updated to reflect the new data fingerprints.

When your source data changes, the existing EDM Identifier on your configured policy must be updated to reflect the new data fingerprints. Using a script allows you to automatically rerun the DLP indexer periodically to update your source data to Secure Access without manually performing the initial procedure over again. After you rerun the DLP indexer with the updated version of the source file against the ID of your EDM Identifier, the DLP Policies configured with that EDM Identifier account for the most recent updates to your critical records.

Procedure

1. In a terminal window, set the the API Key and Secret previously used to index the identifier (saved in Step 8d of Create an Exact Data Match Identifier) to the environment variables **DLP_AUTH_KEY** and **DLP_AUTH_SECRET**.
2. Run the command to re-index the identifier as part of a periodically executed script or manually as needed:

   ```
   java -jar <directory_path>\dlp-indexer.jar -i
   "<directory_path>\<source-file>.csv"

   -e <edm_template-id> -k DLP_AUTH_KEY -s DLP_AUTH_SECRET
   ```

   Where:

   - `\<directory_path>\dlp-indexer.jar` –the relative path to the location of the DLP indexer
   - `"\<directory_path>\<source-file>".csv` –the relative path to the csv spreadsheet with the actual data record.
   - `<edm-template-id>` –the ID used to index the EDM Identifier originally.

Troubleshooting

Provides instructions for completing the Troubleshooting workflow in Cisco Secure Access. If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

Procedure

1. Confirm you have the latest version of the Java Development Kit installed.
2. Confirm that you have your PATH system variable set correctly:
   a. Check the location where you have Java installed.

- For Windows this is normally **C:\Program Files\Java\jdk-<version-number>\bin**
- For Linux this is normally `/usr/java/jdk-<version-number>/bin`

b. Use the instructions here to set the PATH system variable appropriately for your operating system.

What to do next

> **Note**
>
> If the data indexer fails to process the input file and returns a **base64** encoded error code, provide that code to the Secure Access Support to assist you with troubleshooting.

Exact Data Match Field Types

Describes Exact Data Match Field Types in Cisco Secure Access. When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided.

When creating an Exact Data Match (EDM) template, you must choose an EDM type for each field provided. The EDM types are similar to the Built-in Data Identifiers in that specific patterns must be found to match the identifier. Unlike Built-In Identifiers, EDM types do not use keywords to find data matches.

Supported EDM Types

Describes Supported EDM Types in Cisco Secure Access. ABA Routing Number (US)–A 9-digit number used by banks to identify specific financial institutions in the United States.

- **ABA Routing Number (US)**–A 9-digit number used by banks to identify specific financial institutions in the United States.
- **Alphanumeric**–Up to 6 words composed of 1 and 2-byte UTF-8 encoded characters, delimited by spaces.
- **Bank Account Number (US)**–A 5-digit number denoting a bank account number issued in the United States.
- **Carte nationale d'identité sécurisée – CNIS (France)**–A 12-digit number denoting the French national identity card number.
- **Credit Card Number**–A valid 15 or 16-digit credit card number that passes the Luhn validation and includes any of the following delimiters: space, no space, ~, or -.
- **Date**–A date value matching one of the following formats where the `<delimiter>` is no space, /, or -. :
- the European format of `<dd><delimiter><mm><delimiter><yyyy>` or
- the American format of `<mm><delimiter><dd><delimiter><yyyy>`
- **Email Address**–A valid email address using ASCII characters.
- **Fiscal Identification Number – Número de identificación fiscal – NIF (Spain)**–A number issued to Spanish nationals for identification purposes. The pattern matches`<ddddddddd><a>` where:
  - `a`is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
- **ICD Code**–A number matching the pattern of one of the typical International Classification of Diseases (ICD) codes.
- **Individual Taxpayer Identification Number – ITIN (US)**–A United States tax processing number issued by the Internal Revenue Service (IRS). The pattern must match the format of `<ddd><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -

- **International Bank Account Number – IBAN (UK)**–An international bank account number for the UK. The pattern matches a format of `<aadd><delimiter><aaaadddd><delimiter><dddd><delimiter><dddd><delimiter><dd>` where:
  - `a` is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, or -
- **IP Address**–A valid IPv4 address.
- **National Drug Code Number (NDC)**–Segments of the National Drug Code (NDC) used in the united States to identify drugs for human use. The pattern matches a format of `<ddddd><delimiter><ddd><delimiter><dd>` where:
  - `a` is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is ~ or -
- **National Insurance Number – NINO (UK)**–An identification number issued to individuals by the United Kingdom Department for Work and Pensions. The pattern matches with a format of `<aa><delimiter><dd><delimiter><dd><delimiter><dda>` where:
  - `a` is any ASCII alphabet letter from a to z
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .
- **Passport Number (US)**–An identification number issued to citizen and non-citizen nationals of the United states. The pattern must match a format of `<ddddddddd>USA<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9.
- **Passport Number (UK)**–An identification number that serves as proof of nationality or immigration status in the United Kingdom. The pattern must match one of the following formats:
  - a 9-digit number
  - `<ddddddddd>GBR<ddddddd>U<ddddddd>` where `d` is any ASCII digit from 0 to 9
- **Postcode (UK)**–A number matching the typical UK postal code patterns, where the number can include a space between the inward and outward segments.
- **Social Security Number - INSEE (France)**–National identification numbers for The National Institute of Statistics and Economic Studies issued at birth to French nationals. The number can be 12 or 15 digits. The pattern matches a format of `<ddddddddddddd><delimiter><dd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~
- **Social Security Number (US) – Strict**–An identification number issued in the United States to citizens, permanent residents, and temporary working residents. The pattern matches`<aaa><delimiter><dd><delimiter><dddd>` where:
  - `d` is any ASCII digit from 0 to 9
  - `<delimiter>` is a space, no space, ~, -, or .

Indexed Document Match Identifiers

Provides instructions for completing the Indexed Document Match Identifiers workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Indexed Document Matching (IDM) is a data matching technique that detects data loss incidents involving sensitive information maintained in unstructured formats for all DLP-supported file types. IDMs enable Secure Access to scan documents used in a wide range of disciplines such as tax forms, merger and acquisition forms, medical records, bank statements, stock agreements, medical power of attorney forms, US patent files, non-disclosure agreements, resumes, source code, and more.

Secure Access performs Indexed Document Matching by creating hash fingerprints of text extracted from your sensitive documents, as opposed to leveraging pattern matching techniques. To create the fingerprints, you must download the DLP indexer and then run it against your documents from a command line prompt. The indexer extracts the document text, performs fingerprinting and indexing operations on it, then hashes the indexed text and uploads it to the Secure Access DLP. (Generally document text represents a low percentage of total document size, so indexing only text reduces the space required to store IDMs.)

Once you have run the indexer, you will have an Indexed Document Match Identifier associated with the documents. You will then be able to:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- JVM version 17+
- The source file(s) you index must be in one of the formats supported by the DLP policy, listed here.

Procedure

1. Create a Data Classification that uses the IDM as a custom data identifier (as described in Create a Data Classification or Copy and Customize a Built-In Data Classification).
2. Create a DLP rule that uses the Data Classification including that IDM Identifier. (For more information on DLP rules, see Manage the Data Loss Prevention Policy.)

With these configurations in place, Secure Access will be able to monitor and/or block transmission of unstructured files that match at least a user-configurable percentage of the data text indexed for the IDM.

Note

To see a summary of the indexer options available, invoke the indexer with the **-h** option. (`java -jar <directory-path>\dlp-indexer.jar -h`.)

Limitations

Describes Limitations in Cisco Secure Access. The total amount of indexed text for all the IDMs in your organization must not exceed 1 GB.

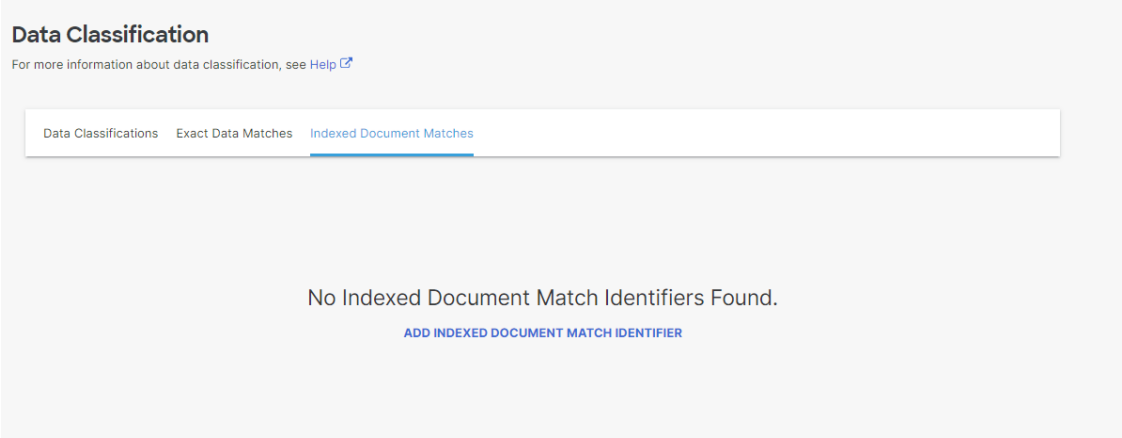
- The total amount of indexed text for all the IDMs in your organization must not exceed 1 GB. You can increase this limit at no cost; contact customer support. The DLP indexer displays an error message if you exceed your allotted quota.
- The data files must contain only 1 byte or 2 byte UTF-8 encoded characters, or Unicode characters.
- After you create an IDM Identifier, when you re-run the indexer using the same IDM Identifier, the indexer completely overwrites the previous index associated with that identifier. To add new data to an existing IDM, when you run the indexer again, include both the original data path and the new data path in the command to run the indexer.

Create an Indexed Document Match Identifier

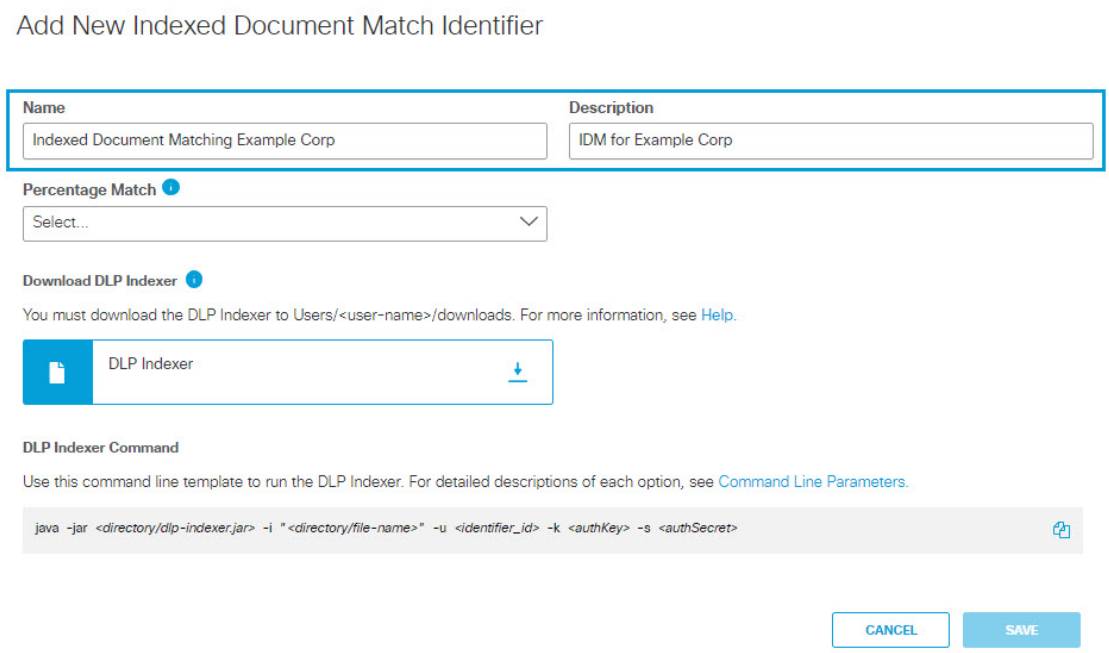
Provides instructions for completing the Create an Indexed Document Match Identifier workflow in Cisco Secure Access. Navigate to Secure Settings Data Classification Indexed Document Matches and click ADD INDEXED DOCUMENT MATCH IDENTIFIER.

Procedure

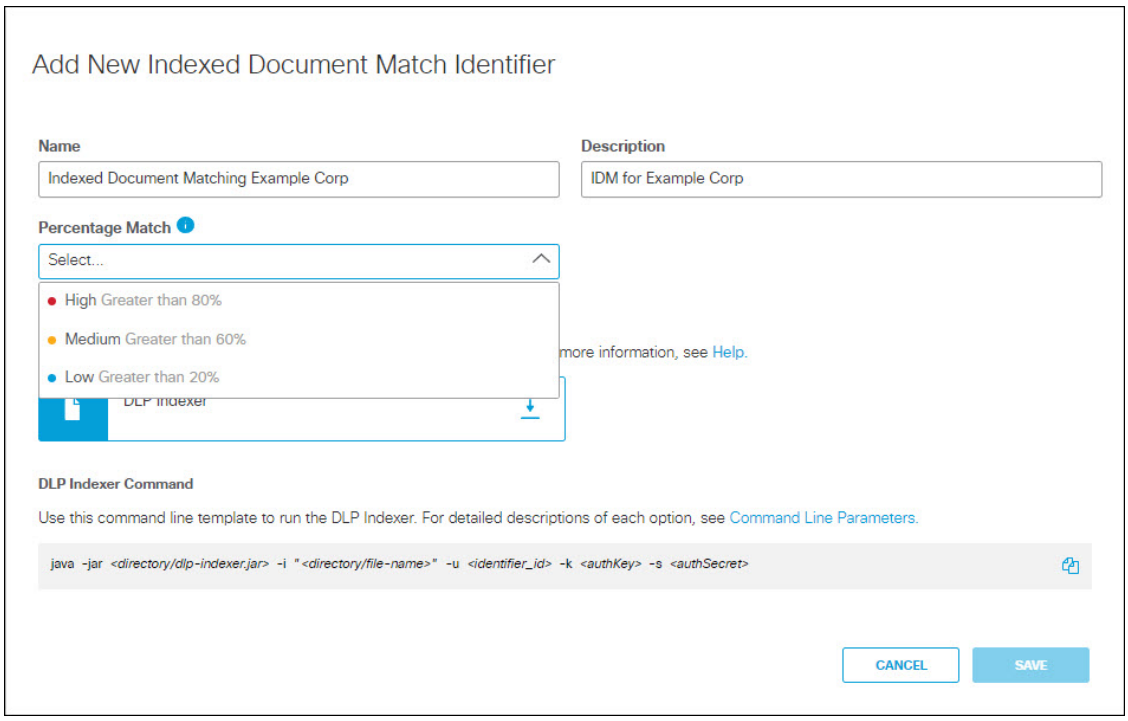
1. Navigate to **Secure** > **Settings** > **Data Classification** > **Indexed Document Matches** and click **ADD INDEXED DOCUMENT MATCH IDENTIFIER**.



2. Provide a name and description for the Indexed Document Match Identifier.

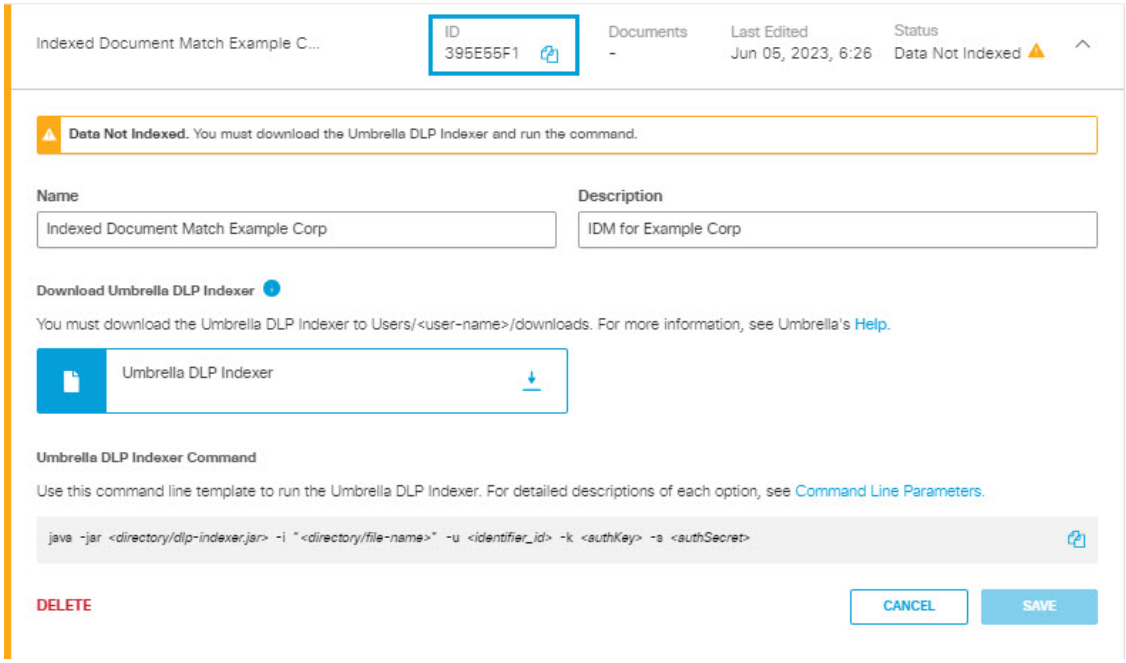


3. Select the level of percentage match required for a scanned document to be considered a match against a document included in the IDM:
   - High: 80% or more of the scanned document must match a document indexed for the IDM.
   - Medium: 60% or more of the scanned document must match a document indexed for the IDM.
   - Low: 20% or more of the scanned document must match a document indexed for the IDM.

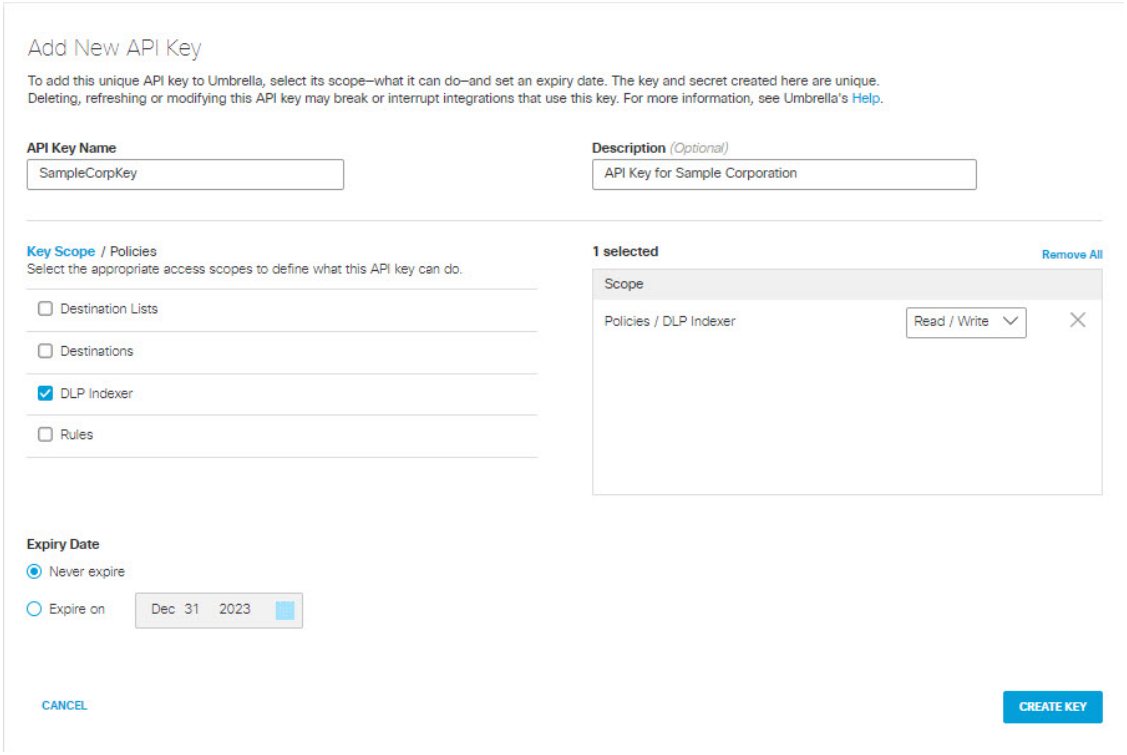


4. If you have not already downloaded the DLP indexer, click the download icon to do so.
5. Click **Save.**
6. The Indexed Document Match Identifier now has a status of **Data Not Indexed.** You can expand the listing to view the details about the IDM Identifier. After you have indexed the IDM Identifier, you will be able to add it to a Data Classification as a custom identifier. Make note of the ID for the Indexed Document Match Identifier; you will need it to run the DLP indexer.

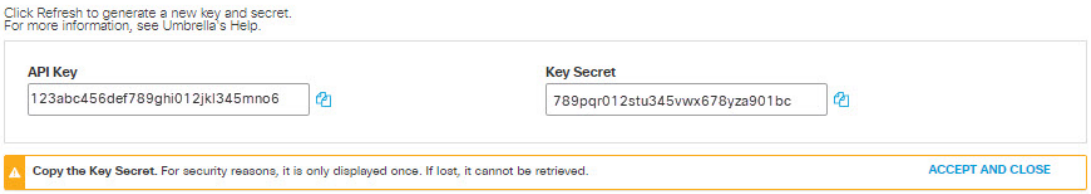
> **Note**
>
> The display page does not display the full IDM Identifier ID; use the **Copy** icon to copy the ID.



7. Create an API key and secret for the DLP indexer.
   a. Navigate to **Admin** > **API Keys** and click **Add**.
   b. Provide an **API Key Name** and **Description** for the API Key.
   c. Select **Policies** > **DLP Indexer** for the scope and choose **Read/Write** for the permissions. Then click **Create Key**.



d. Copy and save the API Key and Secret somewhere safe, as you will need them to run the DLP indexer.

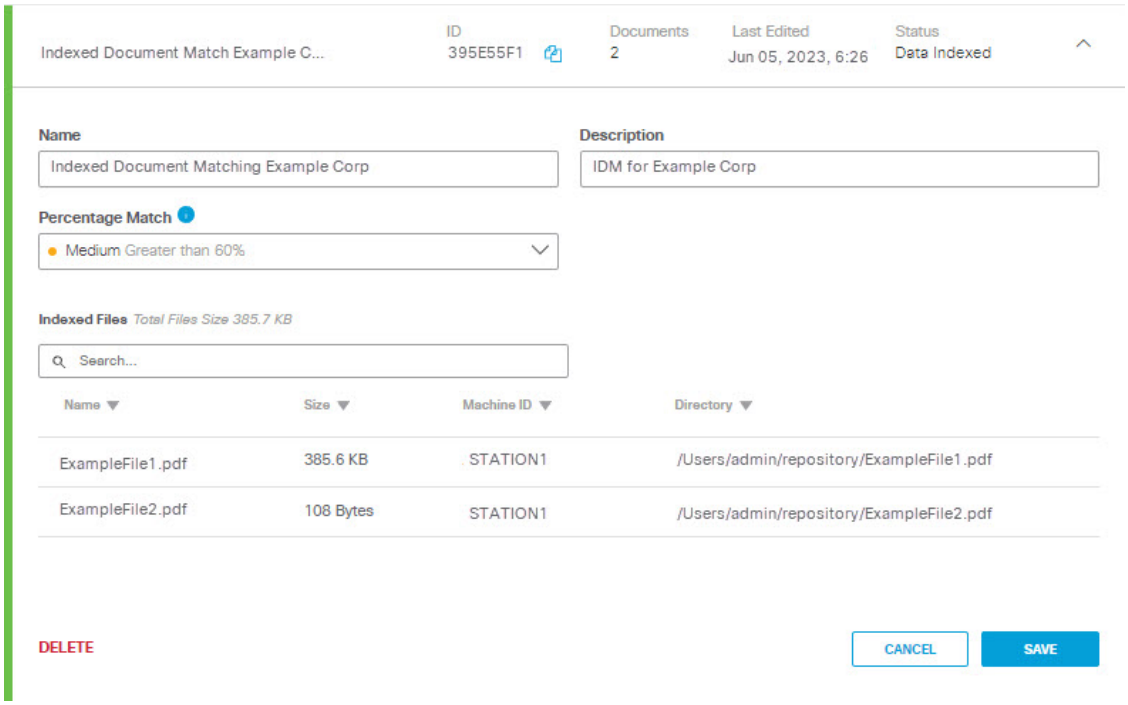


8. Use the Secure Access DLP indexer to fingerprint your example files.

Run the indexer in a terminal window with the following command: `java -jar <directory-path>\dlp-indexer.jar -i "<directory_paths or file-names separated by commas>" -u <IDM-id> -k <authKey> -s <authSecret>`

where:

- `<directory-path>\dlp-indexer.jar`—the relative path to the location of the DLP indexer.
- `<directory_paths or file-names separated by commas>`—the relative path to the directory containing your data, or a comma-separated list of files or directories.
- `<IDM_id>`—the ID of the IDM Identifier retrievable from Secure Access UI. (See Step 6.)
- `<authKey>`—the API Key previously saved at Step 7d.
- `<authSecret>`—the API Secret previously saved at Step 7d.



What to do next

The Indexed Document Match Identifier now has a status of **Data Indexed**; expand the listing to see details about the indexed files. You can now add the IDM to a Data Classification.

If you change your source file or directories you need to run the indexer on that file or directory again using the same IDM Identifier ID, API Key, and API Secret. This ensures that policies configured to use the IDM are updated to reflect the new data fingerprints. For more information, see Monitor the Indexed Data Set and Re-Index as Needed.

Monitor the Indexed Data Set and Re-Index as Needed

Describes Monitor the Indexed Data Set and Re-Index as Needed in Cisco Secure Access. As your source data changes, you need to re-index it using the same IDM Identifier to capture those changes so Secure Access will use them when scanning documents.

As your source data changes, you need to re-index it using the same IDM Identifier to capture those changes so Secure Access will use them when scanning documents. You can automate the re-indexing process to trigger a re-index when the source data has changed. Using the indexer monitor option causes the indexer to perform an initial index, then monitor your source data for updates and re-index as necessary. This is a useful option in a dynamic environment. In monitor mode, after performing an initial index the indexer checks the source data for changes every ten minutes, and if a change is detected, re-indexes the data.

You can run the indexer in monitor mode as a background process to automatically rerun the DLP indexer periodically to update your source data to Secure Access.

Use the following command to start the indexer in monitor mode:

```
java -jar <directory-path>\dlp-indexer.jar -i "<directory_paths or file-names
separated by commas>" -u <IDM-id> -k <_authKey _> -s <authSecret> -y -m
```

Where:

- `<directory-path>\dlp-indexer.jar` – the relative path to the location of the DLP indexer.

- `<directory_paths or file-names separated by commas>`—the relative path to the directory containing your data, or a comma-separated list of files or directories.
- `<IDM_id>`—the ID of the IDM Identifier retrievable from Secure Access UI. (See Step 6.)
- `<authKey>`— the API Key previously saved at Step 7d of Create an Indexed Document Match Identifier.
- `<authSecret>`— the API Secret previously saved at Step 7d of Create an Indexed Document Match Identifier.
- The **-y** argument causes the indexer to automatically overwrite an existing index.

  When you run the indexer to re-index an existing IDM, it prompts for a yes/no confirmation before overwriting that IDM. Using the **-y** argument allows you to run the indexer without manually responding to the prompt.
- The **-m** argument causes the indexer to operate in monitor mode.

Troubleshooting

Provides instructions for completing the Troubleshooting workflow in Cisco Secure Access. If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer reports a failure, examine the output error messages to determine the problem.

If the indexer returns an error message that reads, "Error: A JNI error has occurred, please check your installation and try again," check the following:

Procedure

1. Confirm you have the latest version of the Java Development Kit installed.
2. Confirm that you have your PATH system variable set correctly:
   a. Check the location where you have Java installed.
      - For Windows this is normally **C:\Program Files\Java\jdk-<version-number>\bin**
      - For Linux this is normally **/usr/java/jdk-<version-number>/bin**
   b. Use the instructions here to set the PATH system variable appropriately for your operating system.

What to do next

Note

If the data indexer fails to process the input file and returns a **base64** encoded error code, provide that code to the Secure Access Support to assist you with troubleshooting.

Built-In Data Classifications

Describes Built-In Data Classifications in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access provides five different pre-defined data classifications. You can use the pre-defined data classifications in one of two ways:

- You can create a custom data classification by copying a pre-defined data classification provided by Secure Access, and customizing the copy; see Copy and Customize a Built-In Data Classification
- You can apply a pre-defined data classification template provided by Secure Access to a DLP rule or discovery scan. (See Add a Real Time Rule to the Data Loss Prevention Policy , Add a SaaS API Rule to the Data Loss Prevention Policy, and Discovery Scan.)

Each of the built-in data classifications has a different set of built-in data identifiers associated with it. The built-in data classifications are:

- **PII Data Classification** - Personal Information Identifiers; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. The data identifiers associated with the PII Data Classification are:
  - Multiple Personal Identifiers – PII (Australia) - Strict
  - Multiple Personal Identifiers – PII (European Union)
  - Multiple Personal Identifiers – PII (UK) - Strict
  - Multiple Personal Identifiers – PII (US) - Strict
- **PCI Data Classification** - Data related to the Payment Card Industry. The data identifiers associated with the PCI Data Classification are:
  - Credit Card Number - Strict
  - Expiry Date (Austria)
  - Expiry Date (Belgium)
  - Expiry Date (Croatia)
  - Expiry Date (Cyprus)
  - Expiry Date (Czech)
  - Expiry Date (Denmark)
  - Expiry Date (Estonia)
  - Expiry Date (Finland)
  - Expiry Date (France)
  - Expiry Date (Germany)
  - Expiry Date (Greece)
  - Expiry Date (Hungary)
  - Expiry Date (Ireland)
  - Expiry Date (Italy)
  - Expiry Date (Latvia)
  - Expiry Date (Lithuania)
  - Expiry Date (Luxembourg)
  - Expiry Date (Malta)
  - Expiry Date (Netherlands)
  - Expiry Date (Poland)

- Expiry Date (Portugal)
- Expiry Date (Romania)
- Expiry Date (Slovakia)
- Expiry Date (Slovenia)
- Expiry Date (Spain)
- Expiry Date (Sweden)
- Expiry Date (UK/US)
- Security Code (Austria)
- Security Code (Belgium)
- Security Code (Croatia)
- Security Code (Cyprus)
- Security Code (Czech)
- Security Code (Denmark)
- Security Code (Estonia)
- Security Code (Finland)
- Security Code (France)
- Security Code (Germany)
- Security Code (Greece)
- Security Code (Hungary)
- Security Code (Ireland)
- Security Code (Italy)
- Security Code (Latvia)
- Security Code (Lithuania)
- Security Code (Luxembourg)
- Security Code (Malta)
- Security Code (Netherlands)
- Security Code (Poland)
- Security Code (Portugal)
- Security Code (Romania)
- Security Code (Slovakia)
- Security Code (Slovenia)
- Security Code (Spain)
- Security Code (Sweden)
- Security Code (UK/US/EU except Bulgaria)

- **GDPR Data Classification** - Common personal data associated with the European Union's General Data Protection Regulation. Customers can use these identifiers to support GDPR compliance within their organizations. The data identifiers associated with the GDPR Data Classification are:
  - Carte national d'identité sécurisée – CNIS (France)
  - Credit Card Number - Strict
  - Criminal Record (Austria)
  - Criminal Record (Belgium)
  - Criminal Record (Croatia)
  - Criminal Record (Cyprus)
  - Criminal Record (Czech)
  - Criminal Record (Denmark)
  - Criminal Record (Estonia)
  - Criminal Record (Finland)
  - Criminal Record (France)
  - Criminal Record (Germany)
  - Criminal Record (Greece)
  - Criminal Record (Hungary)
  - Criminal Record (Ireland)
  - Criminal Record (Italy)
  - Criminal Record (Latvia)
  - Criminal Record (Lithuania)
  - Criminal Record (Luxembourg)
  - Criminal Record (Malta)
  - Criminal Record (Netherlands)
  - Criminal Record (Poland)
  - Criminal Record (Portugal)
  - Criminal Record (Romania)
  - Criminal Record (Slovakia)
  - Criminal Record (Slovenia)
  - Criminal Record (Spain)
  - Criminal Record (Sweden)
  - Criminal Record (UK)
  - Date of Birth
  - Driver's License Number (Austria)
  - Driver's License Number (Belgium)
  - Driver's License Number (Croatia)

- Driver's License Number (Cyprus)
- Driver's License Number (Czech Republic)
- Driver's License Number (Denmark)
- Driver's License Number (Estonia)
- Driver's License Number (Finland)
- Driver's License Number (France)
- Driver's License Number (Germany)
- Driver's License Number (Greece)
- Driver's License Number (Hungary)
- Driver's License Number (Ireland)
- Driver's License Number (Italy)
- Driver's License Number (Latvia)
- Driver's License Number (Lithuania)
- Driver's License Number (Luxembourg)
- Driver's License Number (Malta)
- Driver's License Number (Netherlands)
- Driver's License Number (Poland)
- Driver's License Number (Portugal)
- Driver's License Number (Romania)
- Driver's License Number (Slovakia)
- Driver's License Number (Slovenia)
- Driver's License Number (Spain)
- Driver's License Number (Sweden)
- Driver's License Number (UK)
- Email Address
- Ethnicity (Austria)
- Ethnicity (Belgium)
- Ethnicity (Croatia)
- Ethnicity (Cyprus)
- Ethnicity (Czech)
- Ethnicity (Denmark)
- Ethnicity (Estonia)
- Ethnicity (Finland)
- Ethnicity (France)
- Ethnicity (Germany)

- Ethnicity (Greece)
- Ethnicity (Hungary)
- Ethnicity (Ireland)
- Ethnicity (Italy)
- Ethnicity (Latvia)
- Ethnicity (Lithuania)
- Ethnicity (Luxembourg)
- Ethnicity (Malta)
- Ethnicity (Netherlands)
- Ethnicity (Poland)
- Ethnicity (Portugal)
- Ethnicity (Romania)
- Ethnicity (Slovakia)
- Ethnicity (Slovenia)
- Ethnicity (Spain)
- Ethnicity (Sweden)
- Ethnicity (UK)
- Eye Color (Austria)
- Eye Color (Belgium)
- Eye Color (Croatia)
- Eye Color (Cyprus)
- Eye Color (Czech)
- Eye Color (Denmark)
- Eye Color (Estonia)
- Eye Color (Finland)
- Eye Color (France)
- Eye Color (Germany)
- Eye Color (Greece)
- Eye Color (Hungary)
- Eye Color (Ireland)
- Eye Color (Italy)
- Eye Color (Latvia)
- Eye Color (Lithuania)
- Eye Color (Luxembourg)
- Eye Color (Malta)

- Eye Color (Netherlands)
- Eye Color (Poland)
- Eye Color (Portugal)
- Eye Color (Romania)
- Eye Color (Slovakia)
- Eye Color (Slovenia)
- Eye Color (Spain)
- Eye Color (Sweden)
- Eye Colour (UK)
- Gender (Austria)
- Gender (Belgium)
- Gender (Croatia)
- Gender (Cyprus)
- Gender (Czech)
- Gender (Denmark)
- Gender (Estonia)
- Gender (Finland)
- Gender (France)
- Gender (Germany)
- Gender (Greece)
- Gender (Hungary)
- Gender (Ireland)
- Gender (Italy)
- Gender (Latvia)
- Gender (Lithuania)
- Gender (Luxembourg)
- Gender (Malta)
- Gender (Netherlands)
- Gender (Poland)
- Gender (Portugal)
- Gender (Romania)
- Gender (Slovakia)
- Gender (Slovenia)
- Gender (Spain)
- Gender (Sweden)

- Gender (UK)
- Hair Color (Austria)
- Hair Color (Belgium)
- Hair Color (Croatia)
- Hair Color (Cyprus)
- Hair Color (Czech)
- Hair Color (Denmark)
- Hair Color (Estonia)
- Hair Color (Finland)
- Hair Color (France)
- Hair Color (Germany)
- Hair Color (Greece)
- Hair Color (Hungary)
- Hair Color (Ireland)
- Hair Color (Italy)
- Hair Color (Latvia)
- Hair Color (Lithuania)
- Hair Color (Luxembourg)
- Hair Color (Malta)
- Hair Color (Netherlands)
- Hair Color (Poland)
- Hair Color (Portugal)
- Hair Color (Romania)
- Hair Color (Slovakia)
- Hair Color (Slovenia)
- Hair Color (Spain)
- Hair Color (Sweden)
- Hair Colour (UK)
- Height (Austria)
- Height (Belgium)
- Height (Croatia)
- Height (Cyprus)
- Height (Czech)
- Height (Denmark)
- Height (Estonia)

- Height (Finland)
- Height (France)
- Height (Germany)
- Height (Greece)
- Height (Hungary)
- Height (Ireland)
- Height (Italy)
- Height (Latvia)
- Height (Lithuania)
- Height (Luxembourg)
- Height (Malta)
- Height (Netherlands)
- Height (Poland)
- Height (Portugal)
- Height (Romania)
- Height (Slovakia)
- Height (Slovenia)
- Height (Spain)
- Height (Sweden)
- Height (UK)
- International Bank Account Number – IBAN (Austria)
- International Bank Account Number – IBAN (Belgium)
- International Bank Account Number – IBAN (Croatia)
- International Bank Account Number – IBAN (Cyprus)
- International Bank Account Number – IBAN (Czech Republic)
- International Bank Account Number – IBAN (Denmark)
- International Bank Account Number – IBAN (Estonia)
- International Bank Account Number – IBAN (Finland)
- International Bank Account Number – IBAN (France)
- International Bank Account Number – IBAN (Germany)
- International Bank Account Number – IBAN (Greece)
- International Bank Account Number – IBAN (Hungary)
- International Bank Account Number – IBAN (Ireland)]
- International Bank Account Number – IBAN (Italy)
- International Bank Account Number – IBAN (Latvia)

- International Bank Account Number – IBAN (Lithuania)
- International Bank Account Number – IBAN (Luxembourg)
- International Bank Account Number – IBAN (Malta)
- International Bank Account Number – IBAN (Netherlands)
- International Bank Account Number – IBAN (Poland)
- International Bank Account Number – IBAN (Portugal)
- International Bank Account Number – IBAN (Romania)
- International Bank Account Number – IBAN (Slovakia)
- International Bank Account Number – IBAN (Slovenia)
- International Bank Account Number – IBAN (Spain)
- International Bank Account Number – IBAN (Sweden)
- International Bank Account Number – IBAN (UK)
- IP Address
- National Identity Number (Greece)
- National Identity Number – OIB (Croatia)
- National Insurance Number – NINO (UK)
- Passport Number (Austria)
- Passport Number (Belgium)
- Passport Number (Croatia)
- Passport Number (Cyprus)
- Passport Number (Czech Republic)
- Passport Number (Denmark)
- Passport Number (Estonia)
- Passport Number (Finland)
- Passport Number (France)
- Passport Number (Germany)
- Passport Number (Greece)
- Passport Number (Hungary)
- Passport Number (Ireland)
- Passport Number (Italy)
- Passport Number (Latvia)
- Passport Number (Lithuania)
- Passport Number (Luxembourg)
- Passport Number (Malta)
- Passport Number (Netherlands)

- Passport Number (Poland)
- Passport Number (Portugal)
- Passport Number (Romania)
- Passport Number (Slovakia)
- Passport Number (Slovenia)
- Passport Number (Spain)
- Passport Number (Sweden)
- Passport Number (UK)
- Phone Number (Austria)
- Phone Number (Belgium)
- Phone Number (Croatia)
- Phone Number (Cyprus)
- Phone Number (Czech Republic)
- Phone Number (Denmark)
- Phone Number (Estonia)
- Phone Number (Finland)
- Phone Number (France)
- Phone Number (Germany)
- Phone Number (Greece)
- Phone Number (Hungary)
- Phone Number (Ireland)
- Phone Number (Italy)
- Phone Number (Latvia)
- Phone Number (Lithuania)
- Phone Number (Luxembourg)
- Phone Number (Malta)
- Phone Number (Netherlands)
- Phone Number (Poland)
- Phone Number (Portugal)
- Phone Number (Romania)
- Phone Number (Slovakia)
- Phone Number (Slovenia)
- Phone Number (Spain)
- Phone Number (Sweden)
- Phone Number (UK)

- Postcode (Austria)
- Postcode (Belgium)
- Postcode (Croatia)
- Postcode (Cyprus)
- Postcode (Czech)
- Postcode (Denmark)
- Postcode (Estonia)
- Postcode (Finland)
- Postcode (France)
- Postcode (Germany)
- Postcode (Greece)
- Postcode (Hungary)
- Postcode (Ireland)
- Postcode (Italy)
- Postcode (Latvia)
- Postcode (Lithuania)
- Postcode (Luxembourg)
- Postcode (Malta)
- Postcode (Netherlands)
- Postcode (Poland)
- Postcode (Portugal)
- Postcode (Romania)
- Postcode (Slovakia)
- Postcode (Slovenia)
- Postcode (Spain)
- Postcode (Sweden)
- Postcode (UK)
- Race (Austria)
- Race (Belgium)
- Race (Croatia)
- Race (Cyprus)
- Race (Czech)
- Race (Denmark)
- Race (Estonia)
- Race (Finland)

- Race (France)
- Race (Germany)
- Race (Greece)
- Race (Hungary)
- Race (Ireland)
- Race (Italy)
- Race (Latvia)
- Race (Lithuania)
- Race (Luxembourg)
- Race (Malta)
- Race (Netherlands)
- Race (Poland)
- Race (Portugal)
- Race (Romania)
- Race (Slovakia)
- Race (Slovenia)
- Race (Spain)
- Race (Sweden)
- Race (UK)
- Region (Austria)
- Region (Belgium)
- Region (Croatia)
- Region (Cyprus)
- Region (Czech)
- Region (Denmark)
- Region (Estonia)
- Region (Finland)
- Region (France)
- Region (Germany)
- Region (Greece)
- Region (Hungary)
- Region (Ireland)
- Region (Italy)
- Region (Latvia)
- Region (Lithuania)

- Region (Luxembourg)
- Region (Malta)
- Region (Netherlands)
- Region (Poland)
- Region (Portugal)
- Region (Romania)
- Region (Slovakia)
- Region (Slovenia)
- Region (Spain)
- Region (Sweden)
- Region (UK)
- Religion (Austria)
- Religion (Belgium)
- Religion (Croatia)
- Religion (Cyprus)
- Religion (Czech)
- Religion (Denmark)
- Religion (Estonia)
- Religion (Finland)
- Religion (France)
- Religion (Germany)
- Religion (Greece)
- Religion (Hungary)
- Religion (Ireland)
- Religion (Italy)
- Religion (Latvia)
- Religion (Lithuania)
- Religion (Luxembourg)
- Religion (Malta)
- Religion (Netherlands)
- Religion (Poland)
- Religion (Portugal)
- Religion (Romania)
- Religion (Slovakia)
- Religion (Slovenia)

- Religion (Spain)
- Religion (Sweden)
- Religion (UK)
- Social Security Number – INSEE (France)
- VAT ID Number (Austria)
- VAT ID Number (Belgium)
- VAT ID Number (Croatia)
- VAT ID Number (Cyprus)
- VAT ID Number (Czech Republic)
- VAT ID Number (Denmark)
- VAT ID Number (Estonia)
- VAT ID Number (Finland)
- VAT ID Number (France)
- VAT ID Number (Germany)
- VAT ID NumberT (Greece)
- VAT ID Number (Hungary)
- VAT ID Number (Ireland)
- VAT ID Number (Italy)
- VAT ID Number (Latvia)
- VAT ID Number (Lithuania)
- VAT ID Number (Luxembourg)
- VAT ID Number (Malta)
- VAT ID Number (Netherlands)
- VAT ID Number (Poland)
- VAT ID Number (Portugal)
- VAT ID Number (Romania)
- VAT ID Number (Slovakia)
- VAT ID Number (Slovenia)
- VAT ID Number (Spain)
- VAT ID Number (Sweden)
- VAT ID Number (UK)
- Weight (Austria)
- Weight (Belgium)
- Weight (Croatia)
- Weight (Cyprus)

- Weight (Czech)
- Weight (Denmark)
- Weight (Estonia)
- Weight (Finland)
- Weight (France)
- Weight (Germany)
- Weight (Greece)
- Weight (Hungary)
- Weight (Ireland)
- Weight (Italy)
- Weight (Latvia)
- Weight (Lithuania)
- Weight (Luxembourg)
- Weight (Malta)
- Weight (Netherlands)
- Weight (Poland)
- Weight (Portugal)
- Weight (Romania)
- Weight (Slovakia)
- Weight (Slovenia)
- Weight (Spain)
- Weight (Sweden)
- Weight (UK)

- **HIPAA Data Classification** - Personal medical and healthcare data associated with the United States' Health Insurance Portability and Accountability Act. Customers can use these identifiers to support HIPAA compliance within their organizations. The data identifiers associated with the HIPAA Data Classification template are:
  - Date of Birth
  - Drug Name and Person Name (US)
  - Drug Name and Social Security Number (US)
  - Health Condition and Person Name (US)
  - Health Condition and Social Security Number (US)
  - ICD Code
  - ICD Code and Person Name (US)
  - ICD Code and Social Security Number (US)
  - Medical Prescriptions

  - National Drug Code Number - NDC
  - Social Security Number (US) - Strict

- Privacy Data Classification (US) - Personal Information Identifiers used in the United States; data that includes any personal information that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers. The data identifiers associated with the Privacy Data Classification for US States are:
  - ABA Routing Number (US)
  - Bank Account Number (US)
  - Business Number (US)
  - Company Number (US)
  - Driver's License Number (US)
  - Drug name and Person Name (US)
  - Drug Name and Social Security Number (US)
  - National drug code number
  - Health Insurance Number (US)
  - credit card number - strict
  - Medical Prescriptions (US)
  - Passport Number (US)
  - Phone Number (US)]
  - Race (US)]
  - Religion (US)
  - Social Security Number (US) - Strict
  - Student Loan Application Information (US)
  - Tax ID Number - ITIN (US)]
  - Zip Code (US)
  - Eye Color (US)
  - Gender (US)
  - Hair Color (US)
  - Height (US)
  - Weight (US)
  - ICD Code and Person Name (US)
  - ICD Code and Social Security Number (US)
  - Date of Birth and Person Name (US)

46 Built-in Data Identifiers

Topics:

- Built-in Data Identifiers

Provides an overview of Built-in Data Identifiers in Cisco Secure Access, including Built-in Data Identifiers. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Built-in Data Identifiers

Describes Built-in Data Identifiers in Cisco Secure Access. Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

Secure Access provides a wide selection of built-in data identifiers you can choose to incorporate into DLP policy to classify a wide range of sensitive data, both structured and unstructured.

The built-in identifier can classify specific data values based on pattern matching, bloom filters, and dictionaries incorporating proximity terms.

The ML (machine learning) built-in data identifiers are based on a LLM (Large Language Model) that was trained to classify unstructured sensitive data based on its true context. The ML data identifiers work for DLP-supported file types (see Supported File and Form Types); they do not work for form data. The ML built-in data identifiers are:

- Bank Statement
- Consulting Agreement
- CV/Resume
- Employment Agreement
- IRS Forms
- Medical Power of Attorney
- Mergers And Acquisitions
- NDA
- Partnership Agreement
- Source Code (ML)
- Stock
- US Patents

Built-in identifiers are not directly incorporated into DLP rules; you must first select and incorporate them into Data Classifications which you then apply to DLP rules. (See Manage Data Classifications).

The built in data identifiers are available as a PDF document here.

Tolerances

Describes Tolerances in Cisco Secure Access. Some built-in data identifiers have three versions, each with a different tolerance level associated with it.

Some built-in data identifiers have three versions, each with a different tolerance level associated with it. Tolerance levels determine how many instances of an identifier must appear within a document for that document to be considered a match. There are three tolerance levels:

- Lenient tolerance requires only a single instance of an identifier to appear within a document for that document to be considered a match.
- Moderate tolerance requires more occurrences of an identifier than Lenient tolerance, but fewer than Strict tolerance. (The exact number varies depending upon the identifier.)
- Strict tolerance requires the most occurrences of an identifier to appear within a document for that document to be considered a match. (The exact number varies depending upon the identifier.)

For identifiers that support tolerance levels, you can choose the tolerance level that best matches your level of concern for catching every occurrence of those identifiers.

Copy and Customize a Data Identifier

Provides instructions for completing the Copy and Customize a Data Identifier workflow in Cisco Secure Access. You can copy a built-in data identifier and change the threshold and proximity on the copy to create your own customized data identifier.

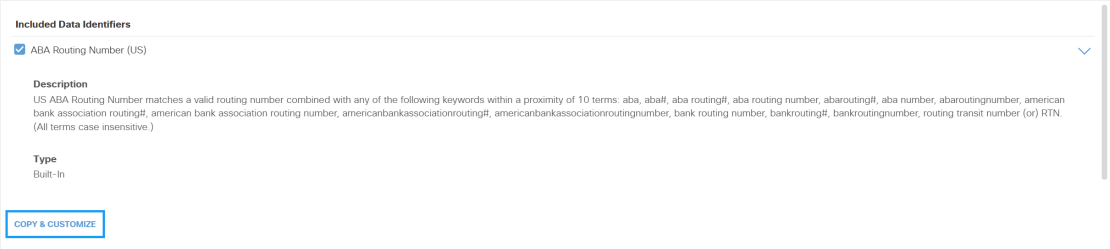
You can copy a built-in data identifier and change the threshold and proximity on the copy to create your own customized data identifier. For a list of built-in data identifiers, see Built-in Data Identifiers.

Before you begin

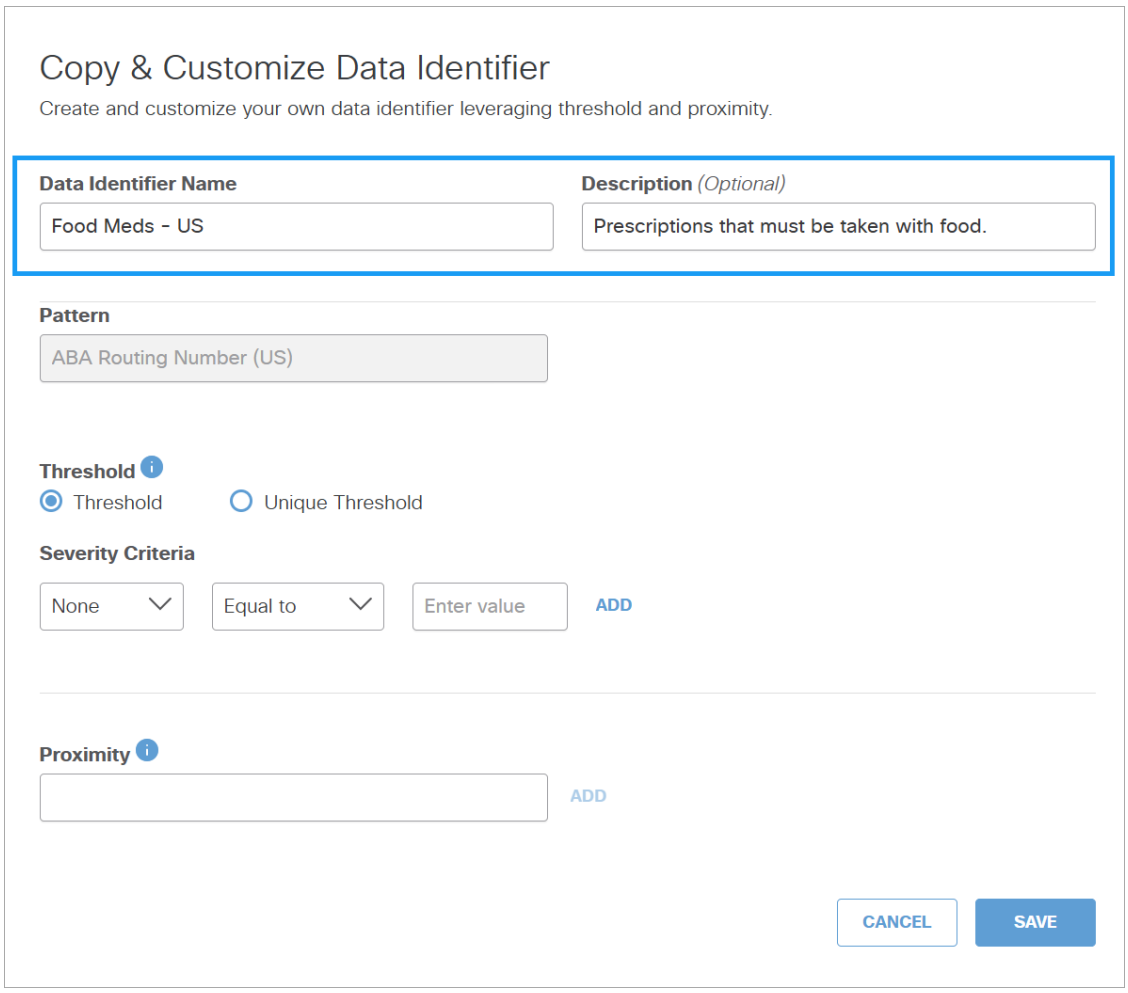
Full Admin user role. For more information, see Manage Accounts.

Procedure

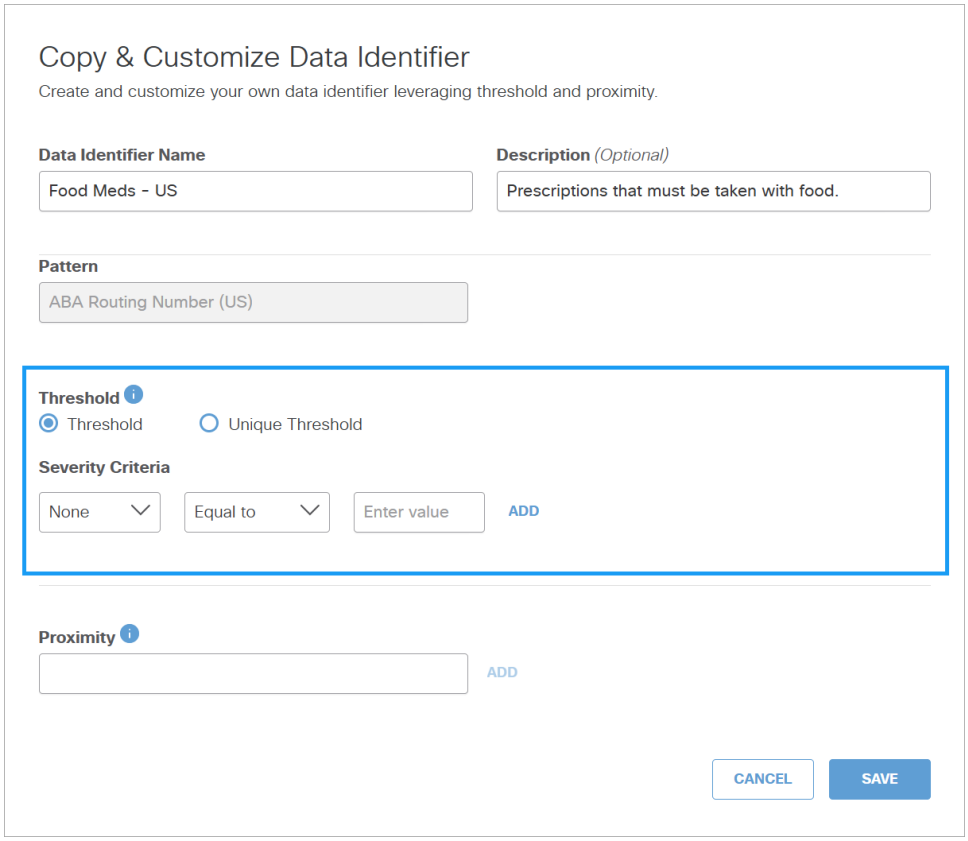
1. Navigate to **Secure** > **Settings** > **Data Classification**.
2. Expand a data classification, then expand a included data identifier within that classification and click **COPY & CUSTOMIZE**.



3. Give the data identifier a meaningful name and description.

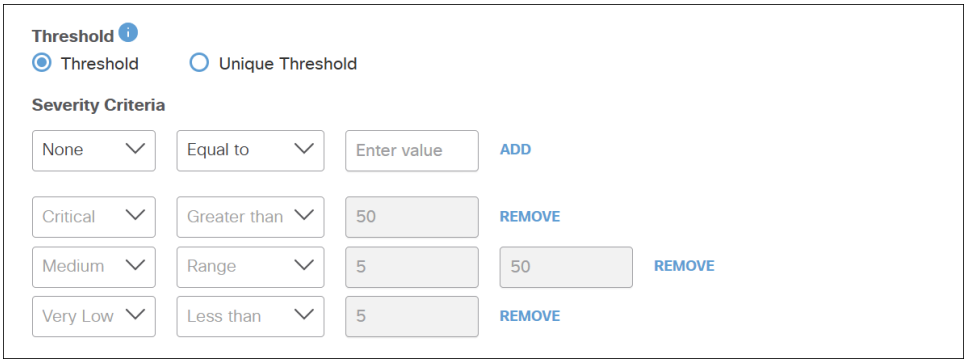


4. (Optional) Select **Threshold** or **Unique Threshold** and then specify the **Severity Criteria**. The **Threshold** value represents the total number of occurrences of this identifier that must be detected in a document for Umbrella to generate an incident. The **Unique Threshold** value represents the number of unique occurrences of this identifier that must be detected in a document for Umbrella to generate an incident. A threshold of 10, for example, only generates an incident if 10 instances of the identifier are found in the file. The default threshold is 1.

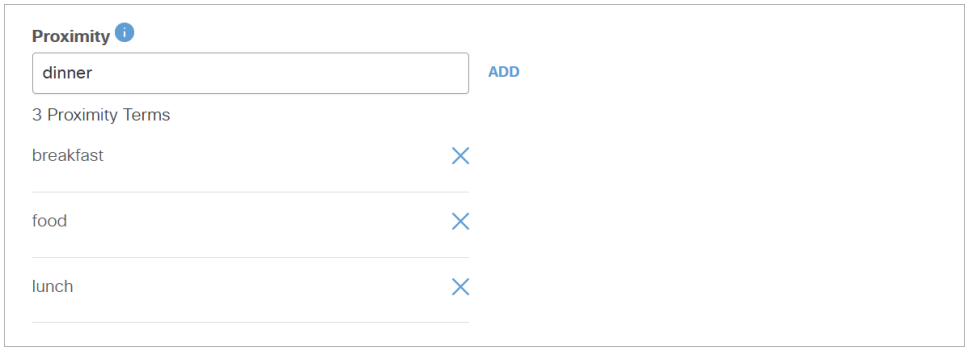


To specify the Severity criteria:

a) Select the severity name from the dropdown list. You can choose a predefined name or select **Custom** and then provide a name.
b) Select the operator to define the value. You can select **Range** to define a range of the threshold value.
c) Enter the threshold value or the range based on the selected operator.



5. To add proximity keywords to match against the pattern, enter a proximity keyword in the **proximity** field and then click **ADD**. Repeat this step to add multiple proximity keywords. Secure Access will not generate an incident unless at least one of the occurrences of a matching term or pattern appears within 20 terms of a proximity keyword.



6. Click **SAVE**.

   The custom identifier appears under Custom Identifiers when creating or editing a classification. (See Create a Data Classification or Copy and Customize a Built-In Data Classification.)

What to do next

> **Note**
>
> **Pattern**
>
> The pattern field is the built-in regular expression designed for this identifier and cannot be edited.

Create a Custom Identifier

Provides instructions for completing the Create a Custom Identifier workflow in Cisco Secure Access. A custom identifier can be used as part of a data classification to define terms and pattern expressions a DLP rule must match to generate an incident.

A custom identifier can be used as part of a data classification to define terms and pattern expressions a DLP rule must match to generate an incident. You can optionally further restrict matching criteria using additional qualifiers:

Specify a threshold, to indicate the minimum number of occurrences of a term or pattern that must appear within a document to qualify as a match.

Specify proximity keywords, at least one of which must appear within 20 terms of a term or pattern to qualify as a match.

Custom identifiers can also be used to match text extracted from images when OCR scanning is configured in Global Settings.

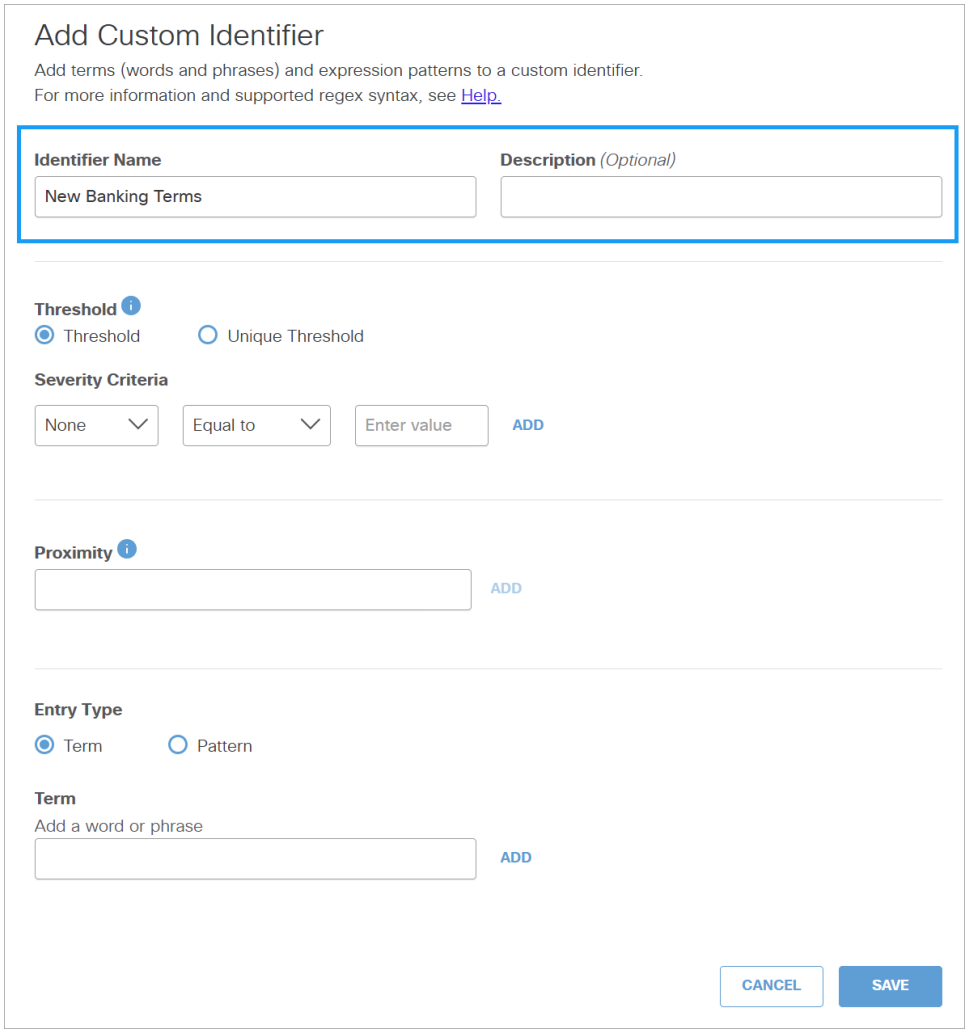
Before you begin

Full Admin user role. For more information, see Manage Accounts.

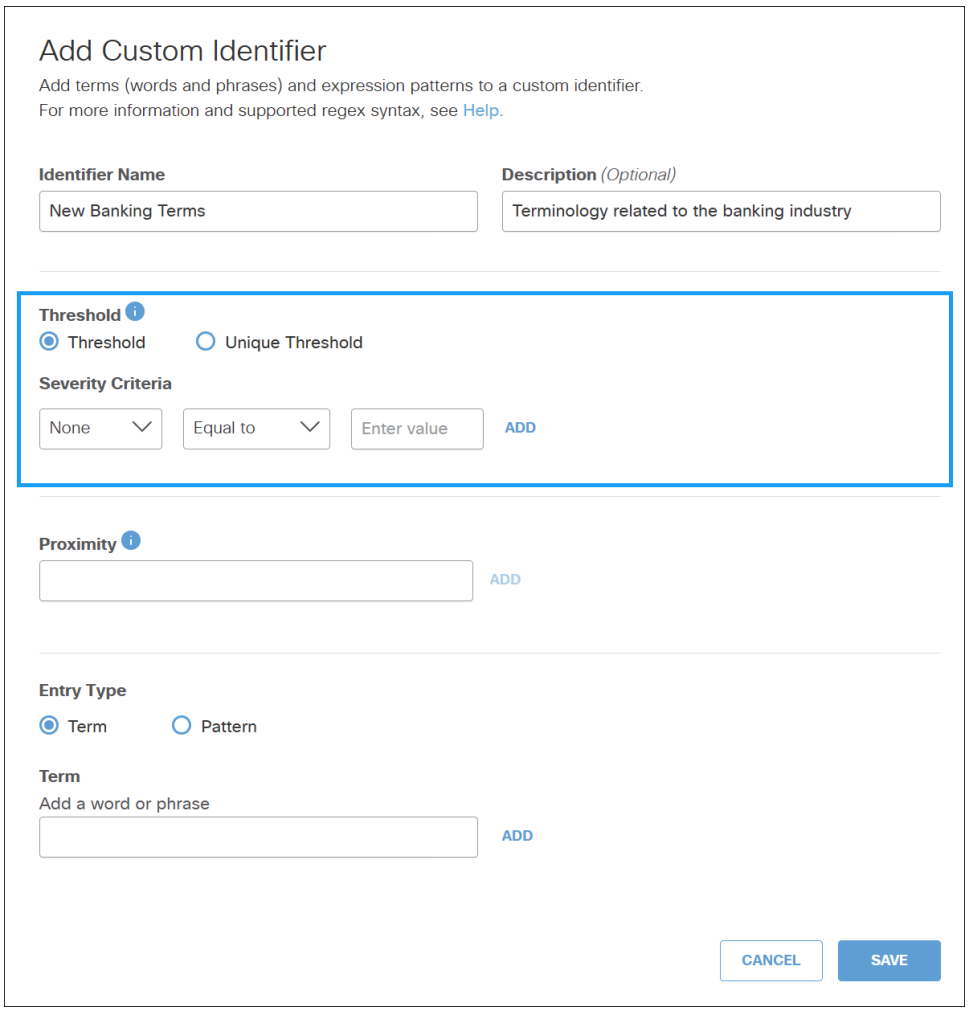
Procedure

---

1. Navigate to **Secure** > **Settings** > **Data Classficiation**.
2. Click **Add Custom Identifier**.
3. Give the custom identifier a meaningful name and description.

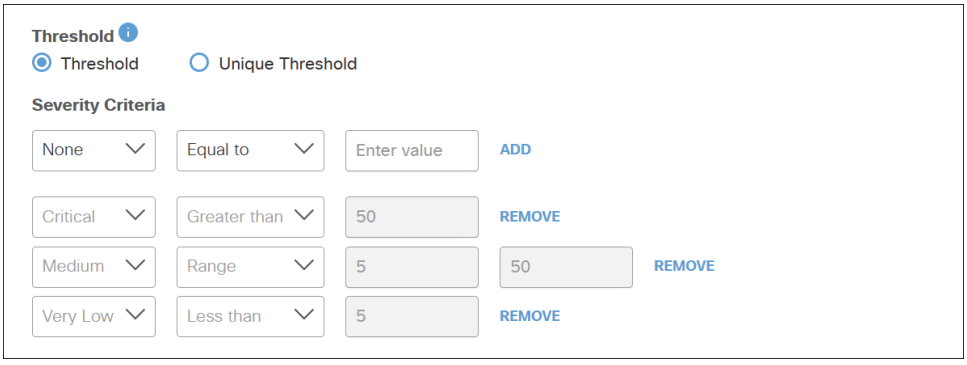


4. (Optional) Select **Threshold** or **Unique Threshold** and then specify the **Severity Criteria**. The **Threshold** value represents the total number of occurrences of this identifier that must be detected in a document for Secure Access to generate an incident. The **Unique Threshold** value represents the number of unique occurrences of this identifier that must be detected in a document for Secure Access to generate an incident. A threshold of 3, for example, only generates an incident if 3 instances of the identifier are found in the file. The default threshold is 1.

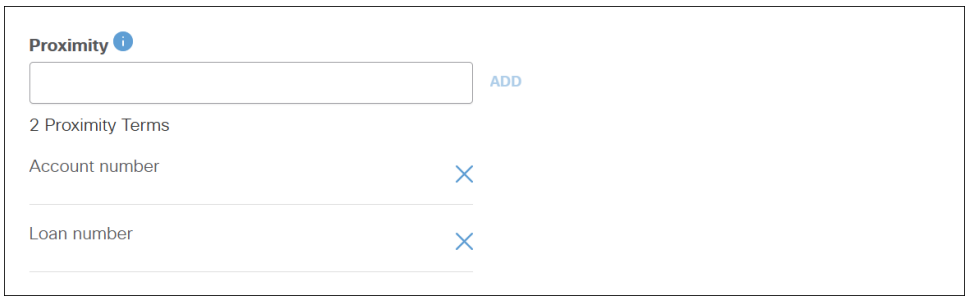


To specify the Severity criteria:

a) Select the severity name from the dropdown list. You can choose a predefined name or select **Custom** and then provide a name.
b) Select the operator to define the value. You can select **Range** to define a range of the threshold value.
c) Enter the threshold value or the range based on the selected operator.



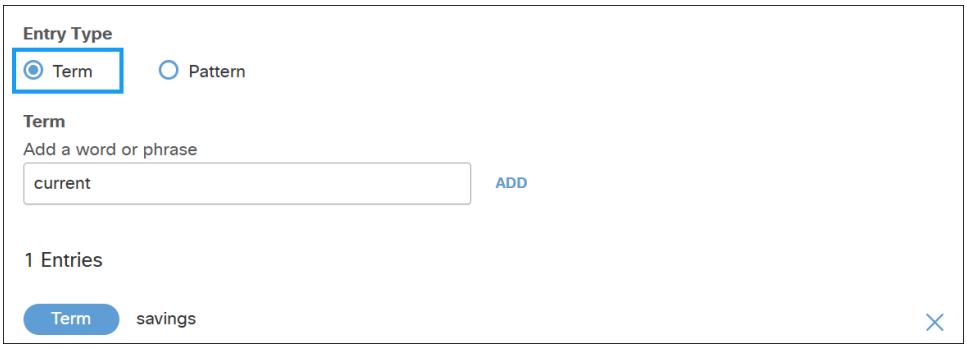
5. (Optional) Specify a proximity keyword and then click **ADD**. You can repeat this step to add up to 10 proximity keywords for your custom identifier. If you specify proximity keywords, Secure Access will not generate an incident unless at least one of the occurrences of a matching term or pattern appears within 20 terms of a proximity keyword.



6. Add terms and patterns to your custom identifier.

> **Note**
>
> You can not upload or enter terms and patterns as a CSV. You must enter each item individually.

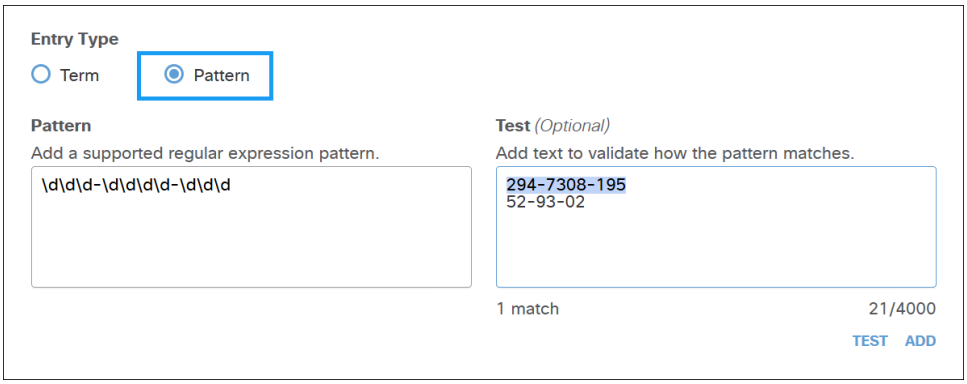
a) For **Terms**, add up to 100 terms and click **ADD** for each term.



b) For **Pattern**, enter a regular expression 3-1,000 characters long. You can add up to 10 patterns to a custom identifier. For more information, see Custom Regular Expression Patterns.

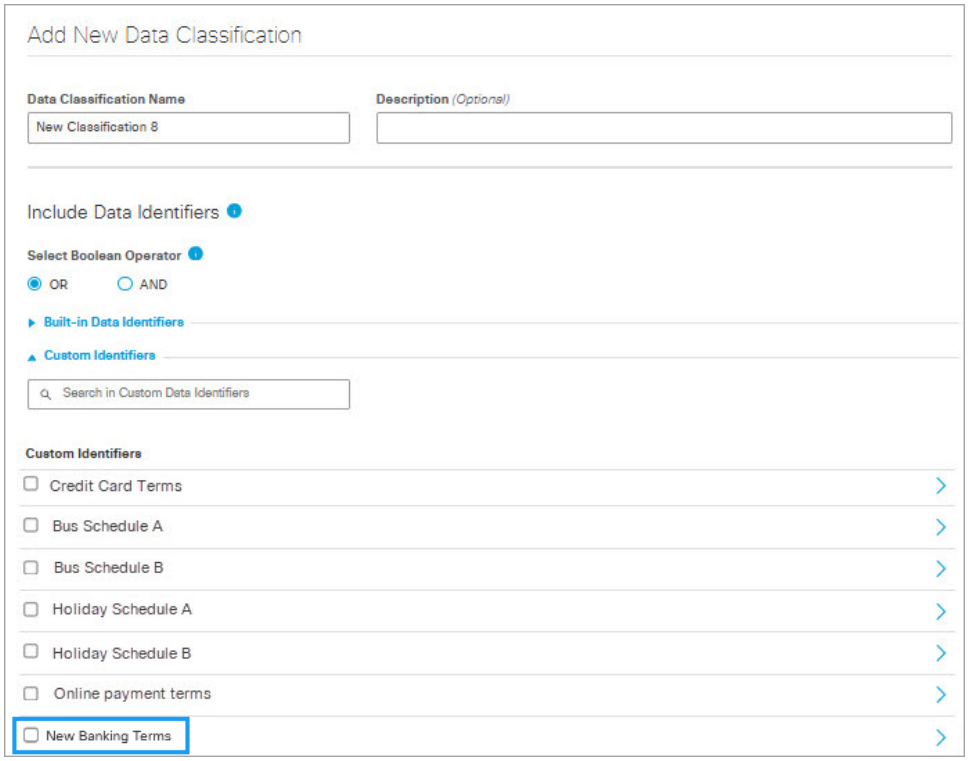
After adding a regular expression, you can enter sample text in the **Test** box, and click **TEST** to verify the pattern matches.

Click **ADD** when you are satisfied that you have the pattern you want.



Enter terms or patterns in the language you want DLP to detect, including text that may be extracted from images by OCR scanning.

7. Click **SAVE**.



What to do next

If you specify both a threshold and proximity keywords, a document is considered a match only if it contains a custom identifier term or pattern that appears at least the number of times indicated by threshold, and at least one of those occurrences appears within 20 terms of at least one of the proximity keywords.

Note

Secure Access blocks documents containing a custom identifier only if the identifier is surrounded by a word boundary. A document containing a custom identifier with an alphanumeric character (a-z, A-Z, 0-9) adjacent to it will not be blocked. For example, for the custom identifier **c.t** matches **cat** and **cot**, but not **housecat** or **citation**.

If you are validating multilingual OCR scanning, you can create separate custom identifiers for each language and then add them to separate or combined data classifications.

Once you create a custom identifier, you can add it to a data classification. To create a data classification, see Create a Data Classification or Copy and Customize a Built-In Data Classification.

Custom Regular Expression Patterns

Describes Custom Regular Expression Patterns in Cisco Secure Access. Custom regular expression patterns for DLP data classifications support basic Java syntax with some limitations.

> **Note**
>
> You must create your own regex. The creation of custom regex is outside the scope of Secure Access Support.

Custom regular expression patterns for DLP data classifications support basic Java syntax with some limitations.

Limitations

General

- A regex can have a maximum of 150 characters.
- A custom dictionary can have a maximum of 10 regex.
- A custom dictionary can have a maximum of 100 entries.
- The minimum length of a regex pattern is 3.
- The maximum number of matches for a regex is 1000.

Regex Syntax

- Anchor Flags
  - `^` can not be used as an input start position.
  - `$` can not be used as an input end position.
- Back References
  - `\n` cannot be used to reference a previous capture group n.

The following must be used for these character definitions:

- Whitespace–`'\u0020'`
- Dash–`'\u002D'`
- Single quote–`(char)0x0027`
- Double quote–`'\u0022'`

Regex Breadth

- Wildcards
  - `.*` and `.+` are not accepted.
  - `()*` and `()+` are not accepted.
- `|` alternations have a maximum of 20 per pattern.

Word Boundary

The regular expression is wrapped in a word boundary to ensure it matches the entire word. Words are comprised of alphanumeric character (a-z, A-Z, 0-9) and the boundary cannot contain a word character on each side of the boundary.

Example:When the regular expression is `cat`, the sentence "The cat chased the mouse" will match, but "The catchased the mouse" will not match.

Individual Data Identifiers

Describes Individual Data Identifiers in Cisco Secure Access and explains Drug Name, Health Condition, and ICD-10 Code. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

These identifiers only appear in combination with other identifiers.

Drug Name

Drug Name is a content identifier that identifies unique drug names as referenced in the "Orange Book" (*Approved Drug Products with Therapeutic Equivalence Evaluations*) published by the US Food and Drug Administration (FDA). It is available from the FDA.

Health Condition

Health Condition is a content identifier that detects health conditions based on a comprehensive dictionary. The dictionary of health conditions is compiled from https://www.cdc.gov/nndss/index.html.

ICD-10 Code

The International Statistical Classification of Diseases and Related Health Problems (ICD) is a classification list compiled by the World Health Organization (WHO) for the purpose of coding diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases. This policy identifies content in the 11th revision of ICD.

US Person Name

Person name is a content identifier used in numerous policies. It is backed by US Census information.

47 AI Guardrails Data Classifications

Topics:

- AI Guardrails Data Classifications

Provides an overview of AI Guardrails Data Classifications in Cisco Secure Access, including AI Guardrails Data Classifications. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

AI Guardrails Data Classifications

Describes AI Guardrails Data Classifications in Cisco Secure Access. AI guardrails data classifications are designed for use in AI Guardrails Rules , which protect against data loss or security violations in prompts and responses and files embedded in prompts exchanged between users and AI applications.

AI guardrails data classifications are designed for use in AI Guardrails Rules , which protect against data loss or security violations in prompts and responses and files embedded in prompts exchanged between users and AI applications. AI guardrails data classifications serve the same purpose as data classifications used in Real-Time and SaaS API rules—they describe the type of data the Data Loss Prevention policy will monitor or block.

AI guardrails rules and data classifications help ensure that AI applications used in your environment adhere to policies and standards you have established. AI guardrails protect your privacy and security, ensure regulatory compliance, and improve customer trust. AI guardrails data classifications focus on three areas of concern to protect your systems:

- Security guardrails protect against prompt injection attacks, ensuring that prompts are safe for the AI model and will not cause the model to perform inappropriate activities such as deleting critical data, exposing sensitive data, or granting unauthorized access to resources in your environment.
- Safety guardrails prevent an AI application from disseminating inaccurate information or information that could be used in a harmful manner, such as instructions for building a bomb or overriding safety precautions in heavy machinery.
- Privacy guardrails prevent the AI application from disseminating personal information identifiers (PII) that may identify an individual, such as financial account numbers, medical records, passport or government identification numbers, or credit card numbers.

Like data classifications use in Real-Time and SaaS API rules, AI guardrails data classifications are groups of data identifiers combined for the purpose of monitoring or blocking closely related content. Data identifiers describe the content the Data Loss Prevention policy monitors or blocks. Secure Access provides a set of built-in AI guardrails data identifiers; you cannot create custom AI guardrails data identifiers. You can use built-in AI guardrails data classifications provided by Secure Access in your AI guardrails rules, or create and use your own customized AI guardrails data classifications.

48 Secure ICAP

Topics:

- Manage Secure ICAP

Provides an overview of Secure ICAP in Cisco Secure Access, including Manage Secure ICAP. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Secure ICAP

Describes Manage Secure ICAP in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Note**
>
> This feature is released under controlled availability. If you wish to enable this feature, contact Secure Access Support for assistance.

You can forward the payload of Realtime DLP violations to on-premises DLP solutions using the secure Internet Content Adaptation Protocol (ICAP). Through ICAP, Secure Access DLP sends the payload that triggers a Realtime rule violation to an on-premises DLP.

To add Secure ICAP integration, define the ICAP server information in Secure Access as described in the Secure ICAP Integration topic.

Once you have established an ICAP connection, by default the payload of all active Realtime DLP rule violations will be sent over ICAP. You can disable this on a rule-by-rule basis; refer to Add a Real Time Rule to the Data Loss Prevention Policy for more information.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- You must have the ICAP server endpoint URI.
- You must have the SSL certificate for the ICAP server.
- Upload your own signed root CA certificate to Cisco Secure Access through the **Secure** > **Certificates** > **Internet destinations** page. The ICAP option is unavailable for configuration until this certificate is uploaded.
- To prevent abuse of the API connection, we recommend you allow only the following IP addresses to your firewall:
  - 3.234.7.118
  - 54.90.48.200
  - 54.153.85.86
  - 184.72.63.136
  - 50.18.191.74
- In addition, EU customers should add the following IP addresses to that list:
  - 3.120.233.38
  - 3.65.158.141
  - 18.168.8.192
  - 18.132.93.175

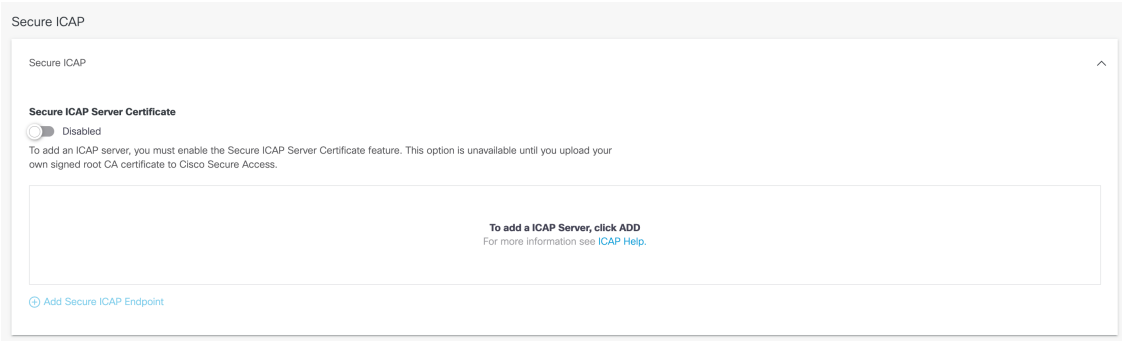
Secure ICAP Integration

This topic describes how to configure a secure ICAP endpoint for data loss prevention and threat inspection.

Secure ICAP integration allows you to extend your existing on premises data loss prevention infrastructure to cloud traffic inspected by Secure Access.

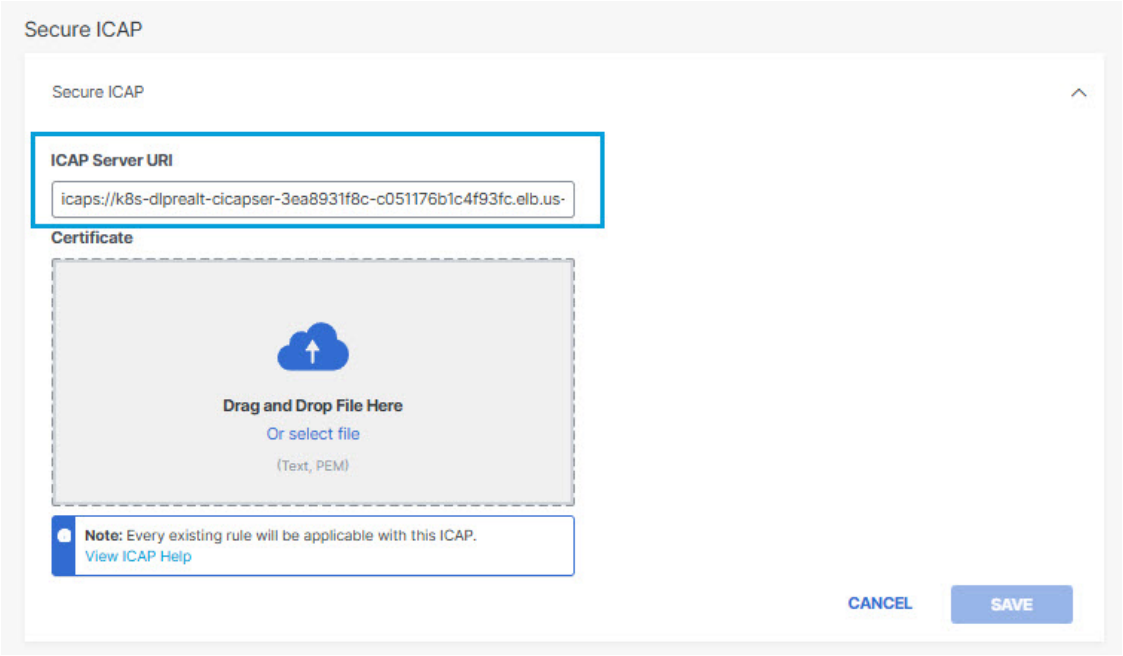
Procedure

1. Navigate to **Admin** > **Authentication**.
2. Expand the **Secure ICAP** section and enable the Secure ICAP Server Certificate feature.



> **Note**
>
> This toggle is unavailable until you upload your own signed root CA certificate to Cisco Secure Access through the **Secure** > **Certificates** > **Internet destinations** page.

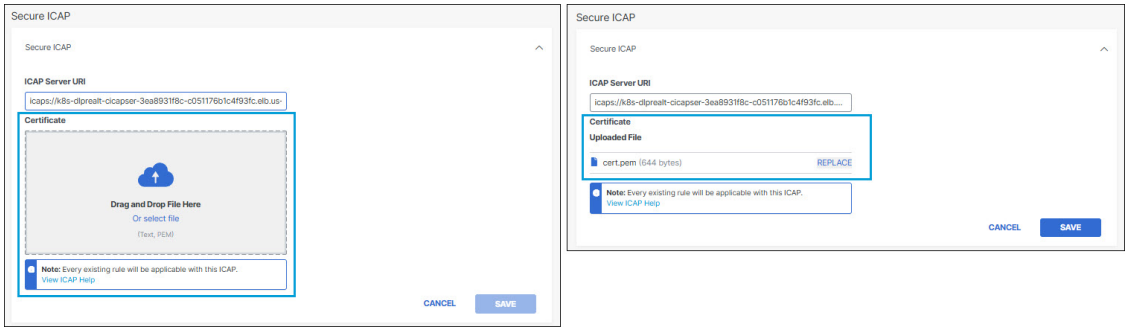
3. Click **Add Secure ICAP Endpoint**.
4. Enter the **ICAP Server Endpoint URI**. (For example, icaps://k8s-dlprealt-cicapser-3ea8931f8c-c051176b1c4f93fc.elb.us-west-1.amazonaws.com:11344/echo).



5. Provide the ICAP server **Certificate** that will be used when the ICAP server requests client authentication. Use one of the following methods:
   - Drag and drop the certificate from your local system to the designated place on the screen.

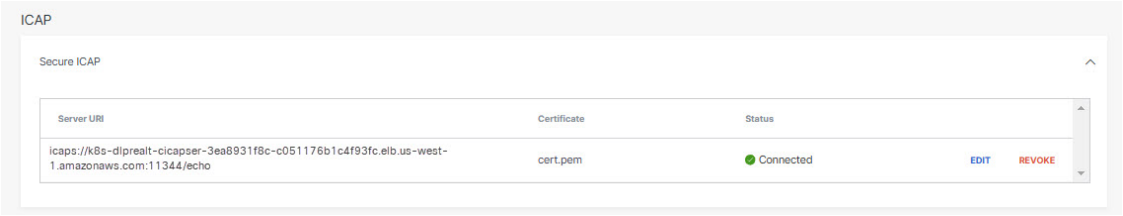
-or-

- Click **Or select file**, navigate to the certificate on your local system, and select the file to upload.



6. Click **Save**.

   The display reflects when the connection is successfully established.



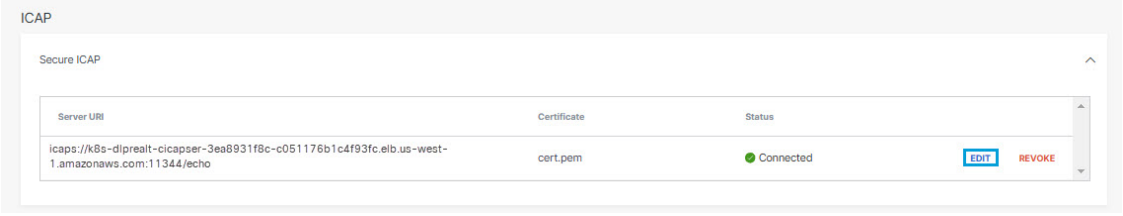
> **Note**
>
> After you configure ICAP settings and establish the ICAP connection, if you remove the signed root CA certificate, the ICAP setting will show as enabled and established, but ICAP events will not be sent to the remote ICAP server.

Modify an ICAP Server Connection

Provides instructions for completing the Modify an ICAP Server Connection workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Click **EDIT** next to the displayed ICAP server connection information.



3. Enter new values for the **ICAP Server Endpoint URI**, the server **Certificate**, or both. (See Steps 3 and 4 of Secure ICAP Integration).
4. Click **SAVE**.

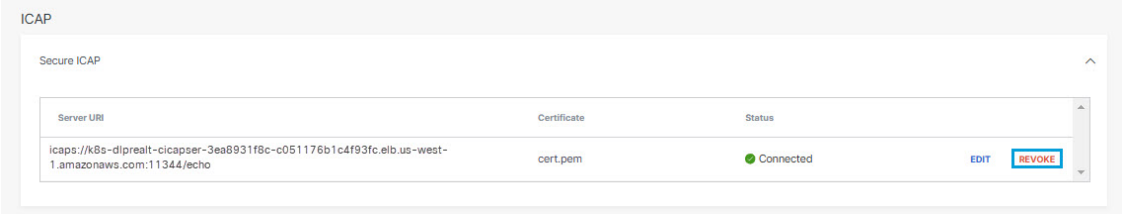
5. The system will attempt to reestablish the connection to the ICAP server with the new parameters and report success or failure.

Disconnect from an ICAP Server

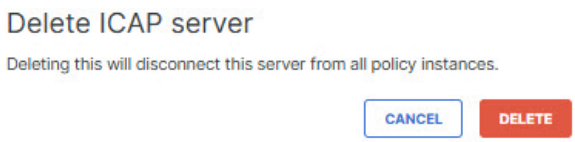
Provides instructions for completing the Disconnect from an ICAP Server workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Choose the ICAP server connection to disconnect and click **REVOKE**.



3. Click **DELETE** to confirm your choice.



4. The system will delete the URI and certificate for the connection; the connection will no longer be available for real time rules that have information sharing through ICAP enabled.

49 Requirements for Salesforce Tenants

Topics:

- Requirements for Salesforce Tenants for Cloud Malware and SaaS API DLP

Provides an overview of Requirements for Salesforce Tenants in Cisco Secure Access, including Requirements for Salesforce Tenants for Cloud Malware and SaaS API DLP. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Requirements for Salesforce Tenants for Cloud Malware and SaaS API DLP

Describes Requirements for Salesforce Tenants for Cloud Malware and SaaS API DLP in Cisco Secure Access. To support Cloud Malware protection or SaaS API Data Loss Prevention for Salesforce tenants, you must meet the requirements listed below.

To support Cloud Malware protection or SaaS API Data Loss Prevention for Salesforce tenants, you must meet the requirements listed below. All of these requirements are referenced from the appropriate topics for authorizing your Salesforce tenants for Cloud Malware protection or SaaS API Data Loss Prevention; they are gathered together here for convenience.

All of these prerequisite activities need be performed only once for any tenant; if you want to support both Cloud Malware and SaaS API DLP for a tenant, you need not do these things twice for that tenant.

- Install or Update `Node.js`. The Salesforce CLI requires `Node.js` to run. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.
- Install the Salesforce CLI. This is the primary tool for interacting with Salesforce orgs and managing Salesforce DX projects.
- Download the Salesforce quarantine package and install it for your Salesforce tenant. This enables Secure Access to support the quarantine response action for Salesforce files.
- Log in to your target Salesforce org.
- Set the appropriate permissions in your Salesforce tenant.

The Salesforce user account to which the which the quarantine package is deployed and permissions are applied must be the same one that will be used to authorize the Salesforce tenant for Cloud Malware Protection and/or SaaS API Data Loss Prevention.

Salesforce sObjects Supported for SaaS API DLP

Describes Salesforce sObjects Supported for SaaS API DLP in Cisco Secure Access. Secure Access SaaS API DLP supports monitoring: the core sObjects listed in the table below.

Secure Access SaaS API DLP supports monitoring:

- the core sObjects listed in the table below.
- any custom sObject that is queryable and has a text field associated with it.

Secure Access supports only the monitor response action (not quarantine) for Salesforce sObjects.

Access	Document Entity Map	Platform Cache Partition Type
Access Share	Duplicate Record Item	Predefined Case Team
Account	Duplicate Record Set	Predefined Case Team Member
Account Contact Role	Email Domain Key	Predefined Case Team Record
Account Share	Email Message	Price Book
Action Link Group Template	Email Service	Price Book Entry
Action Link Template	Email Services Address	Product
Additional Directory Number	Email Template	Profile
Announcement	Endorsement	Push Topic
Apex Class	Endorsement Feed	Queue Sobject

Apex Debug Log
Apex Email Notification
Apex Test Queue Item
Apex Trigger
AppMenuItem
Approval Request
Asset
Attachment
Aura Component Bundle
Auth Session
Auth. Provider
Badge
Badge Feed
Badge Received
Badge Share
Business Hours
Business Process
CORS Whitelist Origin
Call Center
Campaign
Campaign Member
Campaign Member Status
Case
Case Comment
Case Contact Role
Case Solution
Case Team Member
Case Team Member Role
Category Data
Category Node
Chatter invitation
Client Browser
Contact
Content Delivery
Content Document
Entity Subscription
Event
Event Relation
External Data User Authentication
Feed Comment
Feed Item
Field Permissions
Flow Interview
Flow Interview Share
Folder
Forecasting Share
Goal
Goal Share
Group
Group Member
Group Member Request
Group Record
Holiday
Idea
Lead
Letterhead
Library Document
Lightning Component Definition
List View Chart
Login IP
Macro
Macro Instruction
Macro Share
Mail Merge Template
Note
Object Permissions
Opportunity
Opportunity Contact Role
Opportunity Product
Opportunity Share
Quick Text
Quick Text Share
Recently Viewed
Record
Record Type
Role
Setup Entity Access
Skill
Skill Feed
Skill Share
Skill User
Skill User Feed
Social Persona
Social Post
Social Post Feed
Social Post Share
Solution
Static Resource
Streaming Channel
Streaming Channel Share
Task
Tenant Secret
Thanks
Thanks Share
Topic
Topic Feed
Trial Template
TxPolicyGroup
TxPolicyMember
User
User List View
User List View Criteria
User Login
User Package License
User Provisioning Account

Content Document Link	Opportunity: Competitor	User Provisioning Account Staging
Content Folder	Order	User Provisioning Config
Content Folder Member	Order Feed	User Provisioning Log
Content Version	Order Product	User Provisioning Mock Target
Contract	Order Product Feed	User Provisioning Request
Contract Contact Role	Organization	User Provisioning Request Share
Custom Brand	Organization-wide From Email Address	User Share
Customer Brand Asset	Partner	UserAppMenuCustomization
Custom Button or Link	Permission Set	UserAppMenuCustomization Share
Custom S-Control	Permission Set Assignment	Visualforce Component
Daily Record View	Permission Set License Assignment	Visualforce Page
Document	Platform Cache Partition	

Install or Update `Node.js`

Provides instructions for completing the Install or Update Node.js workflow in Cisco Secure Access. We recommend using Node.js 18.x or higher; Node.js 20.x is preferred.

The Salesforce CLI requires `Node.js` to run.

We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.

Procedure

1. Check your current `Node.js` version:
   a) Open your terminal or command prompt and run `node -v`.
   b) If you see a version number (e.g., v18.17.0), you have `Node.js` installed.
      - If you have `Node.js` 18.x or higher , you can skip this task.
      - If the version is below 18.x , or if the command is not found, you need to install or update `Node.js`; proceed to Step 2.

2. Install/update `Node.js` using one of two methods:
   - Using the Node Version Manager (NVM).

     This method allows you to easily switch between different `Node.js` versions, which can be useful if you work on multiple projects with different requirements. To install `Node.js` using NVM, proceed to Step 3.
   - Using the direct installer.

     This is a simple installation suitable if you expect to use a single version of `Node.js`. To install `Node.js` using the direct installer, proceed to Step 4.

3. Install `Node.js` using the Node Version Manager (NVM).
   a) Install NVM using the instructions at the NVM GitHub repository:
      - For macOS/Linux

- For Windows

b) Close and reopen the terminal or command window.
c) Run `nvm install X`. (Where *X* is the desired version number of NVM.)
d) Run `nvm use X`. (Where *X* is the desired version number of NVM.)
e) Run `node -v` to confirm you have the desired version of `Node.js` installed.

4. Install `Node.js` using the direct installer.
   a) Go the official `Node.js` website.
   b) Download the "LTS" (Long Term Support) version installer for your operating system. (This is usually the most stable and recommended version.)
   c) Run the installer and follow the prompts.
   d) Close and reopen the terminal or command window.
   e) Run `node -v` to confirm you have the desired version of `Node.js` installed.

Install the Salesforce CLI

Provides instructions for completing the Install the Salesforce CLI workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Salesforce Command Line Interface (CLI) is the primary tool for interacting with Salesforce orgs and managing Salesforce DX projects.

Before you begin

- Install or Update `Node.js`. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.

Procedure

1. Open a terminal or command prompt window
2. Go to the official Salesforce CLI website.
3. Download the appropriate installer for Windows, macOS, or Linux.
4. Run the installer and follow the prompts.
5. Close and reopen the terminal or command prompt window.
6. Run `sf --version` to confirm you have the desired version of the Salesforce CLI installed.

You should see the installed Salesforce CLI version number. If you see an error, ensure the CLI is added to your system's `PATH` and try again.

Deploy the Salesforce Quarantine Package to your Salesforce Tenant

Provides instructions for completing the Deploy the Salesforce Quarantine Package to your Salesforce Tenant workflow in Cisco Secure Access. You must have full admin access in a Salesforce Enterprise account.

Before authorizing a Salesforce org as a tenant for Cloud Malware protection or SaaS API Data Loss Prevention you must assign the proper permissions and deploy the Salesforce quarantine package to the Salesforce admin user account that will be used to authorize the tenant. This allows the quarantine response action to function in your environment.

> **Note**
>
> If the Salesforce tenant authorization is revoked and then restored with a new admin user, that admin user will need the same permissions enabled and the quarantine package will need to be deployed for that user.

You need to do this only once for any Salesforce tenant; if you want to support both Cloud Malware and SaaS API DLP for a tenant, you need not do it twice for that tenant.

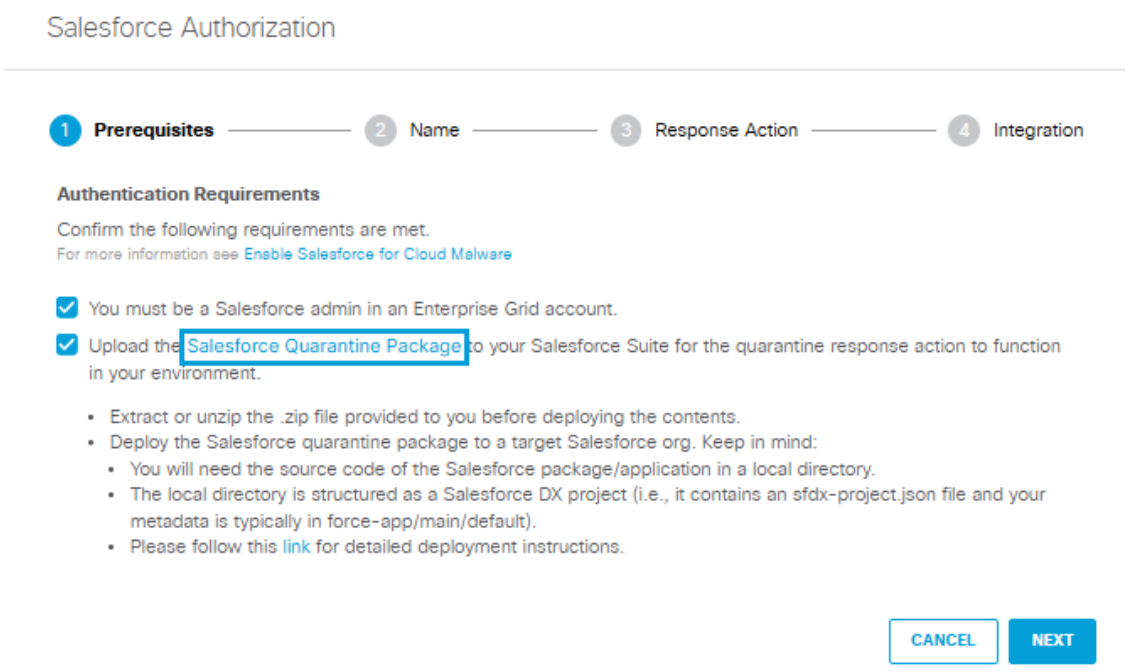
Before you begin

- You must have full admin access in a Salesforce Enterprise account.
- You must install or update `Node.js`. The Salesforce CLI requires `Node.js` to run. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.
- You must have the Salesforce CLI installed.

The Salesforce user account to which the quarantine package is deployed must be the same one that will be used to authorize the Salesforce tenant for Cloud Malware protection and/or SaaS API Data Loss Prevention.

Procedure

1. Upload the Salesforce qurantine package to your local device. Use the link provided in the Secure Access UI in the first step of the Salesforce authorization process for Cloud Malware protectionor the Salesforce authorization process for SaaS API Data Loss Prevention:



   The uploaded file is a signed `.zip` file.

2. Extract or unzip the `.zip` file. Confirm the contents:
   - A signed `QuarantineApp_x.y.z.zip` file.

- A `.sig` file.
- An sha256 manifest file.
- A python script to verify the signed package.
- A `README` file describing how to use the verification script.

3. Extract or unzip the `QuarantineApp_x.y.z.zip` file.

   Confirm the contents: `.cls`, `.xml`, and `.json` files.

4. The extracted package is structured as a Salesforce DX project.
   - The directory must contain an `sfdx-project.json` file.
   - Your metadata should reside in `force-app/main/default`.

5. Set your current directory to the Salesforce DX project directory.
6. Log in to your Salesforce org.
7. Run the deploy command:

   ```
   sf project deploy start --target-org MyTargetOrg --source-dir force-app
   ```

   Where *MyTargetOrg* is an alias for your authorized org.

   This command deploys all metadata from your project's default package directory (usually `force-app/main/default`) to the target org you specify. The CLI will display the deployment progress, including the status of components being deployed, any warnings, and errors.

8. If you have deployed to a sandbox environment, you must run local tests to confirm successful deployment. Run the command:

   ```
   sf apex run test --target-org MyTargetOrg --test-level RunLocalTests
   --code-coverage --result-format human --synchronous
   ```

   Where *MyTargetOrg* is an alias for your authorized org.

   If an error appears, Contact Support.

9. Return to Enable Cloud Malware Protection for Salesforce Tenants or Enable SaaS API Data Loss Prevention for Salesforce Tenants to complete the authorization process for your Salesforce tenant.

Log In to Your Salesforce Org

Provides instructions for completing the Log In to Your Salesforce Org workflow in Cisco Secure Access. You must have full admin access in a Salesforce Enterprise account.

You must log into a Salesforce org in order to run CLI commands that require access to the org.

Before you begin

- You must have full admin access in a Salesforce Enterprise account.
- You must install or update `Node.js`. The Salesforce CLI requires `Node.js` to run. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.
- You must have the Salesforce CLI installed.

The Salesforce user account to which the quarantine package is deployed must be the same one that will be used to authorize the Salesforce tenant for Cloud Malware protection and/or SaaS API Data Loss Prevention.

Procedure

1. Open a local terminal or command prompt.
2. Navigate and set the current directory to your Salesforce DX project directory (this is the folder containing your `sfdx-project.json` file).
3. Run the authorization command to initiate a web-based login flow:

   ```
   sf org login web --alias MyTargetOrg
   ```

   Where *`MyTargetOrg`* is an alias for your authorized org. You can use this alias in future CLI commands to easily refer to it without citing its full username.

   Note

   If your target Salesforce org is a sandbox environment, use the command

   ```
   sf org login web --alias MyTargetOrg --instance-url sandbox-instance-url
   ```

   Where:

   - *`MyTargetOrg`* is an alias for your authorized org.
   - *`sandbox-instance-url`* is the URL for your sandbox org.

4. A browser window will open, prompting you to log in to your Salesforce org. Enter your username and password for the target org.
5. After successful login, you will be prompted to allow access for the Salesforce CLI. Click **Allow**.

Example

Once authorized, your terminal will display a success message confirming the alias and username of the authorized org.

Set Permissions in Salesforce

Provides instructions for completing the Set Permissions in Salesforce workflow in Cisco Secure Access. You must have full admin access in a Salesforce Enterprise account.

Before authorizing a Salesforce org as a tenant for Cloud Malware protection or SaaS API Data Loss Prevention you must assign the proper permissions and deploy the Salesforce quarantine package to the Salesforce admin user account that will be used to authorize the tenant. This allows the quarantine response action to function in your environment.

The Salesforce admin user authorizing the tenant must have the System Administrator or equivalent role, with the following permissions enabled:

- Systems permissions:
  - View All Data
  - Modify All Data
  - Query All Files
- Custom permission set "Cisco Secure Access SF Quarantine Admin"

> **Note**
>
> If the Salesforce tenant authorization is revoked and then restored with a new admin user, that admin user will need the same permissions enabled and the quarantine package will need to be deployed for that user.

You need to do this only once for any Salesforce tenant; if you want to support both Cloud Malware and SaaS API DLP for a tenant, you need not do it twice for that tenant.

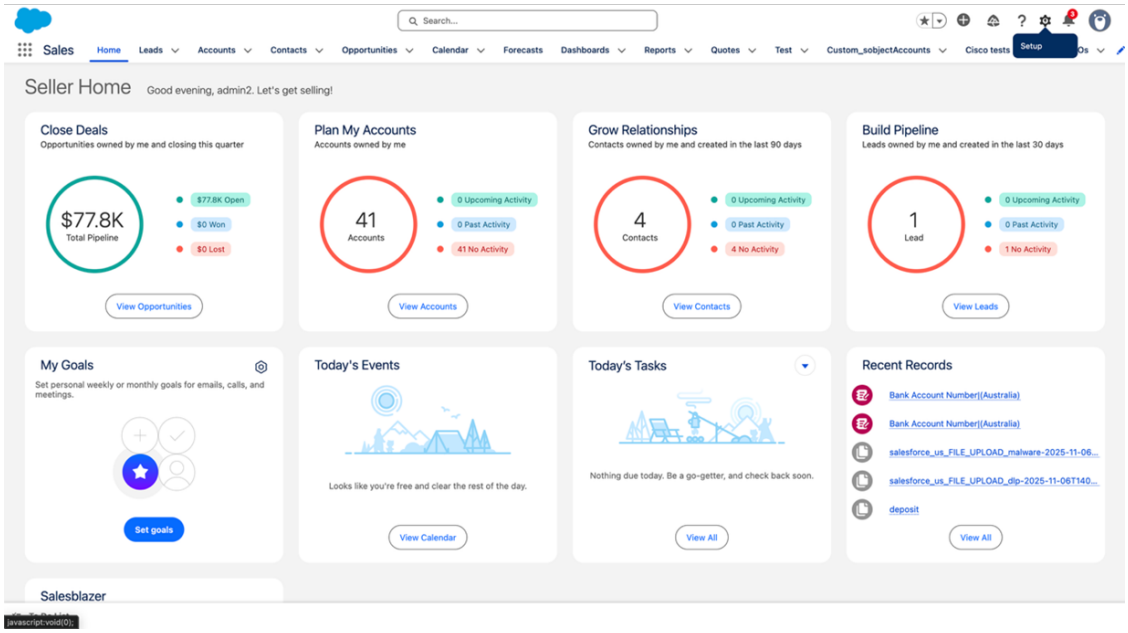
Before you begin

- You must have full admin access in a Salesforce Enterprise account.

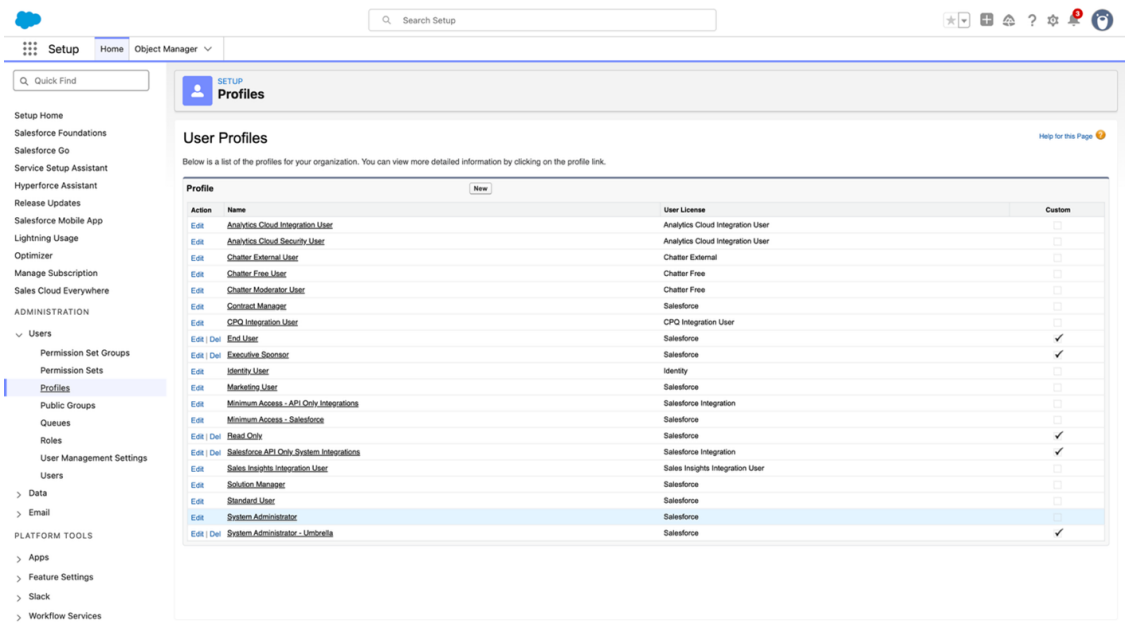
The Salesforce user account to which the permissions are applied must be the same one that will be used to authorize the Salesforce tenant for Cloud Malware protection and/or SaaS API Data Loss Prevention.

Procedure

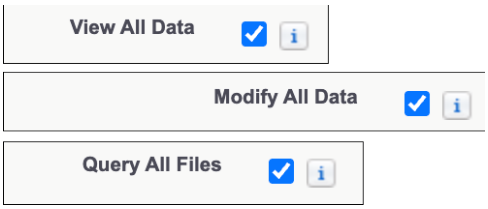
1. Log into your Salesforce Enterprise org with an account that has full admin access.
2. Select **Setup** > **Users** > **Profiles**.



3. Locate and view the profile for the Salesforce admin user to authorize the Salesforce tenant.



4. Find and click **System Permissions**.
5. If disabled, enable the following permissions:
   - View All Data
   - Modify All Data
   - Query All Files



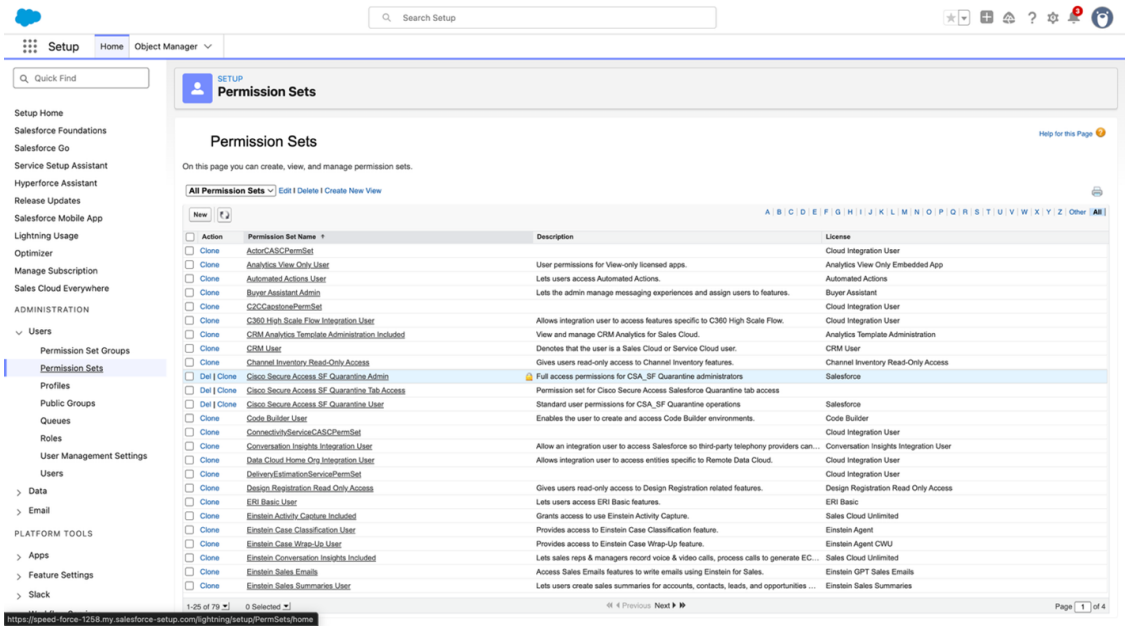
   - Approve Uninstalled Connected Apps

     This permission can be assigned only to users with a full Salesforce user license. It is not available for users with Salesforce Platform or other limited-access licenses.

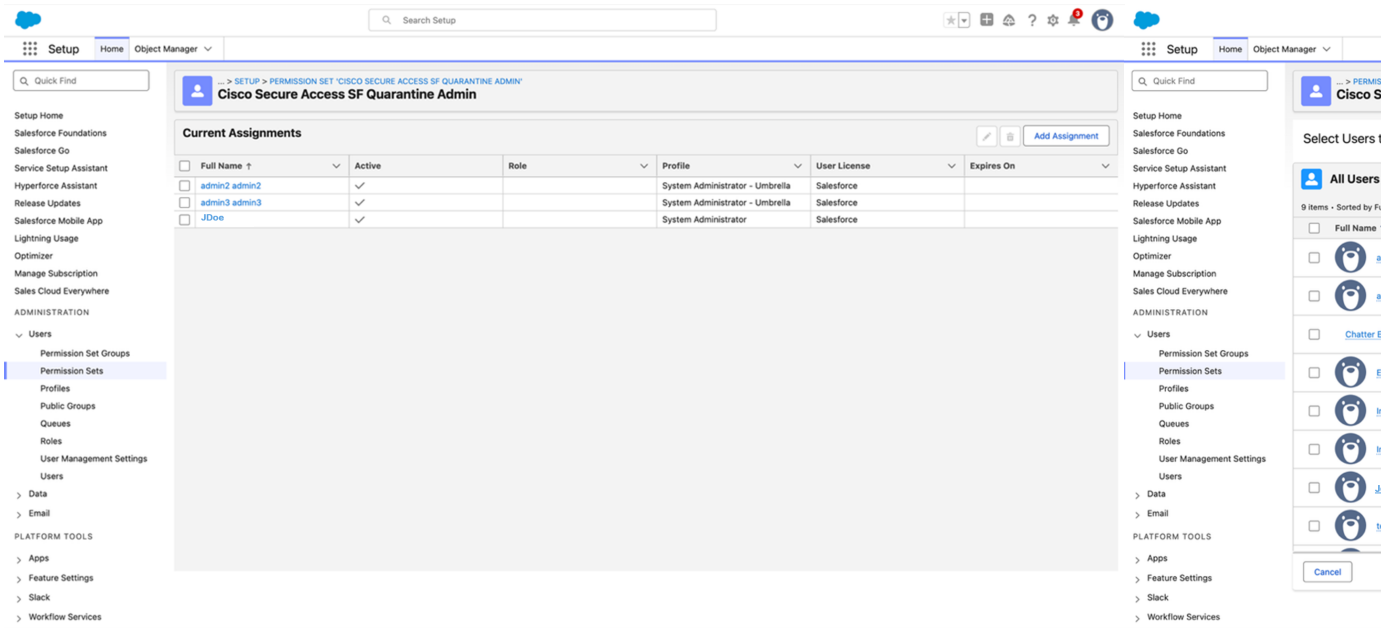
6. If the API Access Control permission is enabled, allow the app Cisco Secure Access DLP.
7. Find and click **Custom Tab Settings**.



8. Locate **Cisco Secure Access SF Quarantines** and set the value to **Default On**.
9. Click **Save**.
10. Find and click **Permission Sets**.



11. Locate and click **Cisco Secure Access SF Quarantine Admin**.
12. Click **Manage Assignments**.
13. Click **Add Assignment**.
14. From the list of users, select the Salesforce administrator to authorize the Salesforce tenant, then click **Next**.



15. Click **Assign**.

50 SaaS API Data Loss Prevention

Topics:

- Manage SaaS API Data Loss Prevention
- Enable SaaS API Data Loss Prevention for AWS Tenants
- Enable SaaS API Data Loss Prevention for Azure Tenants
- Enable SaaS API Data Loss Prevention for Box Tenants
- Enable SaaS API Data Loss Prevention for Confluence Tenants
- Enable SaaS API Data Loss Prevention for Dropbox Tenants
- Enable SaaS API Data Loss Prevention for GitHub Tenants
- Enable SaaS API Data Loss Prevention for Google Drive Tenants
- Enable SaaS API Data Loss Prevention for Jira Tenants
- Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants
- Enable SaaS API Data Loss Prevention for Salesforce Tenants
- Enable SaaS API Data Loss Prevention for Salesforce Commerce Tenants
- Enable SaaS API Data Loss Prevention for ServiceNow Tenants
- Enable SaaS API Data Loss Prevention for Slack Tenants
- Enable SaaS API Data Loss Prevention for Webex Teams

Provides an overview of SaaS API Data Loss Prevention in Cisco Secure Access, including Manage SaaS API Data Loss Prevention and Enable SaaS API Data Loss Prevention for AWS Tenants. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage SaaS API Data Loss Prevention

Describes Manage SaaS API Data Loss Prevention in Cisco Secure Access. The Data Loss Prevention (DLP) policy helps to protect sensitive data uploaded to the web.

The Data Loss Prevention (DLP) policy helps to protect sensitive data uploaded to the web. It can discover and protect sensitive data stored and shared in your cloud-sanctioned applications. Granting Secure Access permissions to the APIs of customers' cloud tenants allows for discovering malicious files and files with data violations. You can enable more than one tenant of a supported platform. For example, a school administrator, with an instance of Box for faculty and another instance for students, can enable both tenants. This results in complete malware protection and data loss prevention for Box.

> **Note**
>
> Secure Access does not save the tenant credentials. For revocation and re-authorization, insert the credentials again.

You can authorize the following platforms, all of which have support for both Cloud Malware and DLP.

- **AWS S3** - Cloud Malware and Data Loss Prevention
- **Azure Storage** - Cloud Malware and Data Loss Prevention
- **Box** - Cloud Malware and Data Loss Prevention
- **Confluence** - Cloud Malware and
- **Dropbox** - Cloud Malware and Data Loss Prevention
- **Google Drive** - Cloud Malware and Data Loss Prevention
- **Jira** - Cloud Malware and Data Loss Prevention
- **Microsoft 365 (Sharepoint, OneDrive, and Outlook)** - Cloud Malware and Data Loss Prevention

  > **Note**
  >
  > For Microsoft Outlook, SaaS API Data Loss Protection applies to the outgoing messages folder only. For messages in the incoming mail folder you can enable Cloud Access Security Broker Protection; see Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants.

- **Salesforce** - Cloud Malware and Data Loss Prevention.
- **Salesforce Commerce** - Data Loss Prevention.
- **ServiceNow** - Cloud Malware and Data Loss Prevention
- **Slack** - Cloud Malware and Data Loss Prevention
- **Webex Teams** - Cloud Malware and Data Loss Prevention

Enable SaaS API Data Loss Prevention for AWS Tenants

Provides instructions for completing the Enable SaaS API Data Loss Prevention for AWS Tenants workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To apply DLP SaaS API rules to files in an AWS tenant, you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when the system finds data in violation of an enabled SaaS API rule it will enforce the action of that rule. To enable this feature:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- You must have an active AWS tenant and the person doing the installation must be an AWS Administrator.
- You must Enable CloudTrail Event Logging for S3 Buckets and Objects from the AWS console. (You need enable this feature only once for your account; you need not do it for each AWS tenant you authorize.)
- You must Obtain your AWS Account ID.
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).

Procedure

1. Enable CloudTrail Event Logging for S3 Buckets and Objects from the AWS console. (You need only enable this feature once for your account; you need not do it for each AWS tenant you authorize.)
2. Authorize an AWS Tenant in Secure Access.
3. For each region within which your tenant has resources deployed, Create an AWS Stack from the AWS console.

What to do next

An AWS account can support at most one Cloud Malware tenant and one SaaS API DLP tenant at the same time. You cannot authorize multiple SaaS API DLP tenants for a single AWS account.

- A tenant that fails to authenticate cannot be deleted.

Enable CloudTrail Event Logging for S3 Buckets and Objects

Provides instructions for completing the Enable CloudTrail Event Logging for S3 Buckets and Objects workflow in Cisco Secure Access. We require that you enable CloudTrail event logging to provide you with a record of activities in your AWS account.

We require that you enable CloudTrail event logging to provide you with a record of activities in your AWS account. You need enable this feature only once for your account; you need not do it for each AWS tenant you authorize.

Procedure

1. In the AWS console, navigate to **CloudTrail** and choose **Create Trail**.



2. Provide a meaningful **Trail name** for your trail.

3. Under **Events**, choose **Data Events** to log data events.
4. For **Storage location**, choose **Use existing S3 bucket**, and choose **Browse** to choose an S3 bucket in your account.
5. You may optionally choose to enable **Log file SSE KMS encryption** for your log files. (If you choose this option, see Step 11.)
6. On the**Choose log events** page, choose **Data events**.
7. For **Data event source** choose **S3**.
8. You can choose from:
   - **Log all current and future S3 buckets** (This is the default.)

     Choose to log **Write** events.
   - **Individual bucket selection** (This can be a more economical choice.)

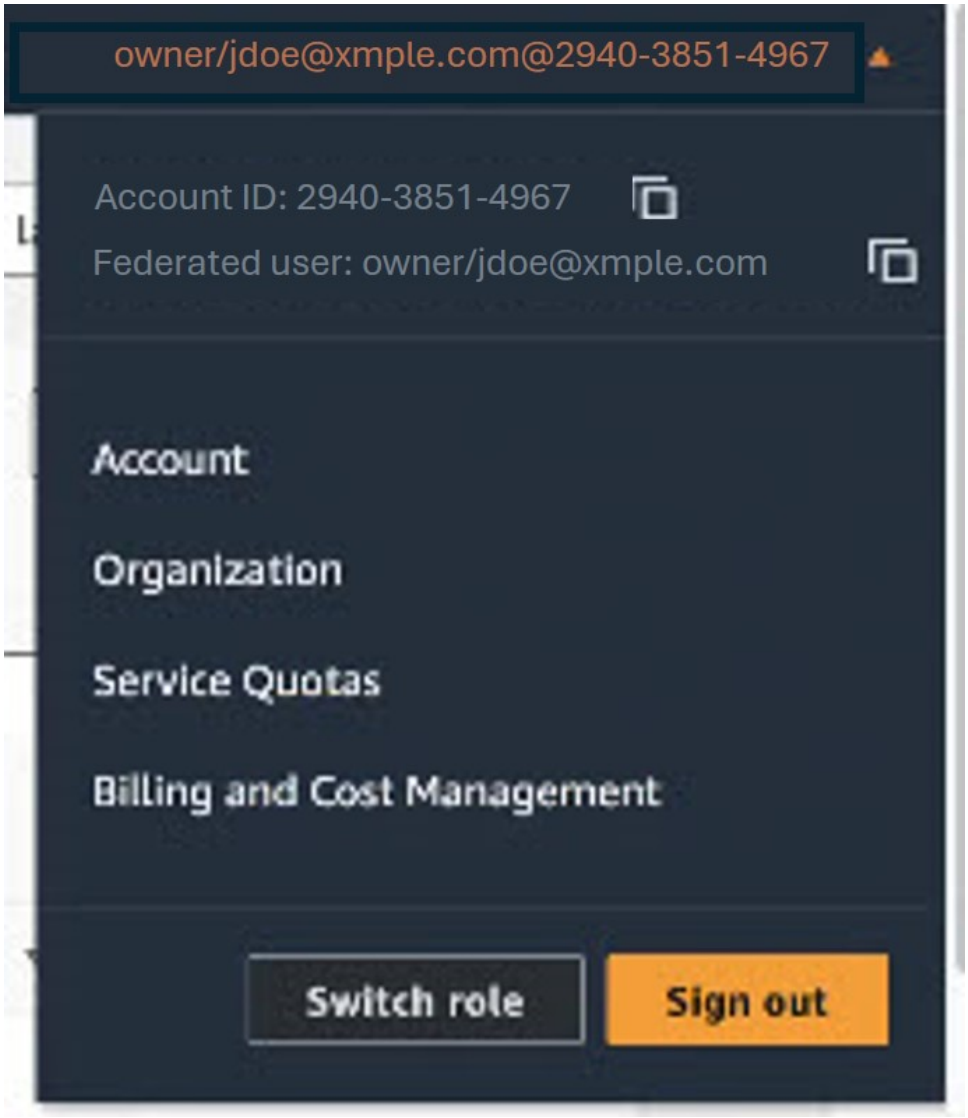
     Browse for existing buckets and click **Add bucket** to log data events for each. Choose to log **Write** events.
9. For the remaining options in the CloudTrail creation wizard, choose the settings appropriate to your environment.
10. On the **Review and Create** page, review your choices and **Edit** if necessary. Then click **Create Trail**.
11. If in Step 5 you chose to enable **Log file SSE KMS encryption** for your log files, grant permission for the encryption key to the role **CiscoSecureAccessScanner**. In the AWS console, under **Key Management Service (KMS)** > **Customer managed keys** > **Key ID** > **Edit key policy**, add a statement to grant permission for the role **CiscoSecureAccessScanner**.
12. If your S3 buckets have restrictive policies associated with them, add statements to those policies to grant the role **CiscoSecureAccessScanner** access to those buckets. In the AWS console, see **Amazon S3** > **Buckets** > > **Bucket Name** > **Permissions** > **Bucket Policy**.

Obtain Your AWS Account ID

Provides instructions for completing the Obtain Your AWS Account ID workflow in Cisco Secure Access. Log in to the AWS Management Console with an Admin account.

Procedure

1. Log in to the AWS Management Console with an Admin account.
2. In the navigation bar at the upper right, click on your user name. The account ID is displayed above your user name.
3. Click the **Copy** icon to the right of the Account ID to copy it.

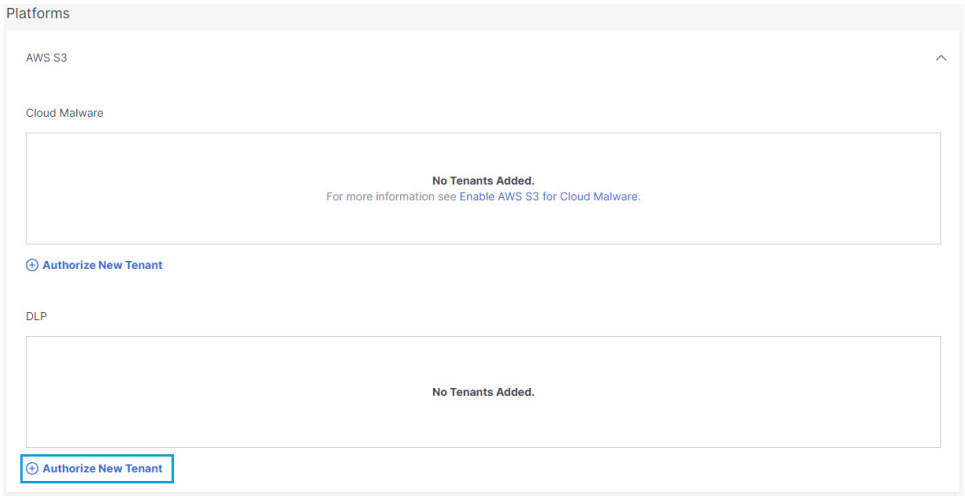


Authorize an AWS Tenant

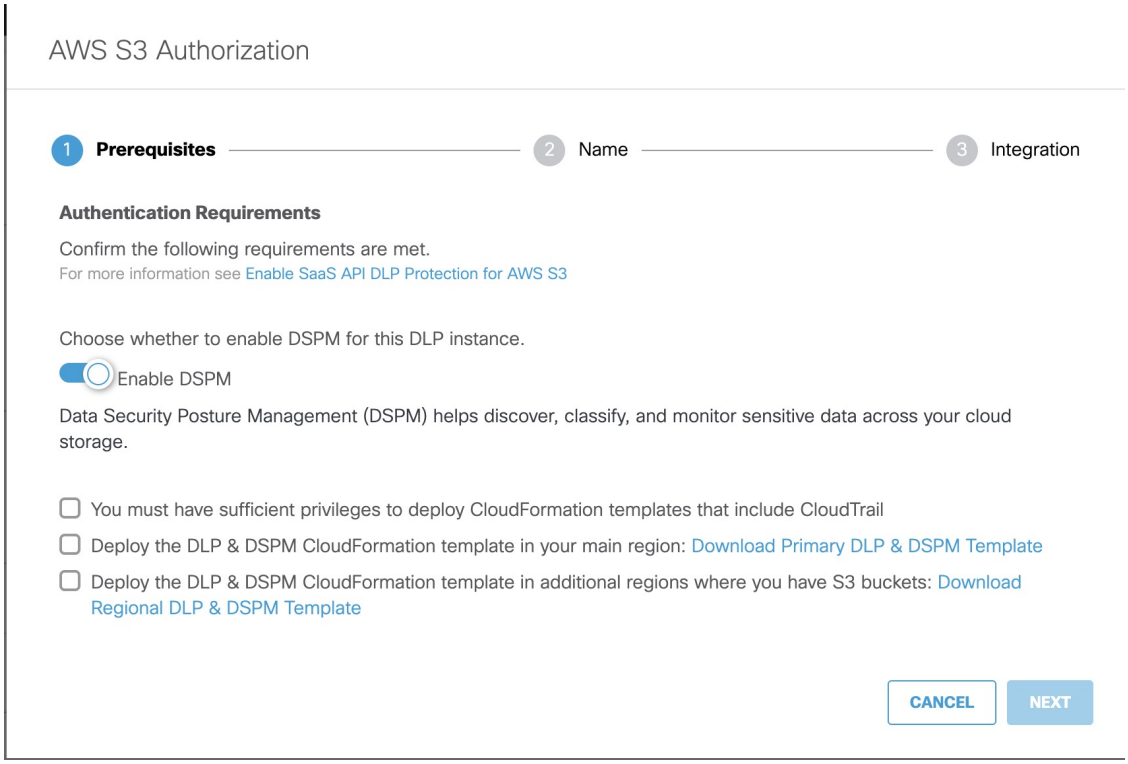
Provides instructions for completing the Authorize an AWS Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click to expand **AWS S3**.
3. In the **DLP** subsection, click **Authorize New Tenant** to add an AWS tenant to your Secure Access environment.



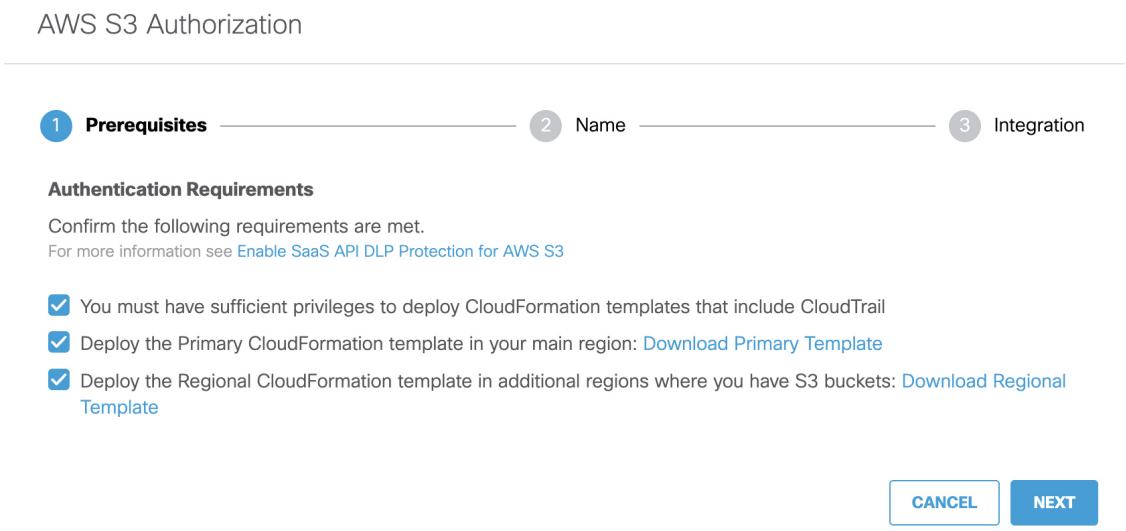
4. In the **AWS S3 Authorization** dialog, click **Download Primary Template** to download an AWS CloudFormation template for your main region (**primary-cloudformation-template.json**). If you have S3 buckets in additional regions, click **Download Regional Template** to download an AWS Cloudformation template for those regions (**regional-cloudformation-template.json**). Save the templates to your local machine, and for each region where you have S3 buckets, Create an AWS Stack before proceeding to the next step.



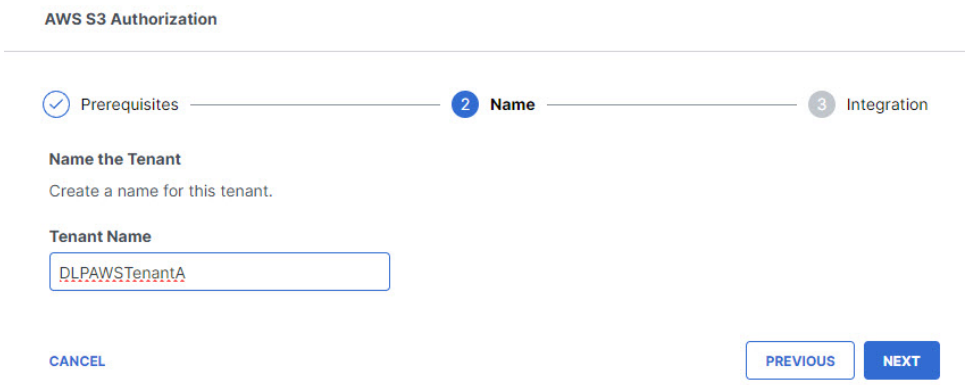
> **Note**
>
> If you enable both DLP and Cloud Malware protection for a region, a single stack can serve for both purposes. If you have already created an AWS stack for Cloud Malware protection, you do not need to create another.

> **Note**
>
> You can enable DSPM at this step. This authorizes the tenant for SaaS API DLP workflows and Data Security Posture Management discovery and posture assessment.

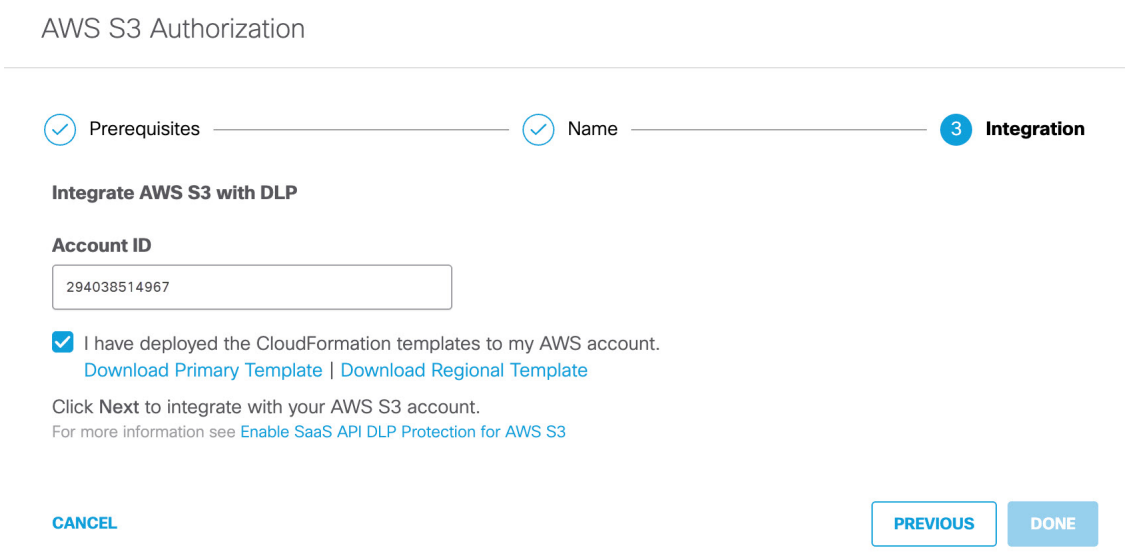
5. In the **AWS S3 Authorization** dialog, check the checkboxes to verify you have created an AWS stack and then click **Next**.



6. Enter a name for your tenant that is meaningful within your environment, then click **Next**.



7. Paste your AWS Account ID in the text box, confirm that you have deployed template(s) to create the necessary AWS stack(s), and click **Done**. (It may take up to 24 hours for the integration to be confirmed and appear as Authorized on the Authentication page.)



Create an AWS Stack

Provides instructions for completing the Create an AWS Stack workflow in Cisco Secure Access. Secure Access requires an AWS stack for each AWS region where you have S3 resources, to monitor and communicate with those resources.

Secure Access requires an AWS stack for each AWS region where you have S3 resources, to monitor and communicate with those resources. If you have more than one AWS tenant, you will need a stack for each region within which each tenant has resources deployed. If you enable both DLP and Cloud Malware protection for a region, a single stack can serve for both purposes.

Note

If you enable both DLP and Cloud Malware protection for an AWS region, and then disable one of those two forms of protection, you must leave the stack intact to support the remaining protection.

Important

Perform this task for each region your tenant accesses, after you have downloaded a CloudFormation Template in Step 4 of Authorize an AWS Tenant. Once you have created the stack, return to Step 5 of that task.

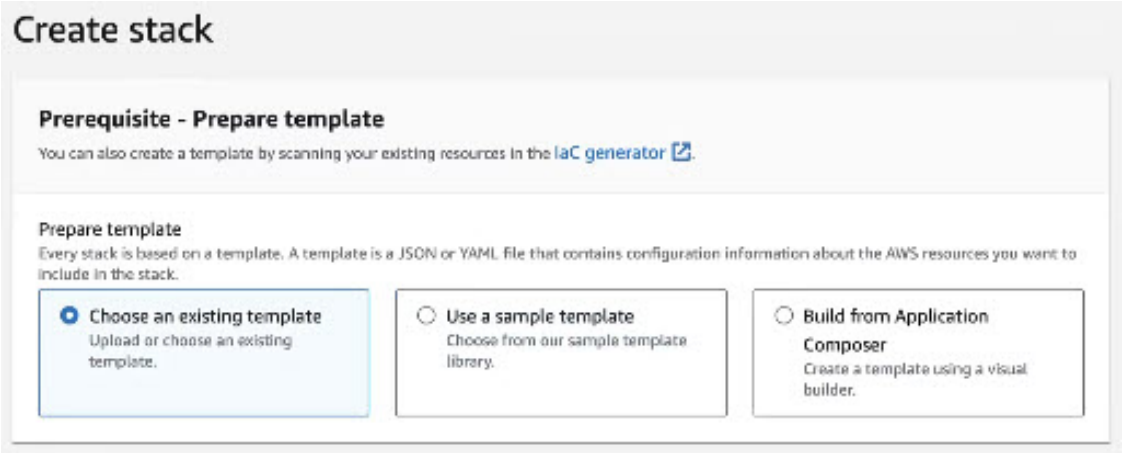
For more information about AWS Stacks, see the Amazon AWS Cloud Formation User Guide.

Procedure

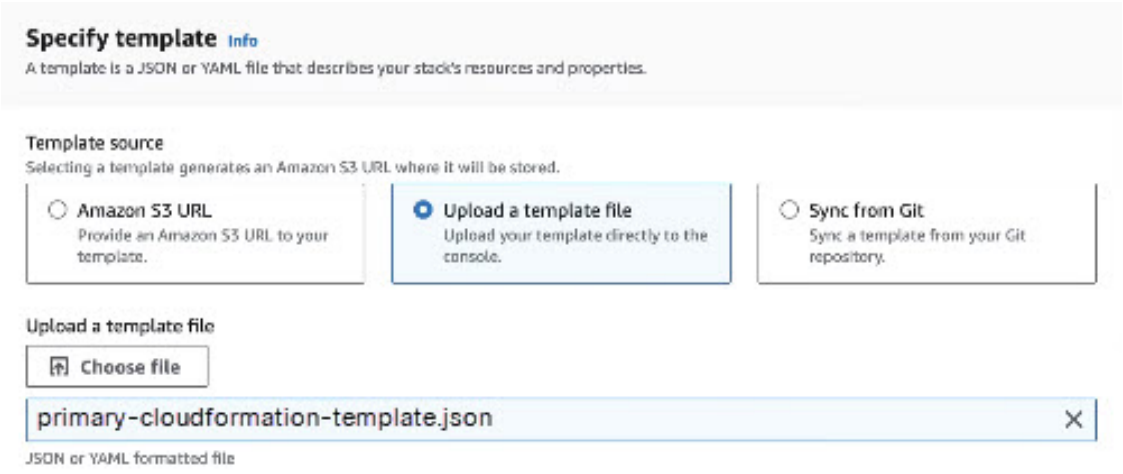
1. Log in to the AWS Management Console with an Admin account.
2. In the AWS console, navigate to **CloudFormation** > **Stacks** and choose **Create new stack** > **With new resources**.

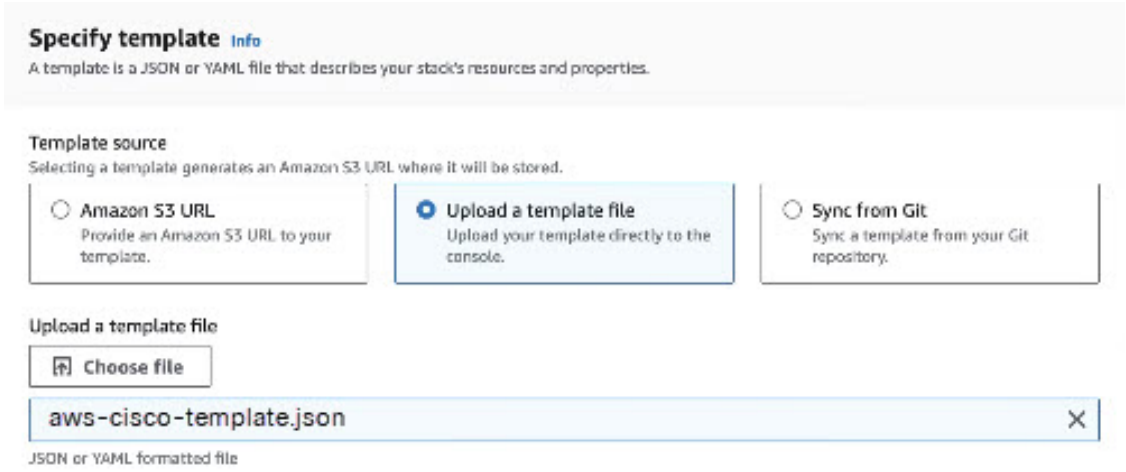


3. On the **Create stack** page, under **Specify Template**, select **Choose an existing template**.

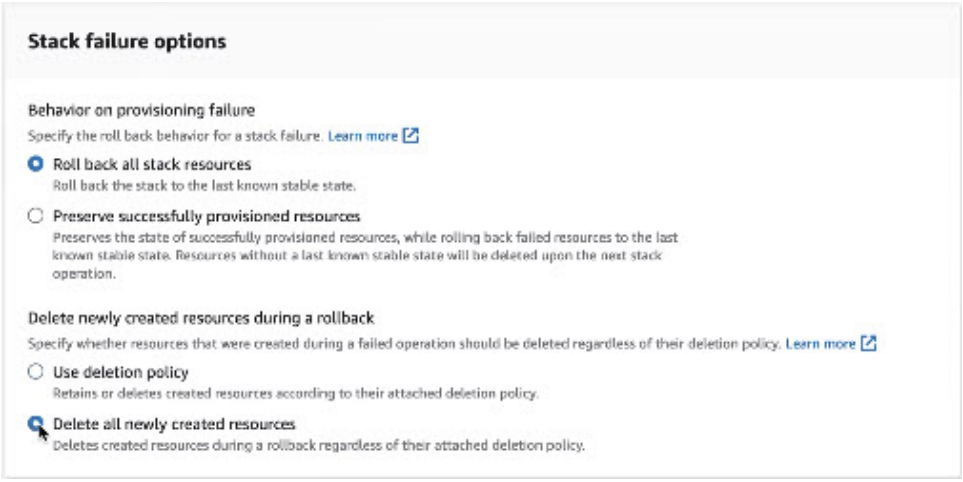


4. On the **Create stack** page, under **Specify template**, select **Upload a template file**, and navigate to a select the JSON file on your local system which you downloaded when you authorized the AWS tenant in Umbrella. (**primary-cloudformation-template.json** for your main region, or **regional-cloudformation-template.json** for any additional regions.)

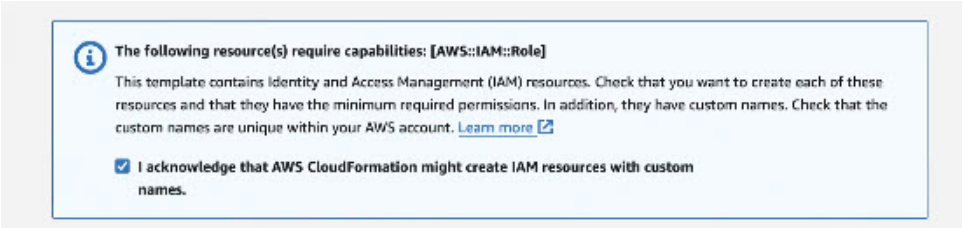




5. (Optional) Click **View in Application Composer** to open a new tab displaying a graphical representation of the stack deployment.
6. Click **Next**.
7. For the remaining options in the stack creation wizard, choose the settings appropriate to your environment. We recommend the following best practices:
   - **Provide a stack name** that is meaningful within your environment.
   - Under **Stack failure options**, choose **Role back stack resources** and **Delete all newly created resources**.



8. Acknowledge that AWS CloudFormation may create IAM resources with custom names within your AWS account.



9. Click **Submit**.
10. In the AWS console the status of all stack in your account is displayed under **CloudFormation** > **Stacks**. Wait until the status for your new stack is displayed as **CREATE_COMPLETE**.

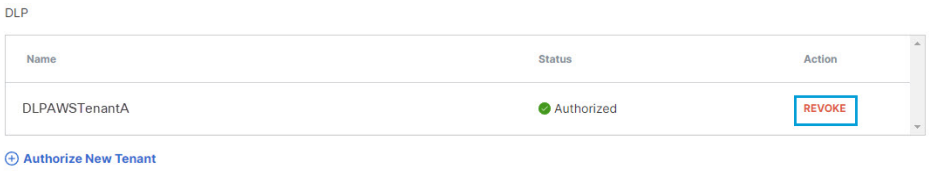
11. Continue with Step 5 of Authorize an AWS Tenant.

Revoke Authorization

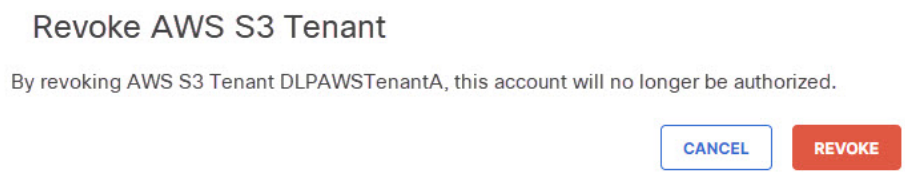
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **AWS S3**.
3. Under **Action** column,, click **Revoke**. You can revoke any authorized tenant.



4. Confirm to proceed. The selected account is no longer authorized.



Consider deleting the AWS stack you created if it is not needed for other purposes.

Enable SaaS API Data Loss Prevention for Azure Tenants

Describes Enable SaaS API Data Loss Prevention for Azure Tenants in Cisco Secure Access. You can apply DLP SaaS API rules to files in an Azure tenant.

You can apply DLP SaaS API rules to files in an Azure tenant. You must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- You must have an active Azure account and the person doing the installation must be an Azure Global Admin.
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Limitation

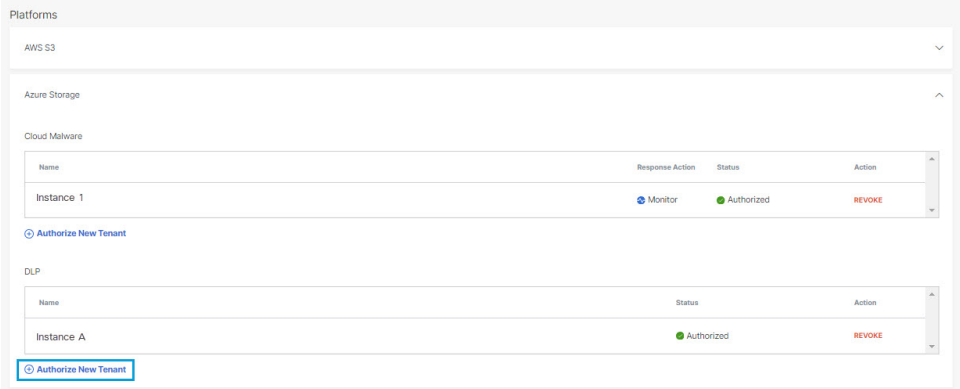
- A tenant that fails to authenticate cannot be deleted.

Authorize an Azure Tenant

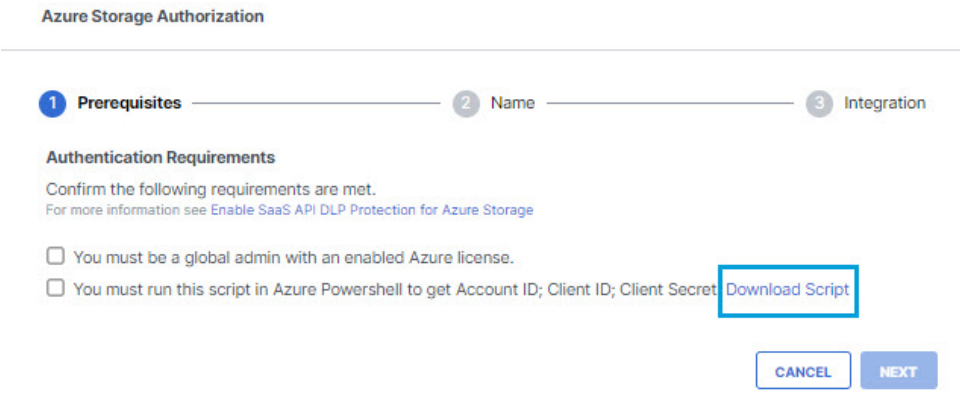
Provides instructions for completing the Authorize an Azure Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

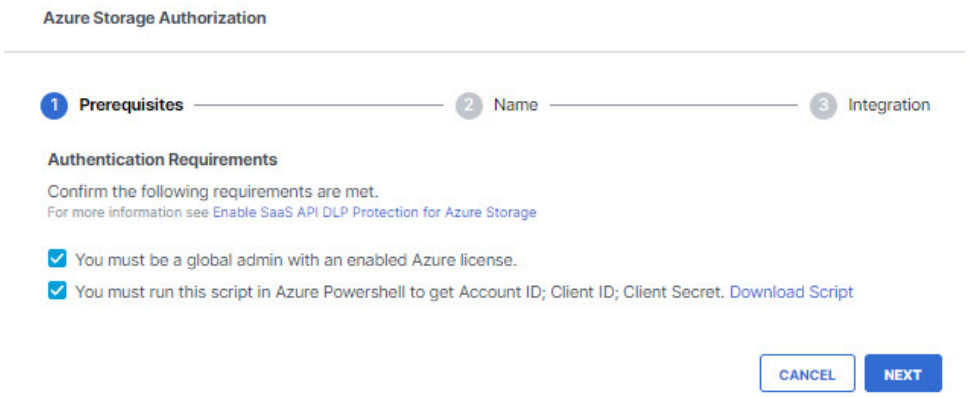
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click to expand **Azure Storage**.
3. In the **DLP** subsection, click **Authorize New Tenant** to add an Azure tenant to your Secure Access environment.



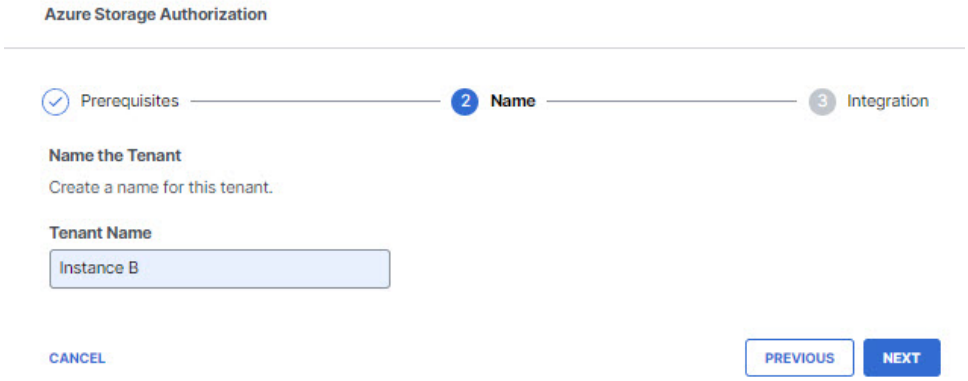
4. In the **Azure Storage Authorization** dialog, click **Download Script** to download the Azure PowerShell script **AzureOnboarding.ps1**. Save the script to your local machine, then run the script in the Azure PowerShell before proceeding to the next step. Be sure to note the information the script will provide: , **Client ID**, and **Client Secret**.



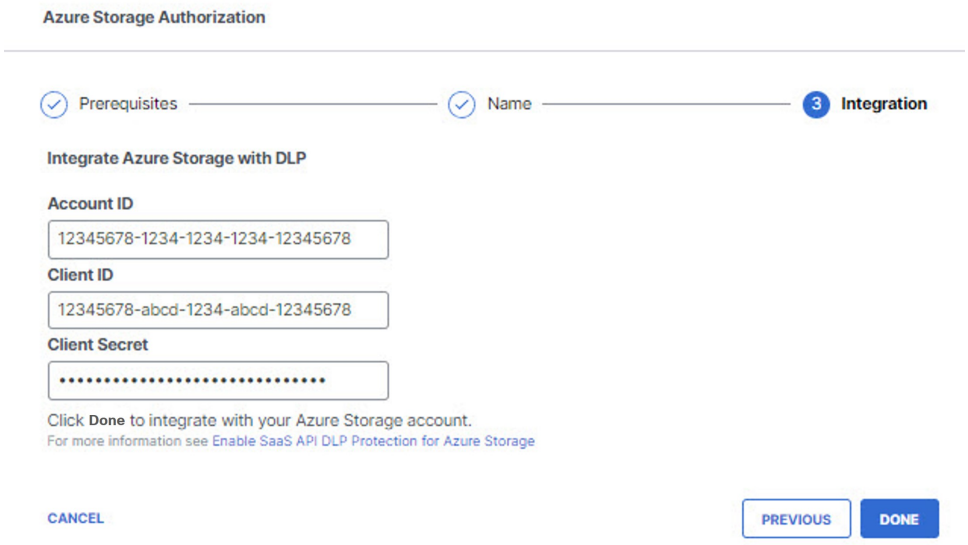
5. In the **Azure Storage Authorization** dialog, check the checkboxes to verify you have met the prerequisites, then click **Next**.



6. Enter a **Tenant Name** that is meaningful within your environment, then click **Next**.



7. Paste the **Account ID**, **Client ID**, and **Client Secret** (which you obtained when you ran the PowerShell script in the Azure portal) in the appropriate boxes and Click **Done**. (It may be up to 24 hours for the integration to be confirmed and appear as **Authorized** on the Authentication page)



Run an Azure PowerShell Script to Obtain Account Information

Provides instructions for completing the Run an Azure PowerShell Script to Obtain Account Information workflow in Cisco Secure Access. In the Azure portal, open a terminal window to the PowerShell.

Procedure

1. In the Azure portal, open a terminal window to the PowerShell.
2. Upload the script you downloaded in Step 4 of Authorize an Azure Tenant: In the Azure portal choose **Manage Files** > **Upload**, and choose the file.
3. Azure will display a message reporting **Successfully uploaded a file** and show the location and file name; note this information before dismissing the message.
4. In the terminal window, set your current directory to the location of the uploaded file.
5. To run the script, at the caret prompt (**>**) in the terminal window, enter **./AzureOnboarding.ps1**.
6. The script will prompt you to log into a web browser at https://microsoft.com/deviceLogin, and provide you with a code to authenticate. (If you get an error indicating you are already signed in, log out and log back in again.)
7. After initiating the login process, return to the terminal window.
8. The login process will present you with a numbered list of subscriptions available to you. (The subscription provides the environment where Azure will create resources needed to onboard Azure Storage for Secure Access DLP protection.) Enter the number corresponding to the subscription you want to work in, or press enter to use the default subscription, indicated with an asterisk.
9. The script will present a list of available subscriptions. Enter the name of the same subscription you chose during the login process in the previous step.
10. The script will present a list of Resource Groups available within the subscription you have chosen, and prompt you to enter the name of the Resource Group you want to use. This is where the resources needed for onboarding will reside.
11. For each Storage Account associated your subscription, the script will offer you the chance to add that Storage Account to the list of Storage Accounts with data to be scanned by Secure Access DLP. When presented with each Storage Account name, press Enter to add that account to the list, or Escape to skip that account. Azure will display messages confirming your choices. The script then proceeds to create the resources needed to support Secure Access DLP.
12. When the script has completed processing, it will display an **Account ID**, a **Client ID**, and **Client Secret**. Copy that information and return to Step 5 in Authorize an Azure Tenant .

Revoke Authorization

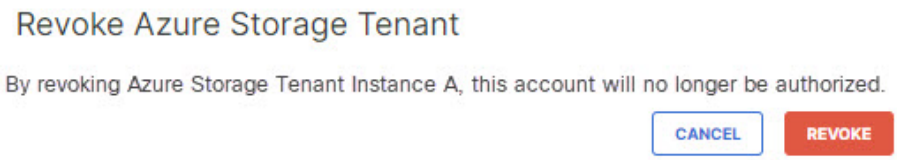
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Azure Storage**.
3. Under **Action** column,, click **Revoke**. You can revoke any authorized tenant.



4. Click **Revoke**. The selected account is no longer authorized.



Enable SaaS API Data Loss Prevention for Box Tenants

Describes Enable SaaS API Data Loss Prevention for Box Tenants in Cisco Secure Access. To apply DLP SaaS API rules to files in a Box tenant, you must authorize the tenant using the procedure described below.

To apply DLP SaaS API rules to files in a Box tenant, you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Limitation

Secure Access supports SaaS API Data Loss Prevention only for Box Enterprise accounts.

Prerequisites

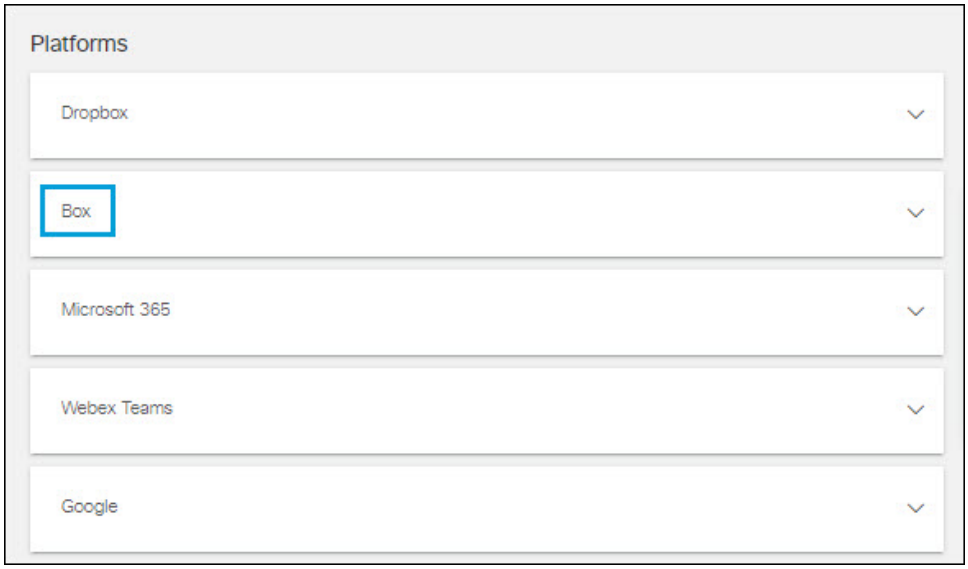
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).
- The user performing the installation *must* use a Box account with Box admin privileges. (Co-admin privileges are insufficient.)

Authorize a Tenant

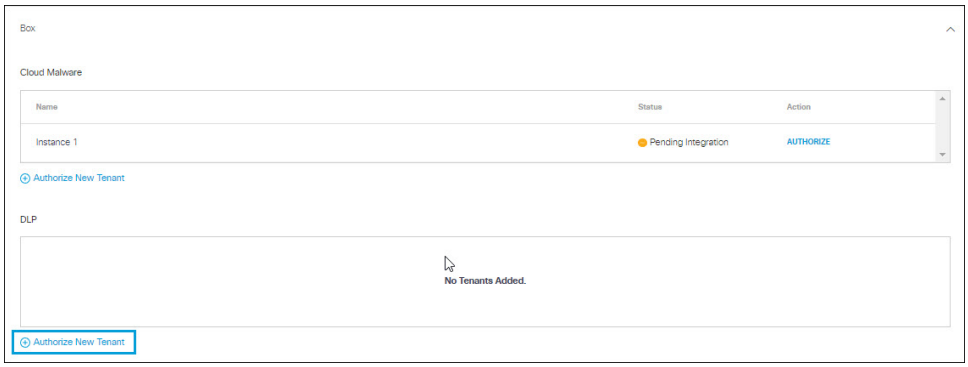
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

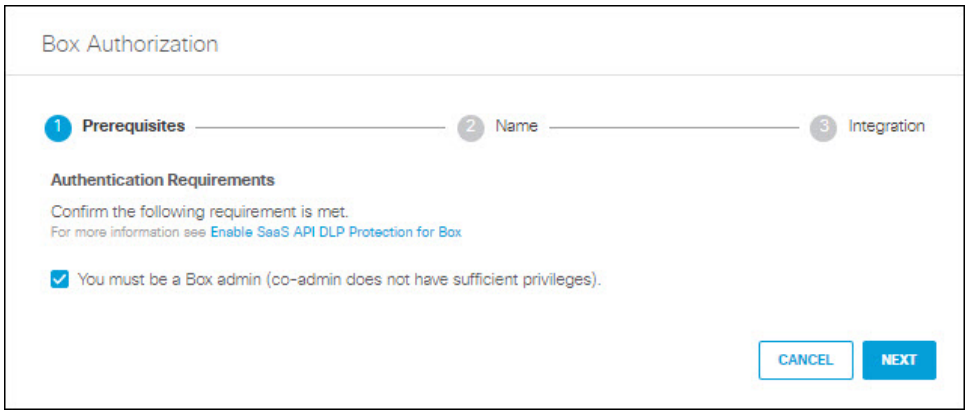
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Box**.



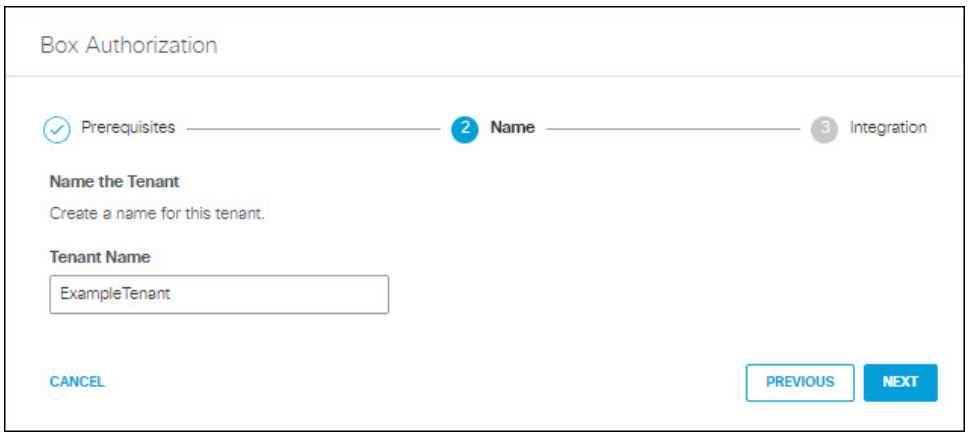
3. In the DLP subsection, click **Authorize New Tenant** to add a Box tenant to your Secure Access environment.



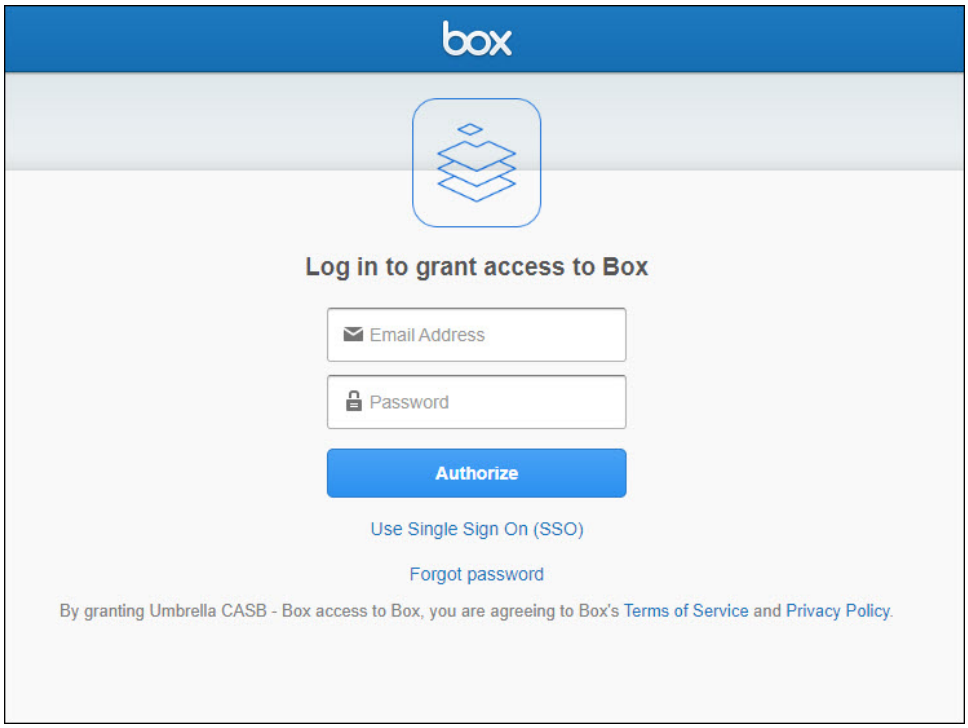
4. In the **Box Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



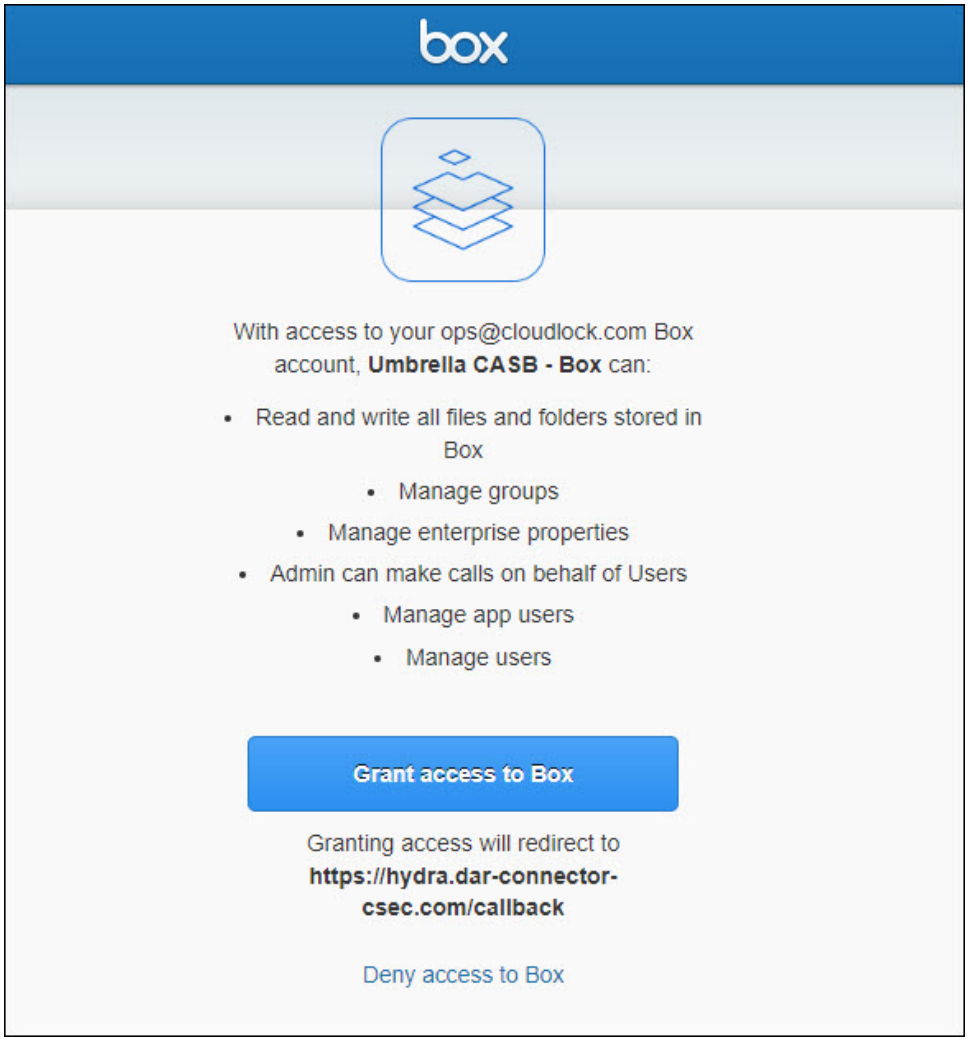
5. Enter the name of your tenant, then click **Next**.



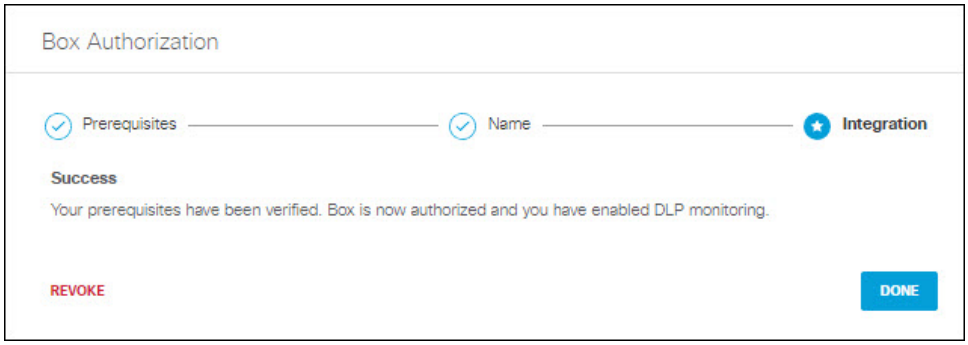
6. Click **Next** to be redirected to the Box login page.
7. Log in to Box with admin privileges to grant access.



8. Click **Grant access to Box** to complete the authorization.



9. You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

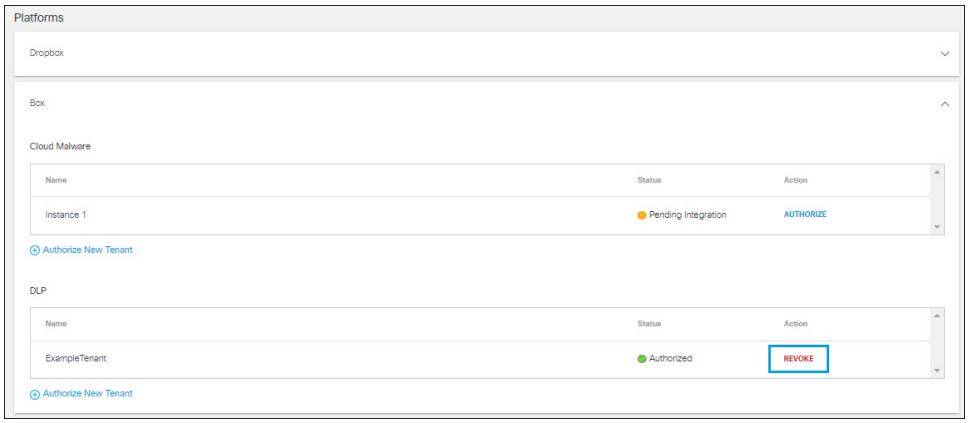


Revoke Authorization

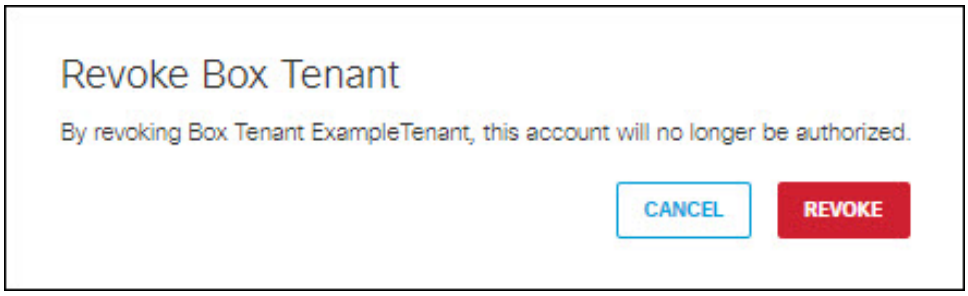
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Prevention for Confluence Tenants

Provides instructions for completing the Enable SaaS API Data Loss Prevention for Confluence Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports SaaS API DLP protection in Confluence Enterprise sites for page content, comments, and file attachments. Secure access does not provide SaaS API DLP protection for Confluence whiteboards or database tables. A tenant can access only a single Confluence site; to apply SaaS API DLP protection to multiple Confluence sites, you must establish a separate tenant for each.

To use this feature you must authorize the tenant using the procedure described below. Once the tenant is authorized, for pages, comments, and attachments residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

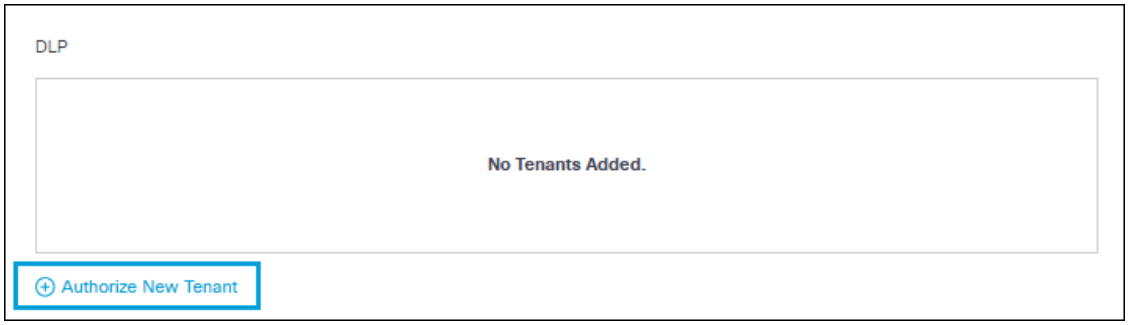
Before you begin

- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Confluence account.

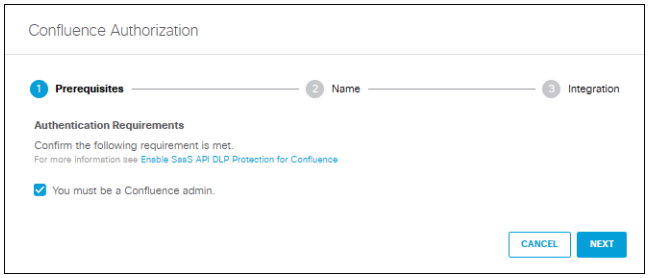
Procedure

1. Navigate to **Admin > Authentication**.
2. Under **SaaS API Platforms**, click to expand **Confluence**.

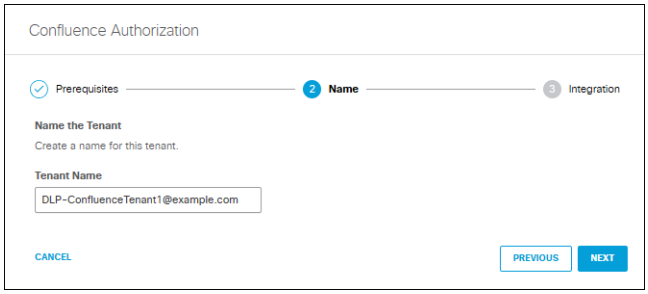
3. In the **DLP** subsection, click **Authorize New Tenant** to add a Confluence tenant to your Secure Access environment.



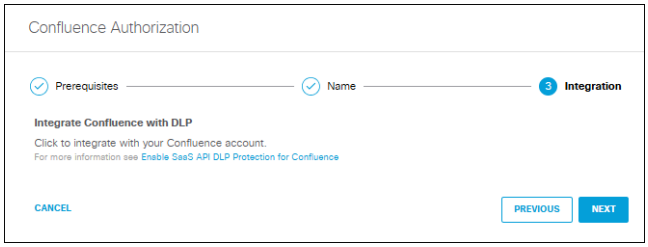
4. In the **Confluence Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



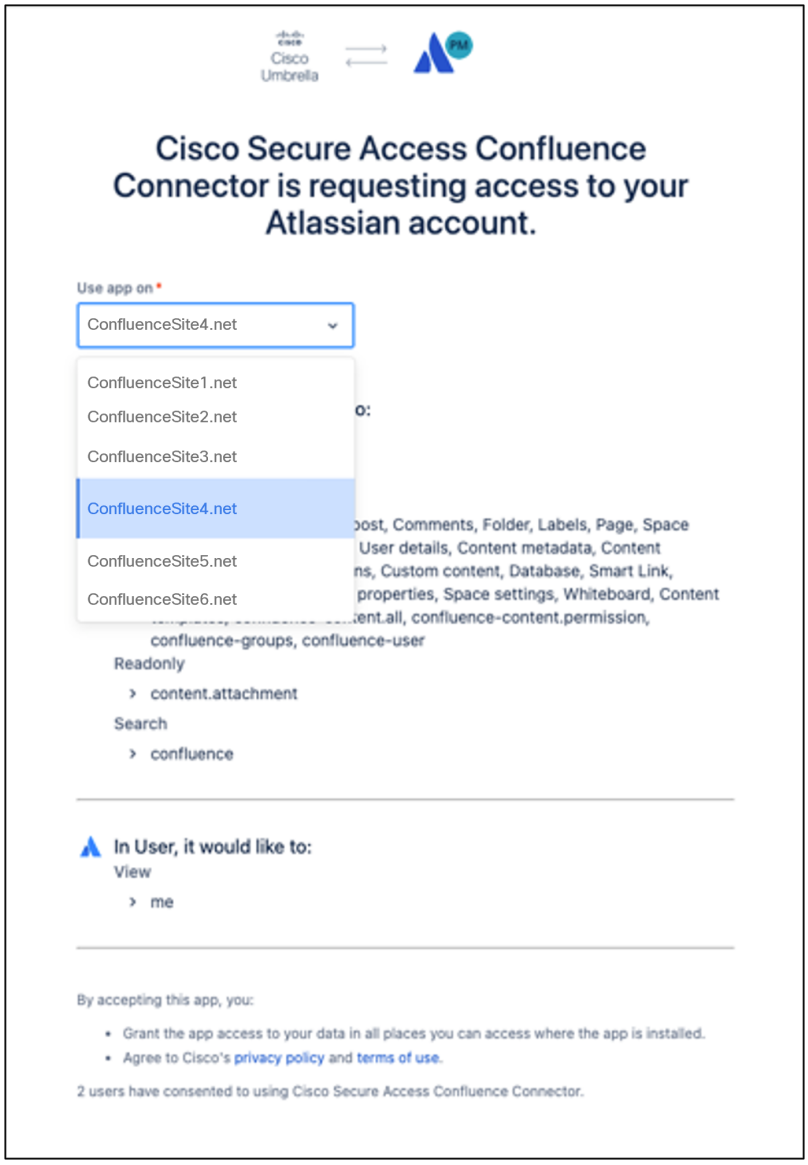
5. Enter the name of your tenant, then click **Next**.



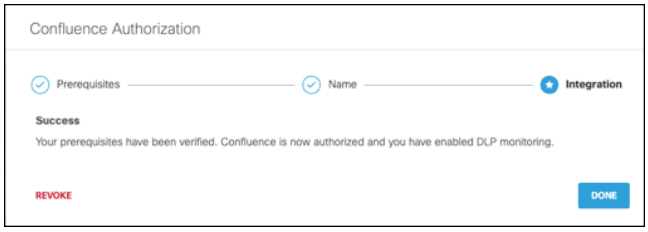
6. Click **Next** to be redirected to the Atlassian login page.



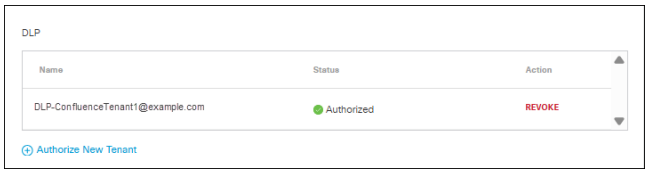
7. Log in with Confluence admin credentials. The Confluence Access Authorization page will appear.
8. Select a Confluence site for the new tenant to access from the **Use app on** drop-down. (Each tenant can access only one Confluence site.) Click **Accept**.



9. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.



10. The new tenant will appear on the Authorization page in the list under **Confluence**.



Enable SaaS API Data Loss Prevention for Dropbox Tenants

Describes Enable SaaS API Data Loss Prevention for Dropbox Tenants in Cisco Secure Access and explains Prerequisites and Limitation. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Secure Access DLP Connector must be installed in the tenant by a Dropbox Admin User.
- It is recommended to use a service account for the installation.

Limitation

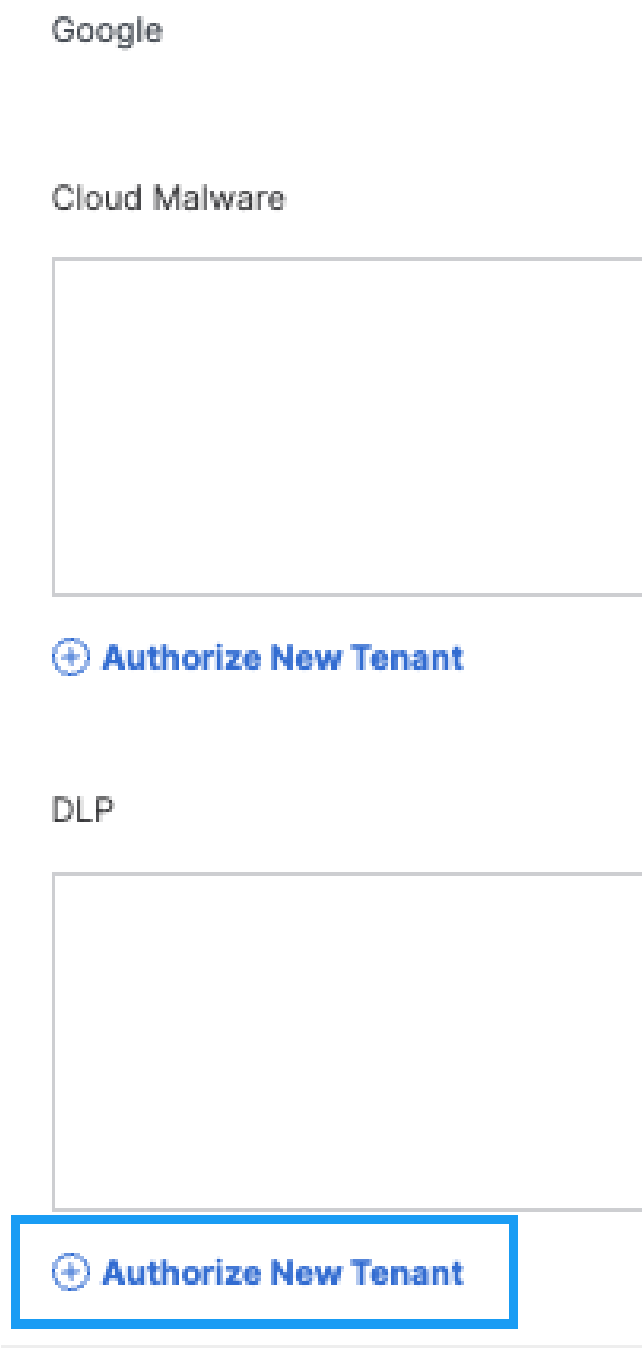
- Secure Access supports SaaS API Data Loss Prevention only for Dropbox Enterprise accounts.

Authorize a Tenant

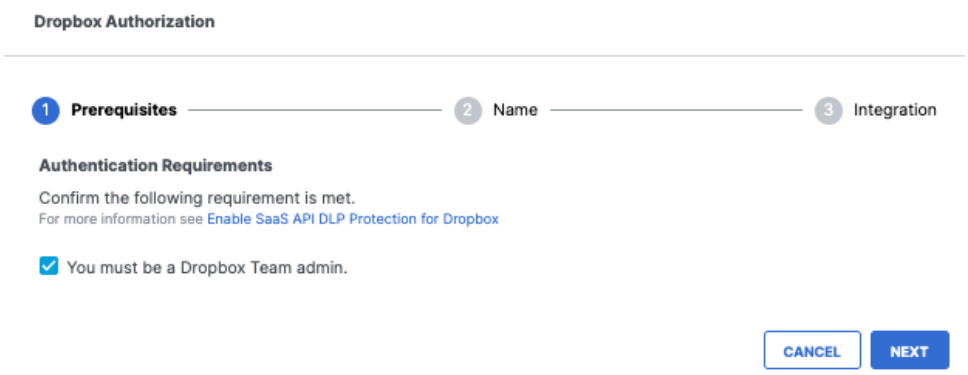
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

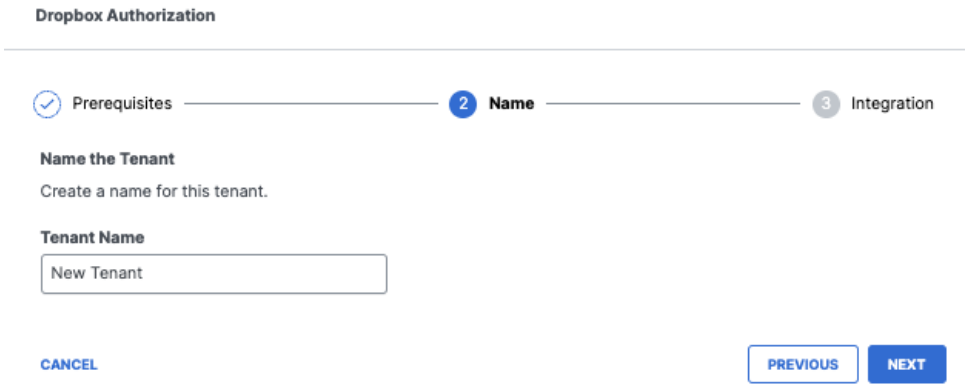
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Dropbox**.
3. Under **DLP**, click **Authorize New Tenant** to add a Dropbox tenant to your Secure Access environment.



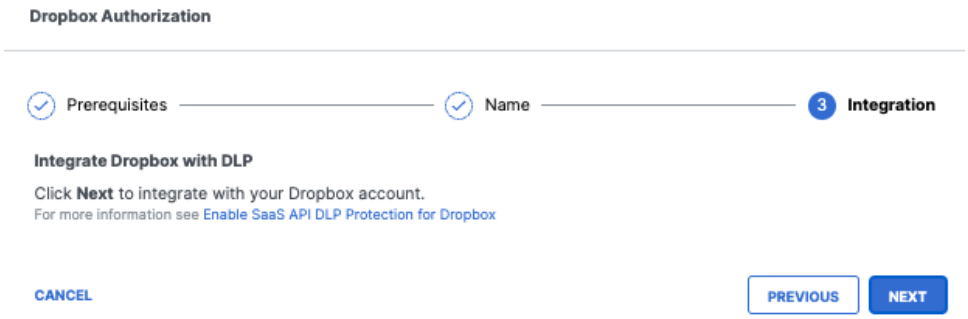
4. In the **Dropbox Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



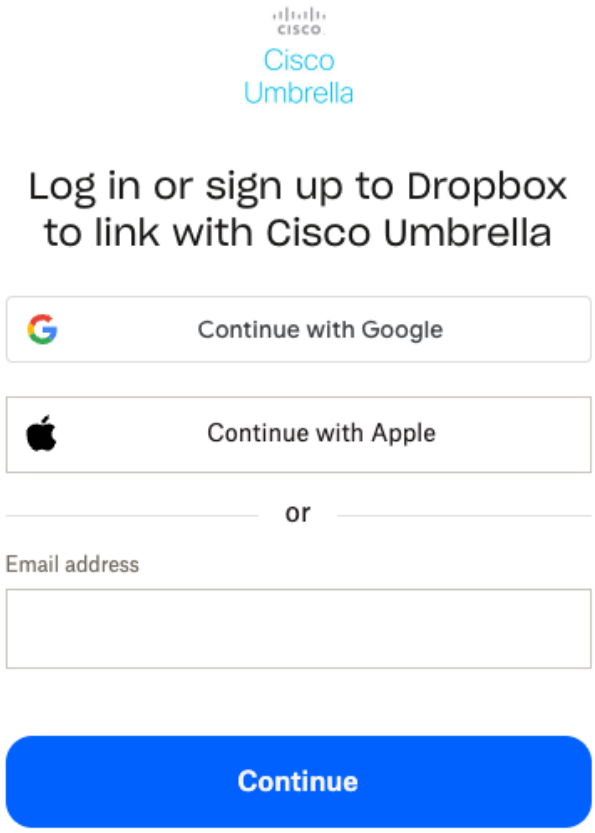
5. Enter the tenant name, then click **Next**.



6. Click **Next** to be redirected to the Dropbox login page.



7. Log in to Dropbox with Dropbox Team admin credentials to grant access.



8. You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may take up to eight hours for the integration to be confirmed and appear as **Authorized**.
9. Click **Done** to complete.

Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Prevention for GitHub Tenants

Explains how SaaS API Data Loss Prevention (DLP) policies are applied to GitHub tenants to identify and protect sensitive data by scanning various content types.

Secure Access identifies sensitive data through Data Loss Prevention (DLP) scanning for GitHub.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).
- Secure Access for GitHub connector must be installed in the tenant by a GitHub Admin User.

Supported content types

The following table outlines the content types supported for scanning and the specific scan types available.

Table 23: Security scan support for GitHub content

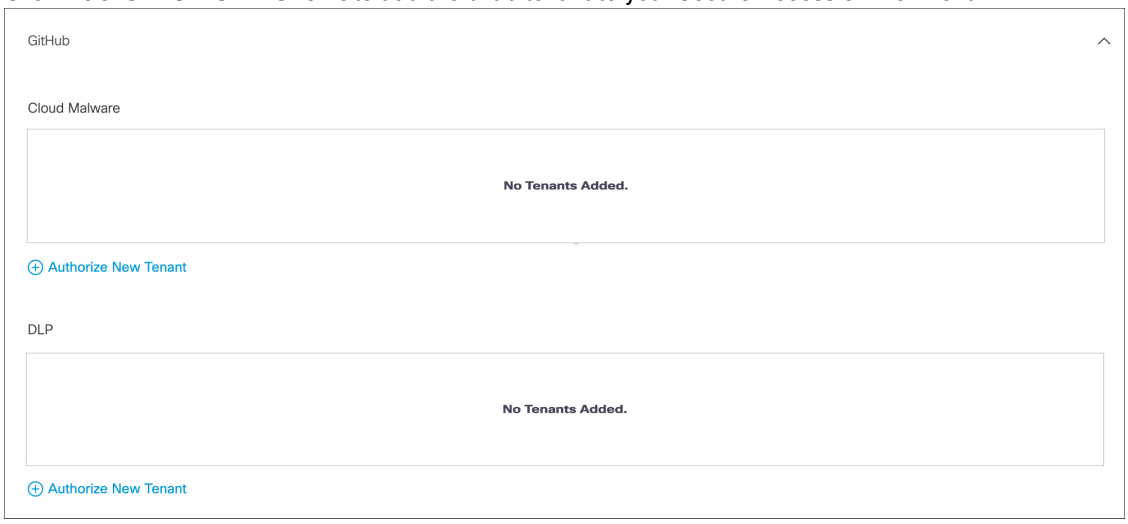
Content Type	DLP Scan
Repository files	Yes
Commit messages	Yes
Pull request (PR) descriptions	Yes
PR changed files	Yes
PR reviews	Yes
PR review comments	Yes
Issues (body)	Yes
Issue comments	Yes
Commit comments	Yes
Release notes (body)	Yes
Release binary assets	No
Embedded image attachments	Yes*
Embedded file attachments	No

*** Image attachment expiration**: Embedded images use time-limited links that expire approximately 5 minutes after generation. After the 5-minute duration, the image will not be scanned.

Authorize a Tenant

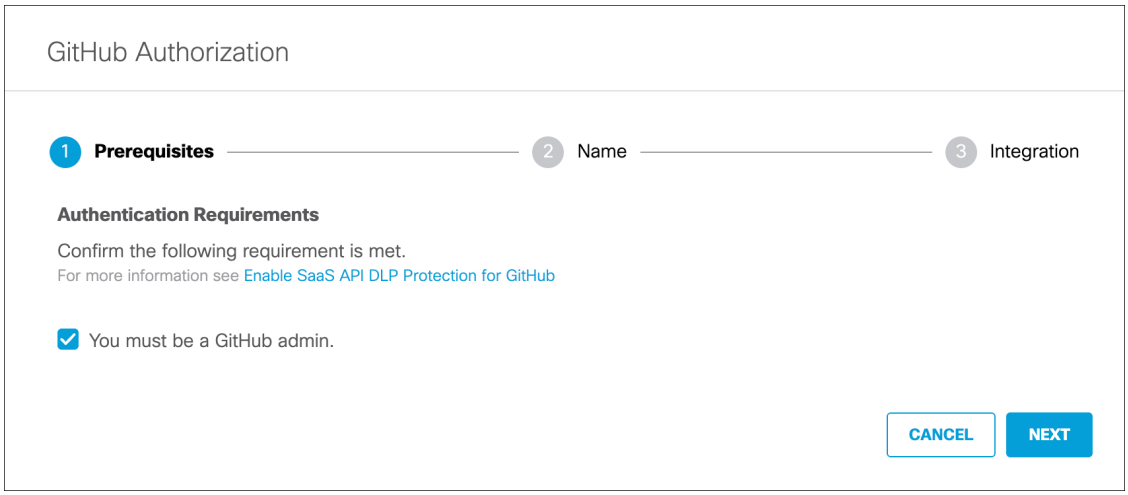
Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click **GitHub**.
3. Click **Authorize New Tenant** to add a GitHub tenant to your Secure Access environment.

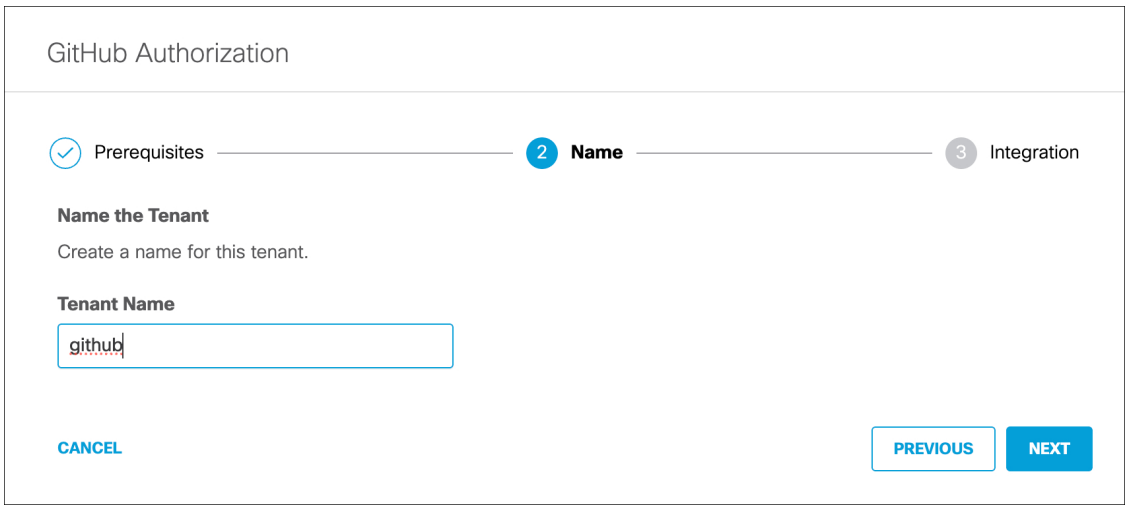


4. In the **GitHub Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

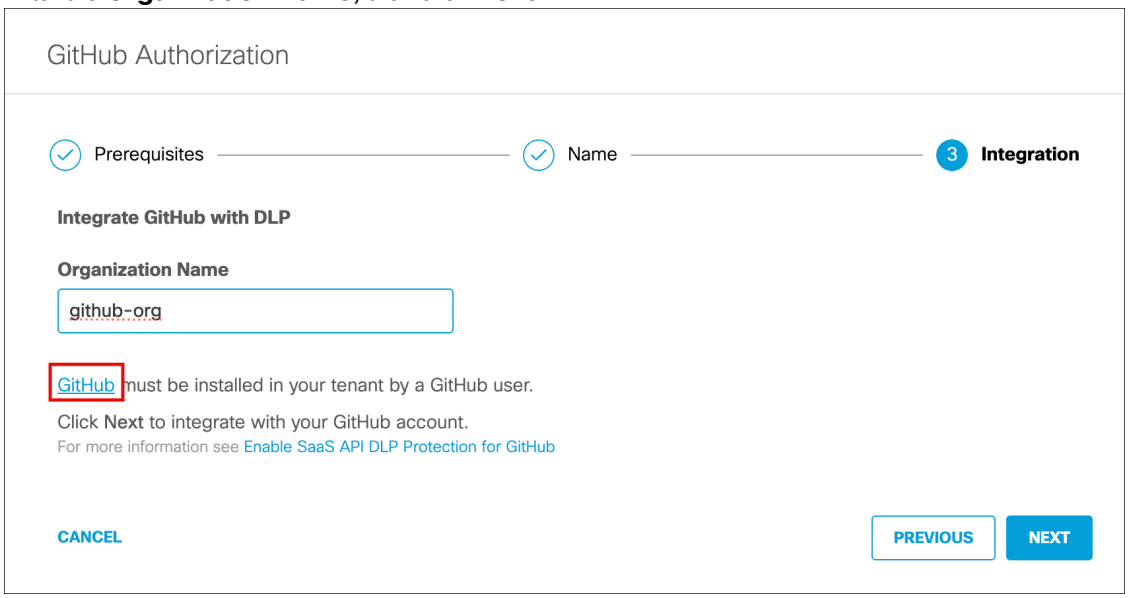
> **Note**
>
> The link to the SaaS API Connector brings you to the Cisco Secure Access for GitHub connector site in the GitHub. This is correct, despite the nomenclature difference.



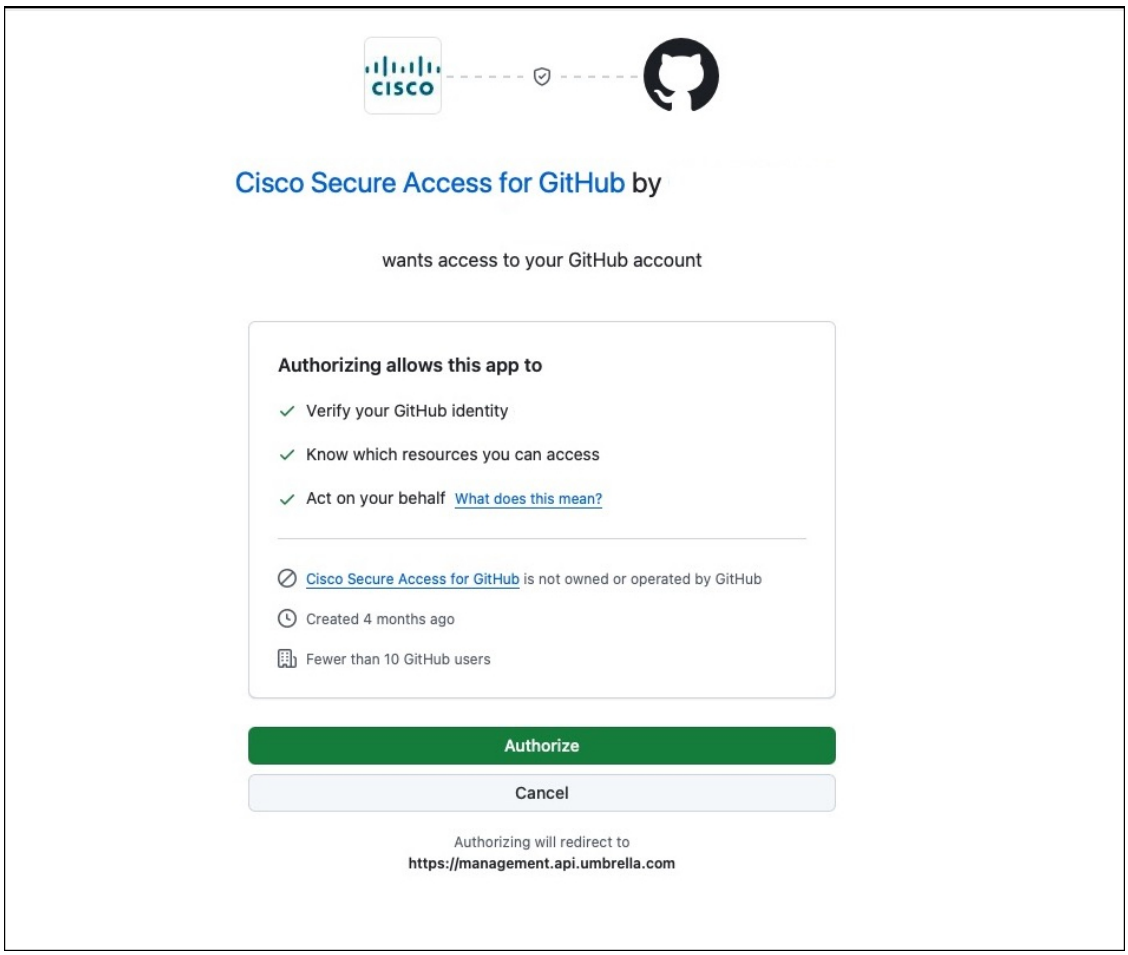
5. Enter the tenant name, then click **Next**.



6. Enter the **Organization Name**, then click **Next**.



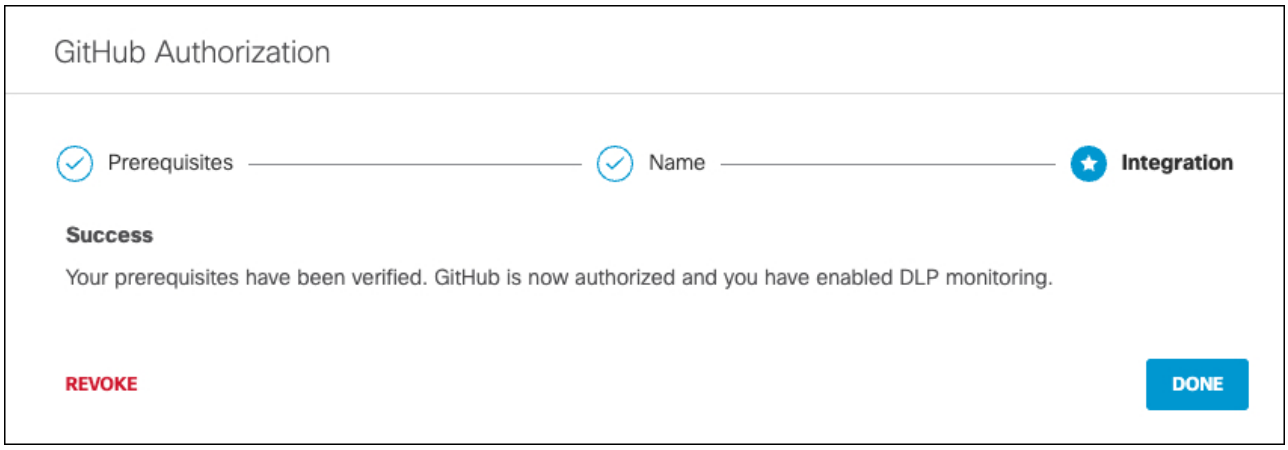
7. (Optional) If you have not installed the GitHub connector in GitHub, click **GitHub**.
   For steps to install the GitHub connector, see Install the GitHub connector.
8. Review the permissions requested by the Cisco Secure Access for GitHub application in the GitHub authorization page.



9. Click Authorize to grant the application access to your GitHub account.

   You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 8 hours for the integration to be confirmed and appear as **Authorized**.

10. Click **Done** to complete.



Install the GitHub connector

Deploy the GitHub connector to integrate your GitHub organization with Cisco Secure Access for automated security monitoring.

Installing the connector establishes a secure link that allows Cisco Secure Access to scan your repositories for sensitive data and malicious files.

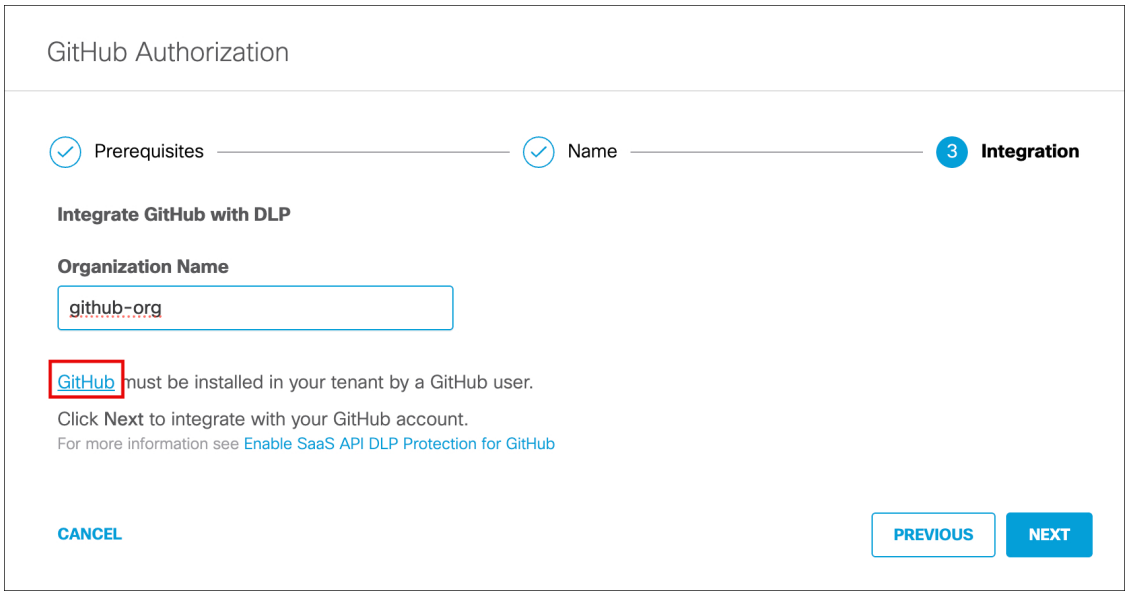
Follow these steps to install the GitHub connector:

Before you begin

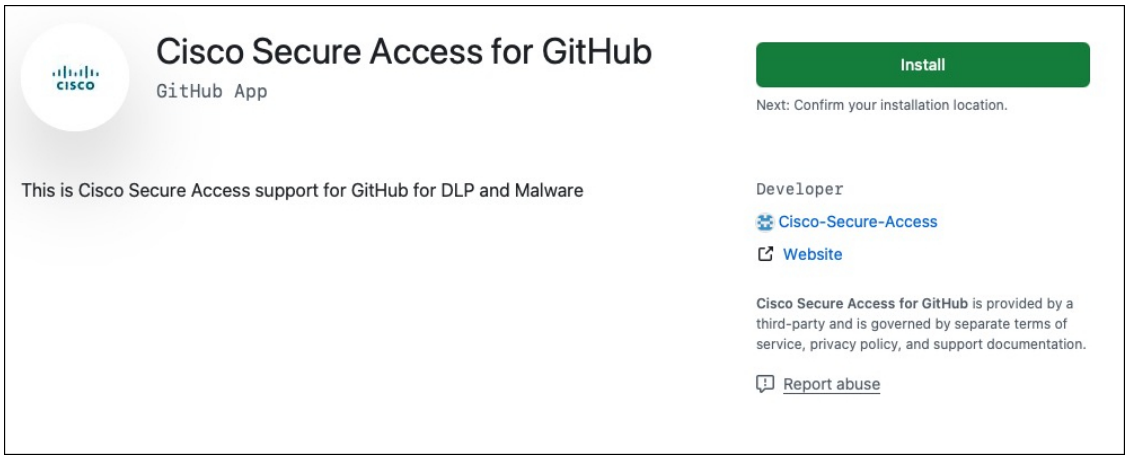
- Ensure you have administrative access to your GitHub organization.
- Verify that you have the required administrative permissions in the Cisco Secure Access console.

Procedure

1. Click **GitHub** in the Integrate GitHub with DLP workflow.



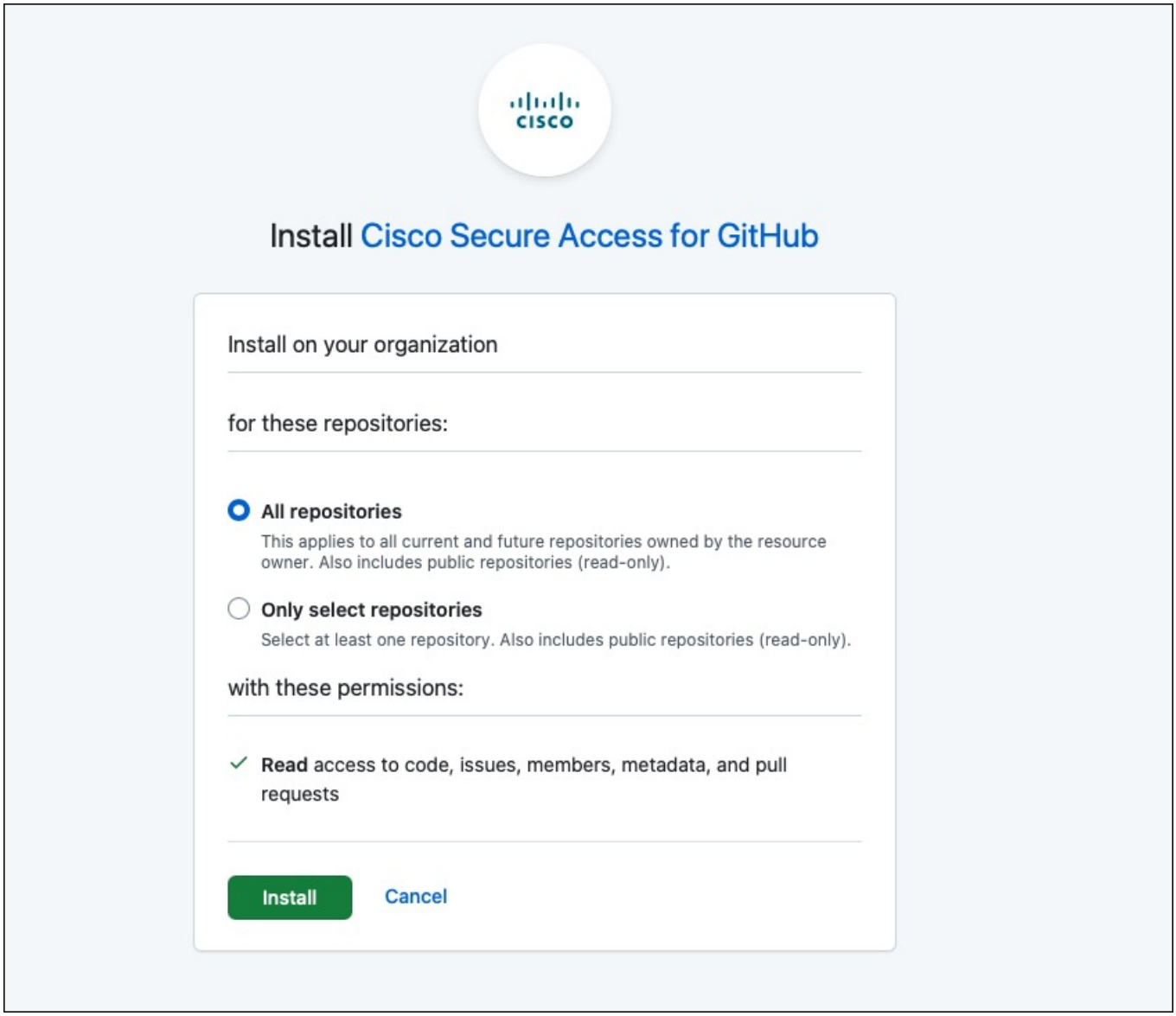
2. Click **Install**.



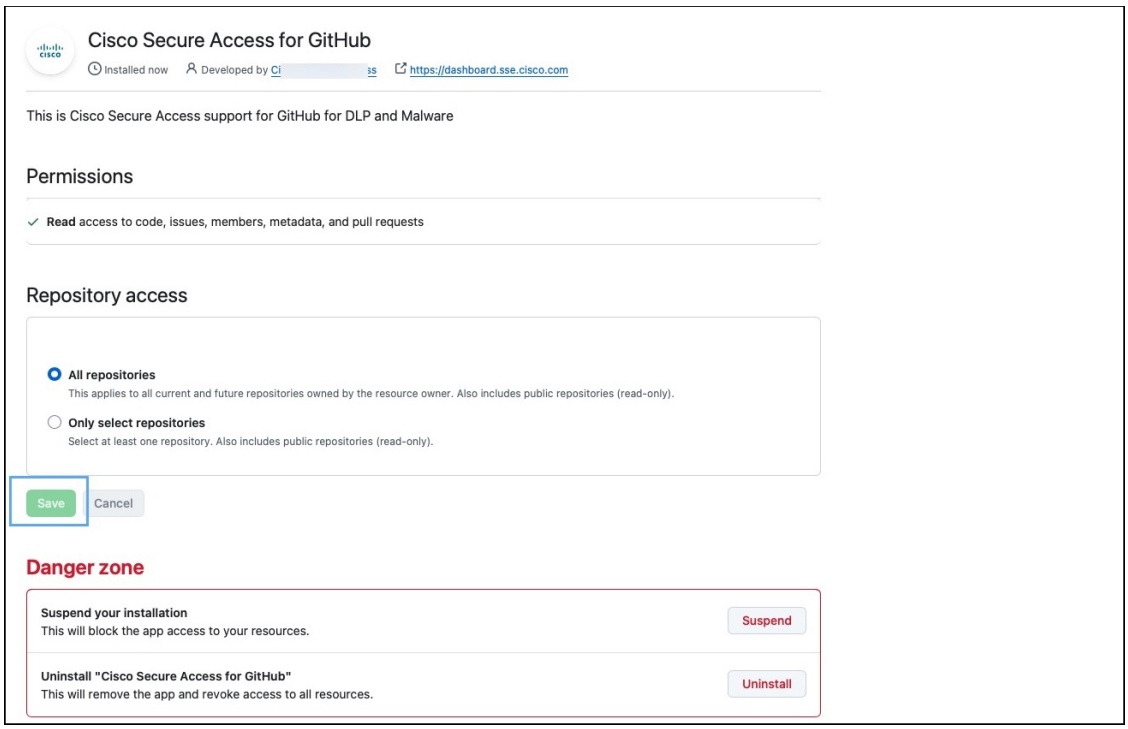
3. Select the GitHub organization.



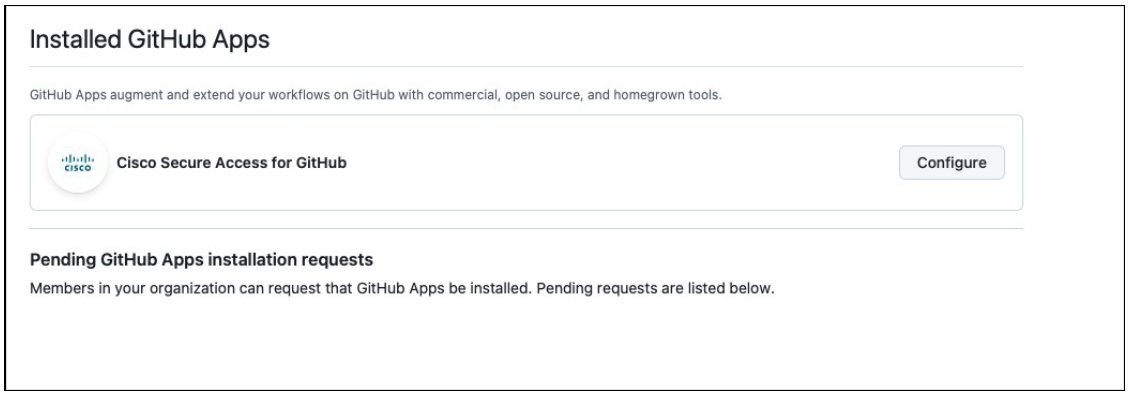
4. Click **Install**.



5. Verify the application permission and click **Save**.



6. Go to **Third-party Access** in GitHub to verify the installation.



The GitHub connector is successfully installed, authorized, and actively monitoring your repositories for security policy violations.

Verify Cisco Secure Access for GitHub app integration

Verify Cisco Secure Access for GitHub app integration.

Ensure that your GitHub account or group is properly integrated with Cisco Secure Access for enhanced security and management.

Procedure

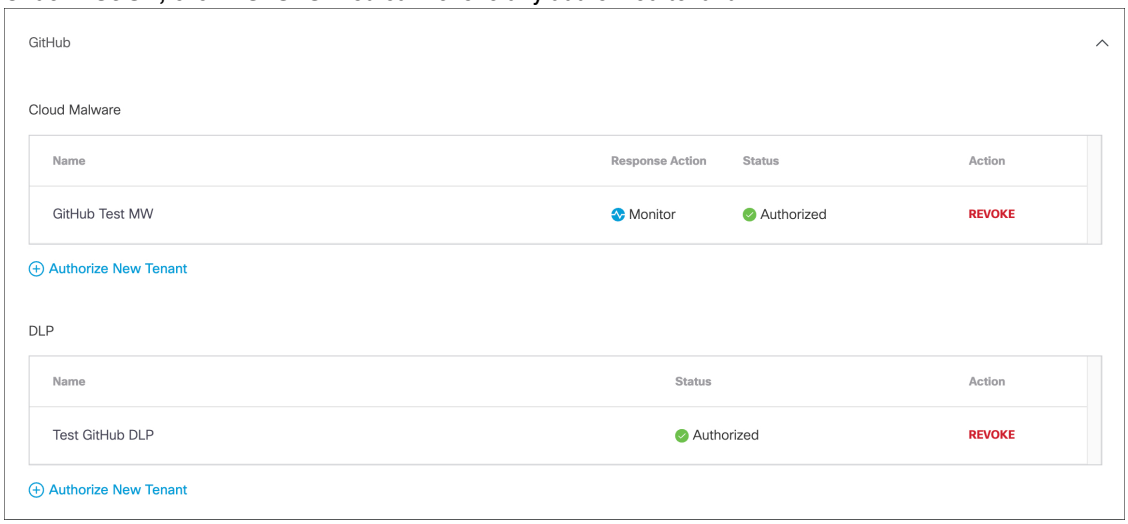
1. Log in to https://github.com with admin credentials.
2. Navigate to **Settings** > **Third-party Access** > **GitHub Apps**.
3. Ensure that the **Cisco Secure Access for Github** application is present and enabled for your admin or for the group you are a part of.

The Cisco Secure Access for GitHub app is confirmed to be present and active for your account or group.

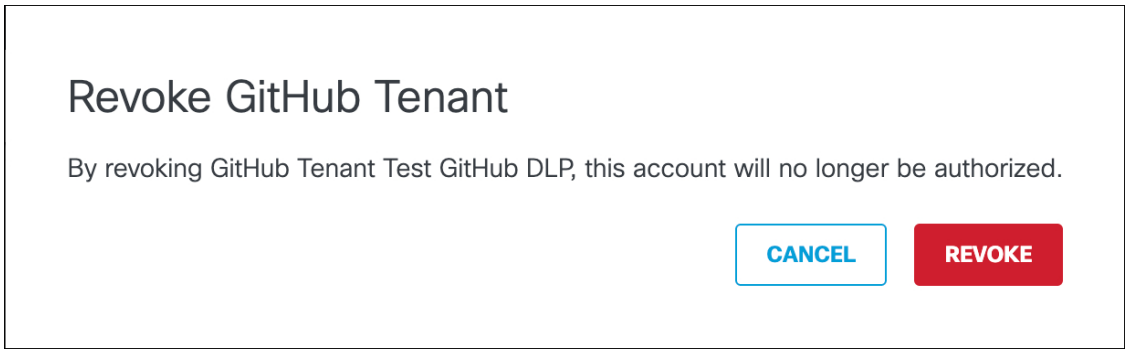
Revoke Authorization

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Prevention for Google Drive Tenants

Describes Enable SaaS API Data Loss Prevention for Google Drive Tenants in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Secure Access DLP Connector must be installed in the tenant by a Google Admin User.
- It is recommended to use a service account for the installation.

Validation

Provides instructions for completing the Validation workflow in Cisco Secure Access. Log in to https://admin.google.com with admin credentials.

Procedure

1. Log in to https://admin.google.com with admin credentials.
2. Navigate to **Apps** > **Google Workspace Marketplace Apps** > **App List**.
3. Ensure that the **Secure Access DLP Connector** application is present and enabled for your admin or for the group you are a part of.
4. Navigate to **Apps** > **Google Workspace** > **Drive And Docs** and ensure that the drive service is enabled for your admin or for a group you are part of.

What to do next

The Secure Access DLP Connector needs access to your Google account. This allows Secure Access DLP Connector to:

View, Edit, Create, and Delete all of your Google Drive files

View domains related to your customers

View groups on your domain

View organization units on your domain

View and manage the provisioning of users on your domain

View Information about users on your domain

View audit reports for your G suite domain

View usage reports for your G suite domain

View, Edit, Configure, and Delete your Google Cloud data and view the email address for your Google Account

View your primary Google Account email address

View your personal information that is made publicly available

Manage your sites

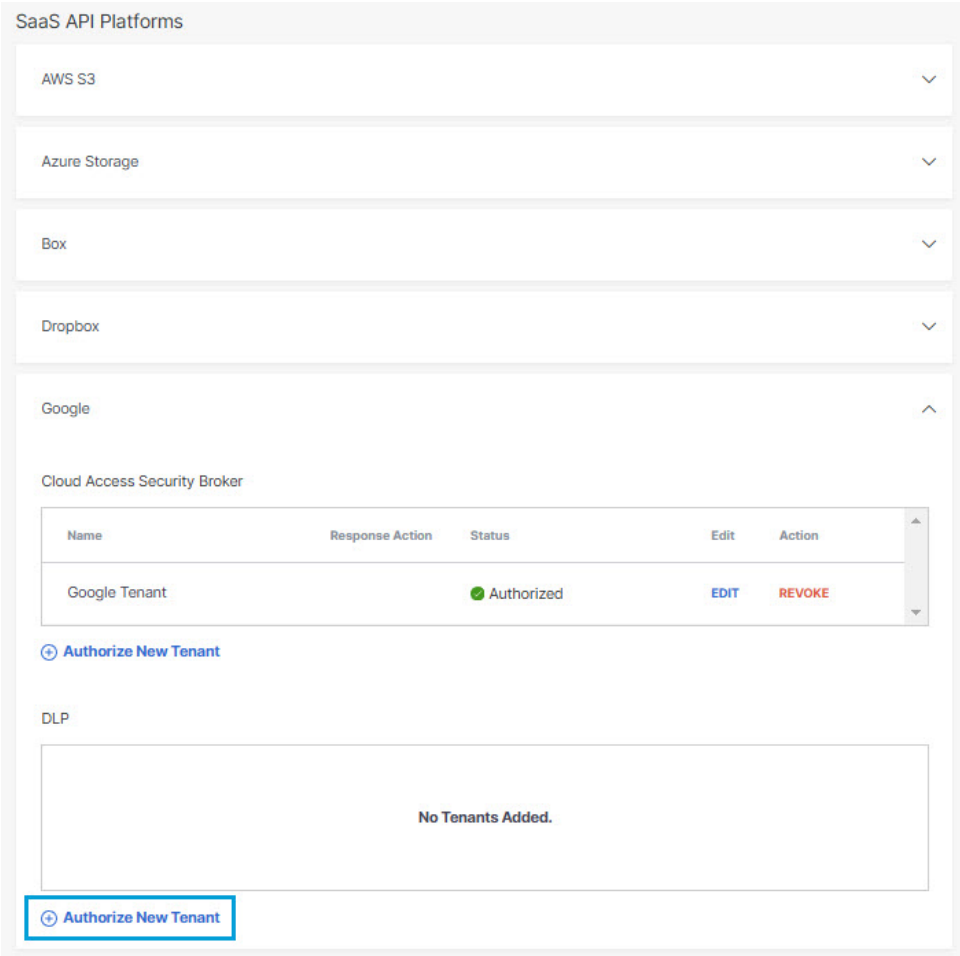
View the activity history of your Google apps

Authorize a Tenant

Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

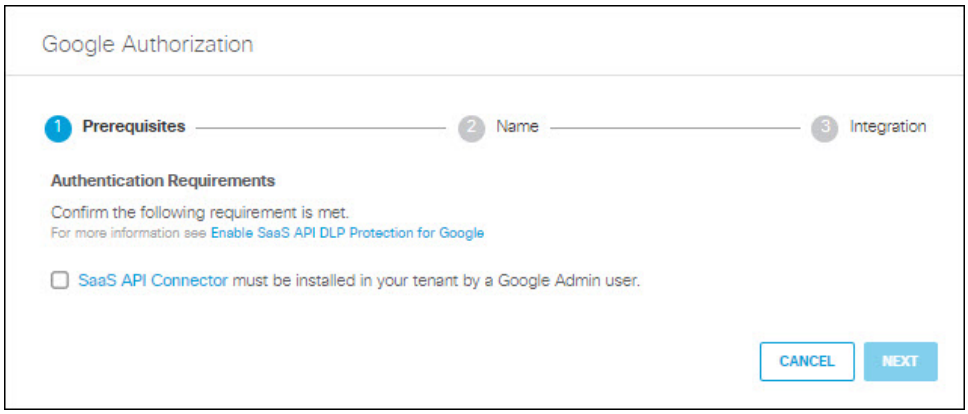
Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click **Google**.
3. Click **Authorize New Tenant** to add a Google Drive tenant to your Secure Access environment.

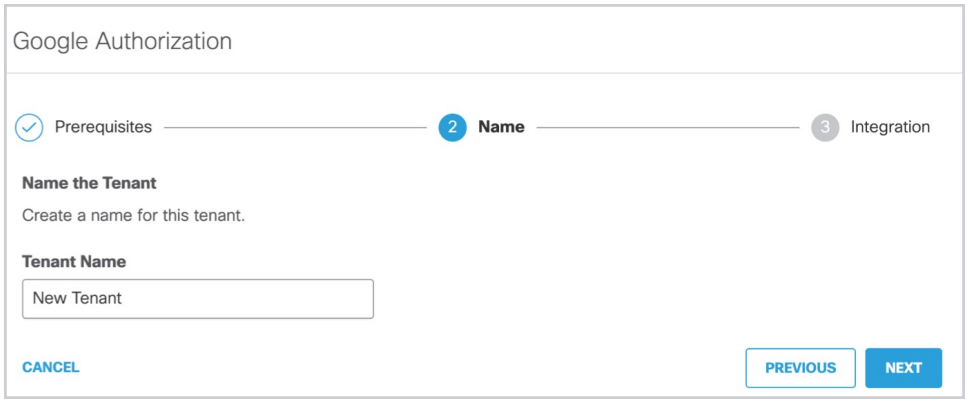


4. In the **Google Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

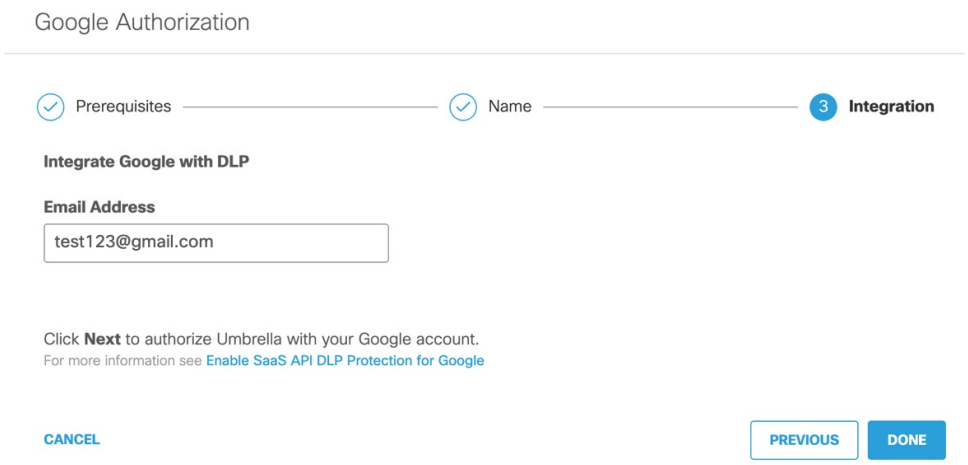
> **Note**
>
> The link to the SaaS API Connector brings you to the Umbrella DLP Connector site in the Google Workspace Marketplace. This is correct, despite the nomenclature difference.



5. Enter the tenant name, then click **Next**.



6. Enter the **Email Address**, then click **Next**.



You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 8 hours for the integration to be confirmed and appear as **Authorized**.

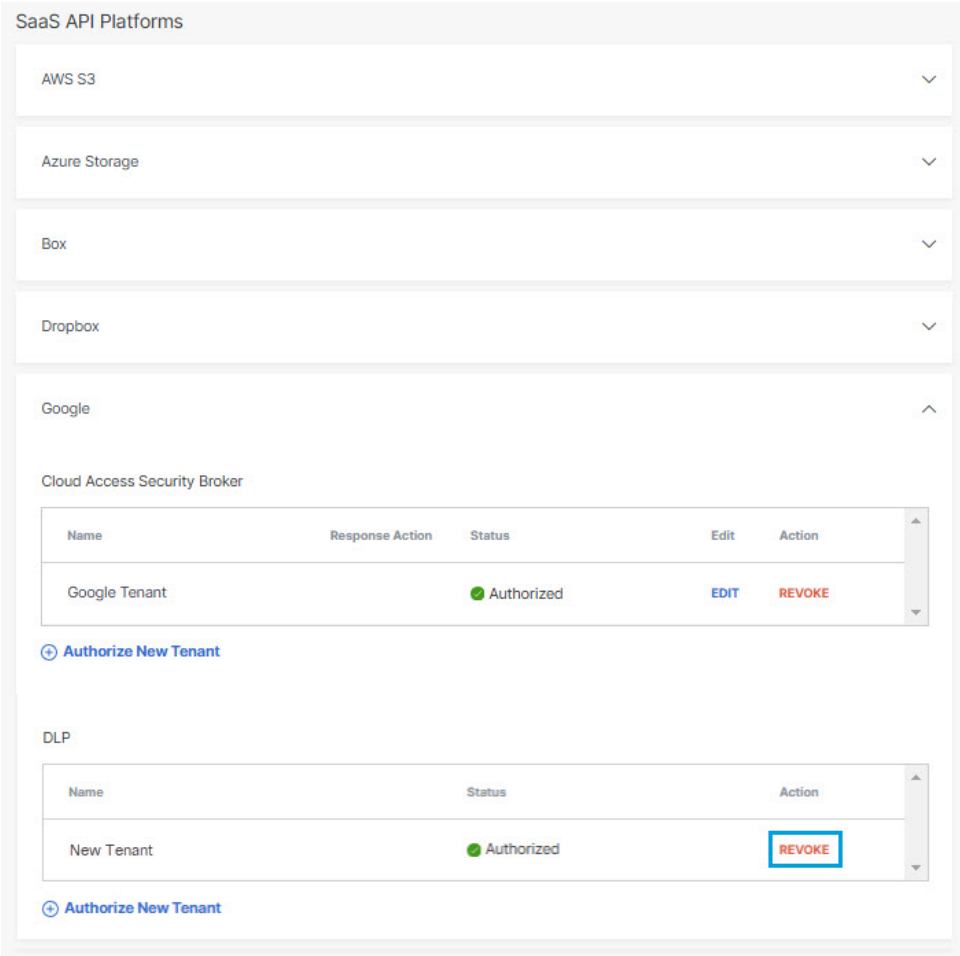
7. Click **Done** to complete.

Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.

Enable SaaS API Data Loss Prevention for Jira Tenants

Provides instructions for completing the Enable SaaS API Data Loss Prevention for Jira Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports SaaS API DLP protection in Jira sites for page content, comments, and file attachments. A tenant can access only a single Jira site; to apply SaaS API DLP protection to multiple Jira sites, you must establish a separate tenant for each.

To use this feature you must authorize the tenant using the procedure described below. Once the tenant is authorized, for pages, comments, and attachments residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Before you begin

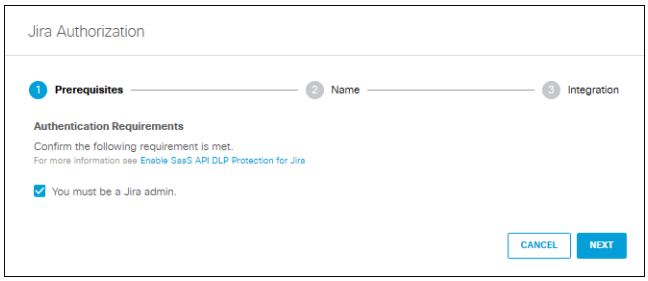
- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Jira account.

Procedure

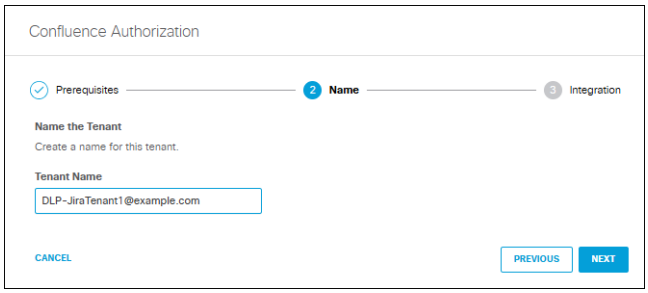
1. Navigate to **Admin > Authentication**.
2. Under **SaaS API Platforms**, click to expand **Jira**.
3. In the **DLP** section, click **Authorize New Tenant** to add a Jira tenant to your Secure Access environment.



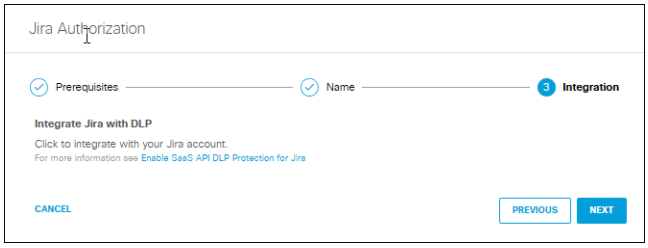
4. In the **Jira Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



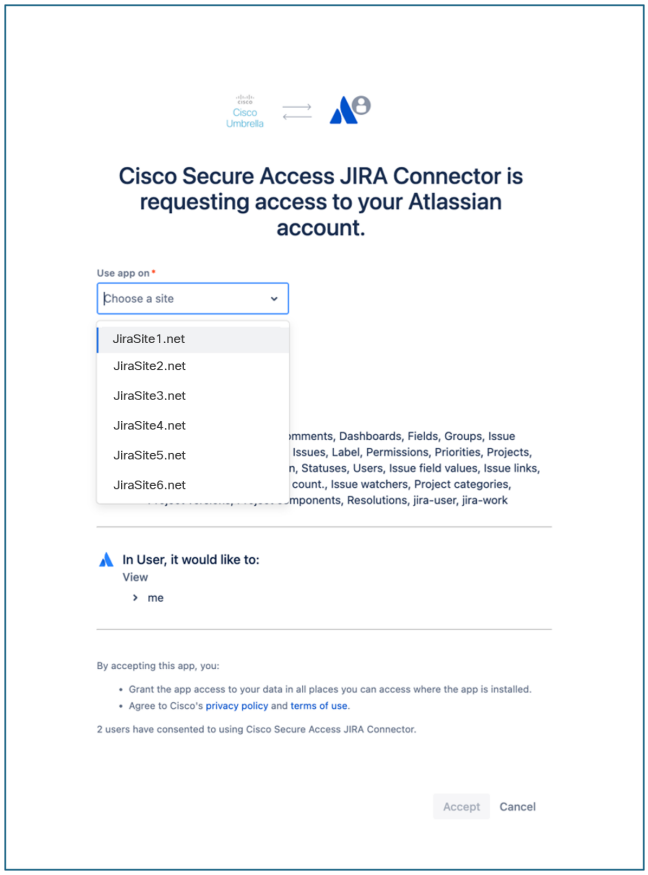
5. Enter the name of your tenant, then click **Next**.



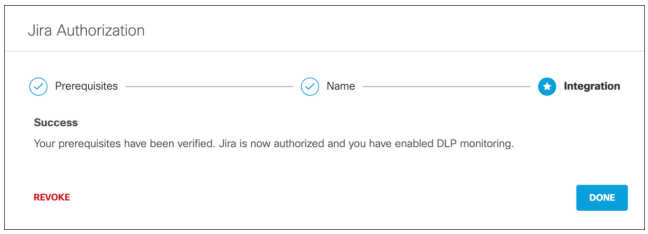
6. Click **Next** to be redirected to the Atalassian login page.



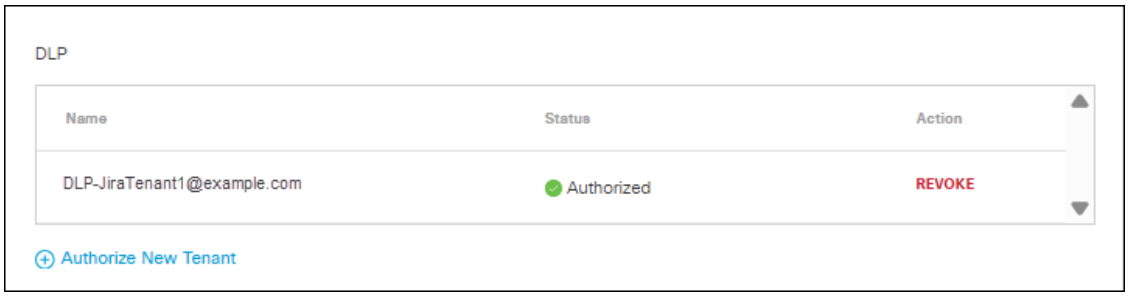
7. Log in with Jira admin credentials. The Jira Access Authorization page will appear.
8. Select a Jira site for the new tenant to access from the **Use app on** drop-down. (Each tenant can access only one Jira site.) Click **Accept**.



9. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.



10. The new tenant will appear on the Authorization page in the list under **Jira**.



Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants

Describes Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can enable SaaS API Data Loss prevention for authorized tenants that use the following Microsoft 365 applications:

- Sharepoint Online
- OneDrive
- Outlook (For outgoing mail only. For incoming mail you can enable Cloud Access Security Broker Protection; see Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants.)

> **Note**
>
> You cannot add an application to an existing tenant. If you have an existing Microsoft 365 tenant that uses one or two of these applications and you wish to add another application to that tenant, you must first revoke authorization for the existing tenant, then create a new tenant using all the desired applications.

Prerequisites for Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants

Describes Prerequisites for Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- The user performing the installation *must* use a service account with a Microsoft 365 Global Admin and active license
- SharePoint Online and OneDrive must be enabled
- Audit log must be enabled for Microsoft 365. For more information, refer to Microsoft technical documentation and search for **Turn auditing on or off.**
- The following IP addresses must be allowed if there are Firewall rules that prevent third-party applications:
  - 146.112.161.0/24
  - 146.112.163.0/24
  - 146.112.165.0/24
  - 146.112.167.0/24
- Users must have the following API permissions for Microsoft:

API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	Read files in all site collections	Yes
Sites.Read.All	Delegated	Read items in all site collections	No
User.Read	Delegated	Sign in and read user profile	No
User.Read.All	Application	Read all users' full profiles	Yes

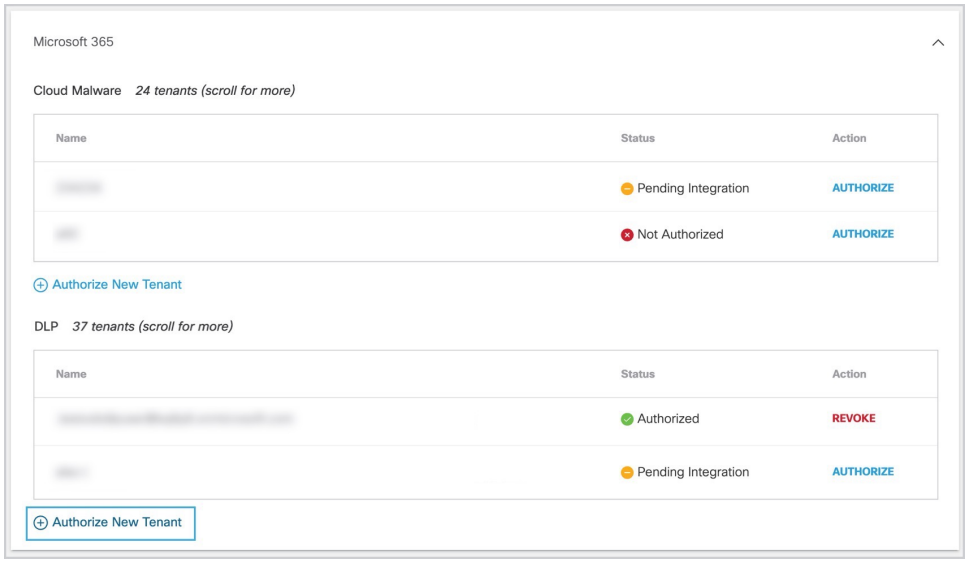
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft 365 Management APIs			
ActivityFeed.Read	Application	Read activity data for the Organization	Yes
SharePoint			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes

Authorize a Microsoft 365 Tenant

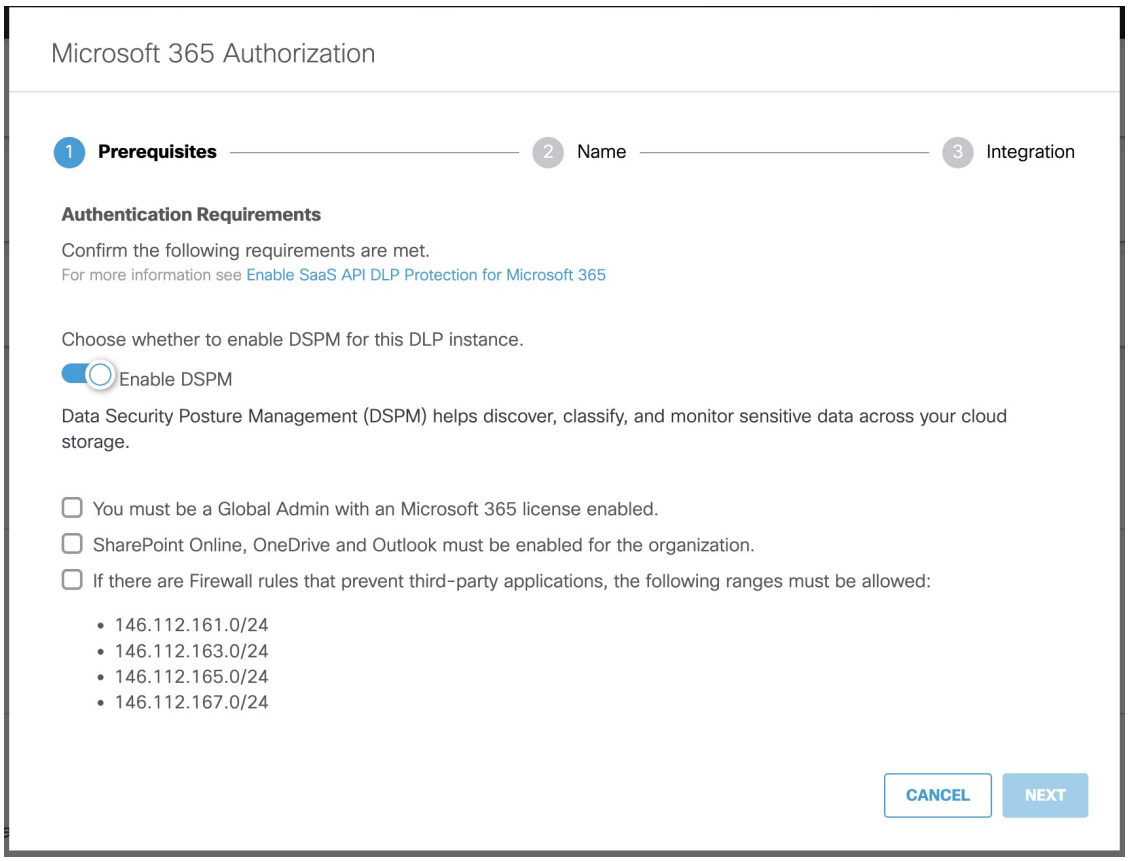
Provides instructions for completing the Authorize a Microsoft 365 Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Microsoft 365**.



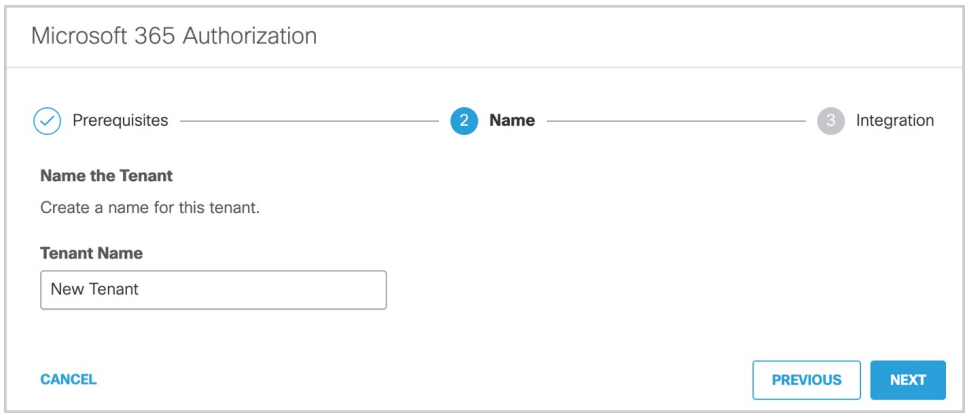
3. Click **Authorize New Tenant** in the **DLP** subsection to add a Microsoft 365 tenant to your Secure Access environment.
4. In the **Microsoft 365 Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.



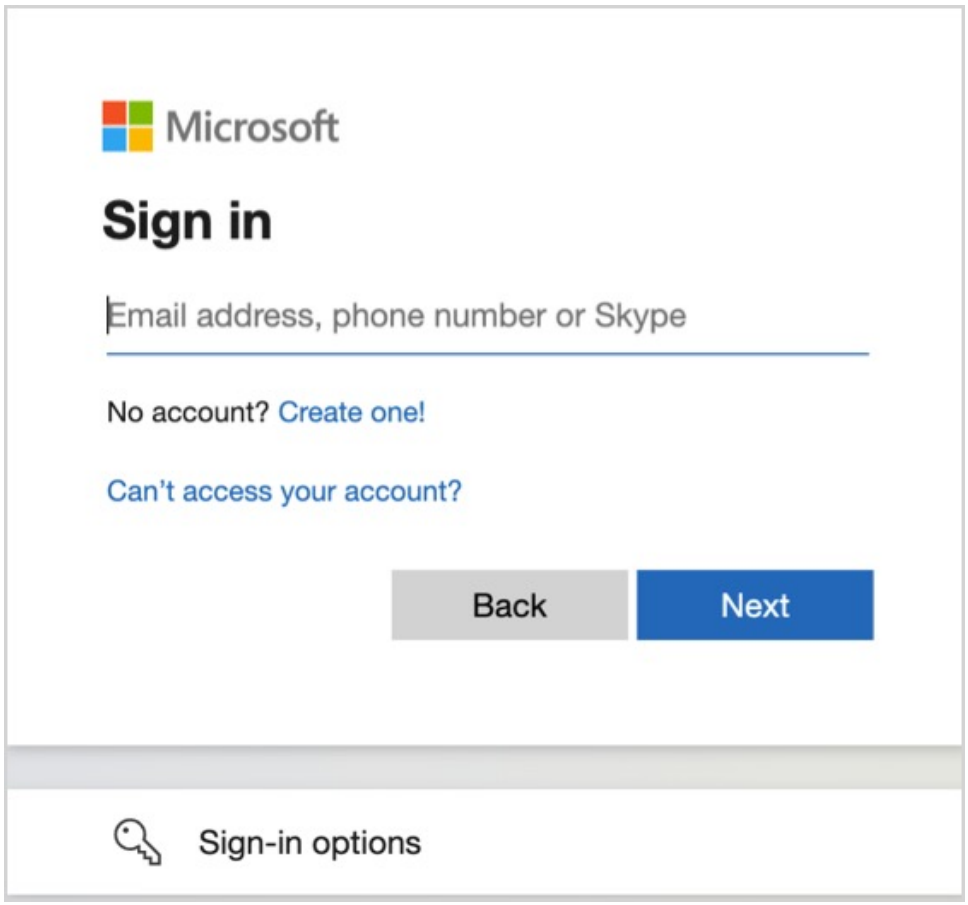
Note

You can enable DSPM at this step. This authorizes the tenant for SaaS API DLP workflows and Data Security Posture Management discovery and posture assessment.

5. Provide a name for your tenant, then click **Next**.



6. Click **Next** to be redirected to the Microsoft 365 login page.
7. Log in to Microsoft 365 with admin credentials to grant access.



You are redirected to Secure Access and a message appears showing the integration was successful.

8. Click **Done** to complete.

Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



Enable SaaS API Data Loss Prevention for Salesforce Tenants

Provides instructions for completing the Enable SaaS API Data Loss Prevention for Salesforce Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports SaaS API DLP protection in Salesforce Enterprise Grid deployments for both production and sandbox development for:

- files uploaded to your Salesforce Enterprise Grid deployment in the Sales Cloud and Service Cloud.
- files exchanged in Salesforce chatter posts.
- chatter posts exchanged with your tenant.
- core sObjects residing in your tenant.
- custom sObjects residing in your tenant.

> **Note**
>
> It may take up to 24 hours after a new custom sObject is created for the system to start scanning that sObject.

To use this feature you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file, chatter post, core sObject, or custom sObject residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

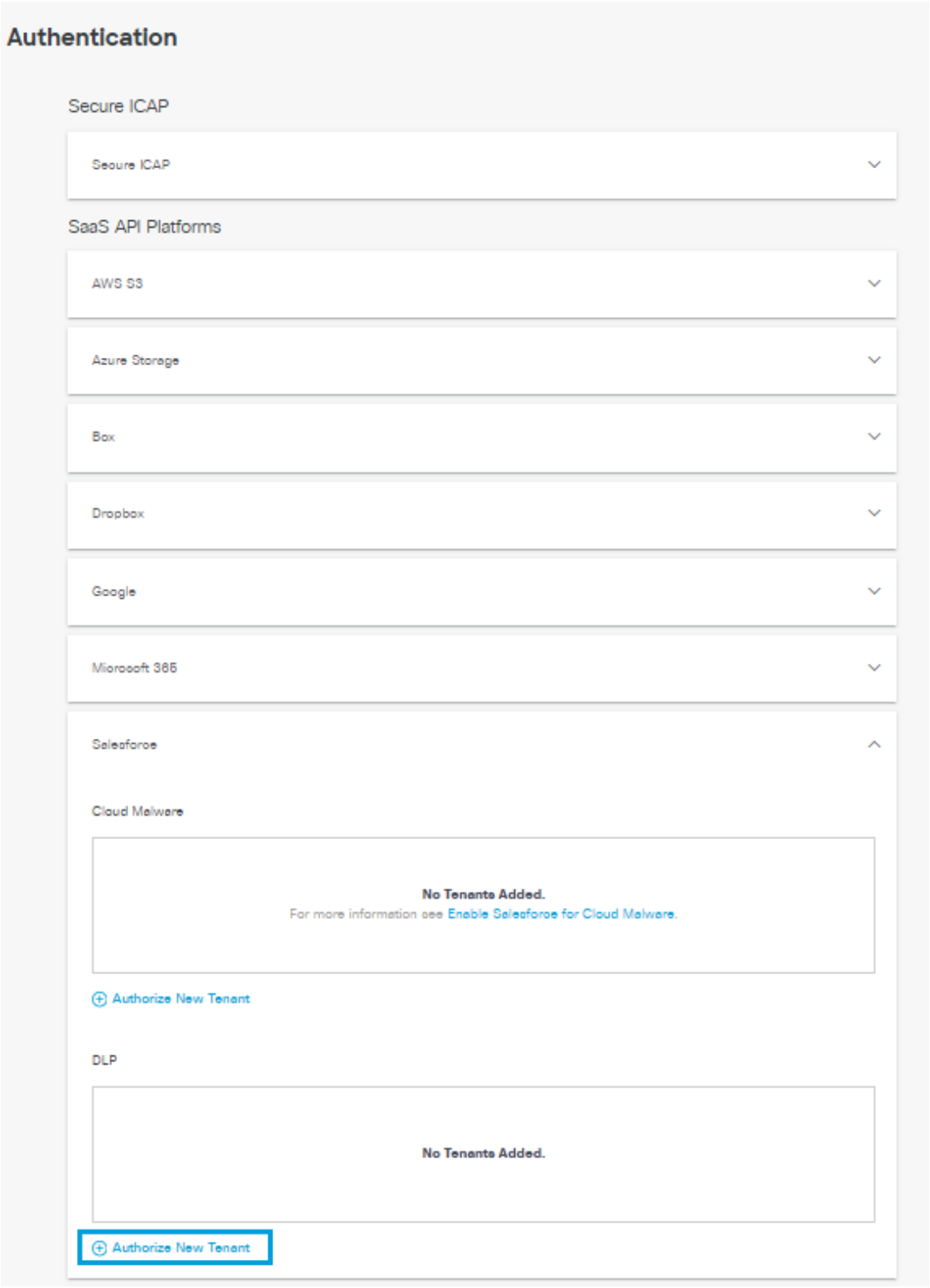
Before you begin

- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Salesforce Enterprise Grid account.
- You must install or update `Node.js`. The Salesforce CLI requires `Node.js` to run. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.
- You must install the Salesforce CLI. This is the primary tool for interacting with Salesforce orgs and managing Salesforce DX projects.
- You must log in to the Salesforce org you intend to authorize as a tenant.
- You must Download the Salesforce quarantine package and install it for your Salesforce tenant. This enables Secure Access to support the quarantine response action for Salesforce files. (If you have already done this to support Cloud Malware Protection for this tenant, you need not do it again.)
- You must set the appropriate systems permissions in your Salesforce deployment. (If you have already done this to support Cloud Malware Protection for this tenant, you need not do it again.)

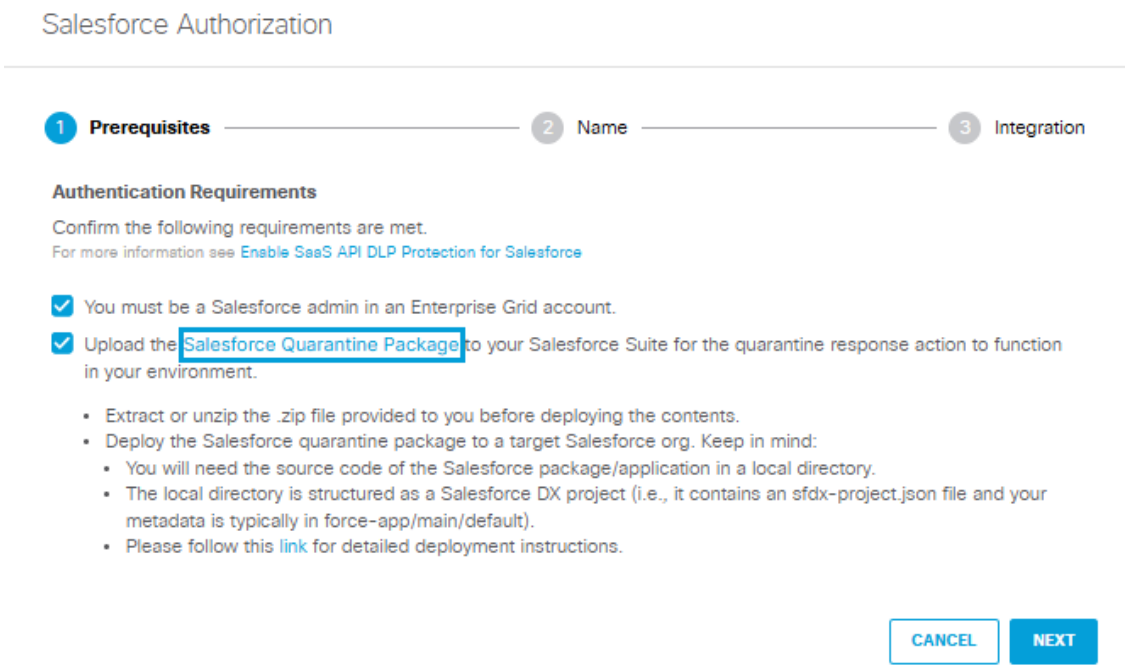
The Salesforce user account to which the quarantine package is deployed and permissions are applied must be the same one that will be used to authorize the Salesforce tenant for SaaS API Data Loss Prevention.

Procedure

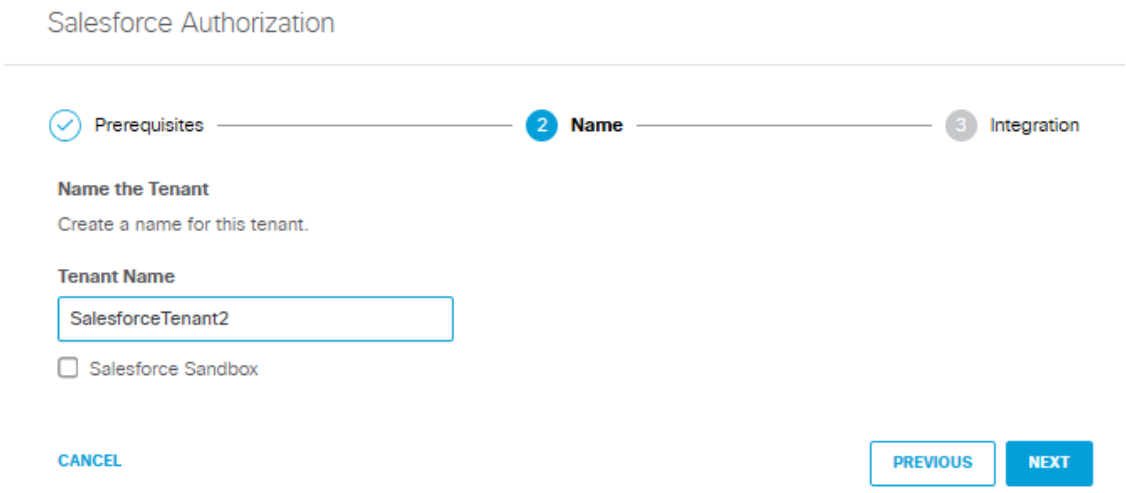
1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click to expand **Salesforce**.



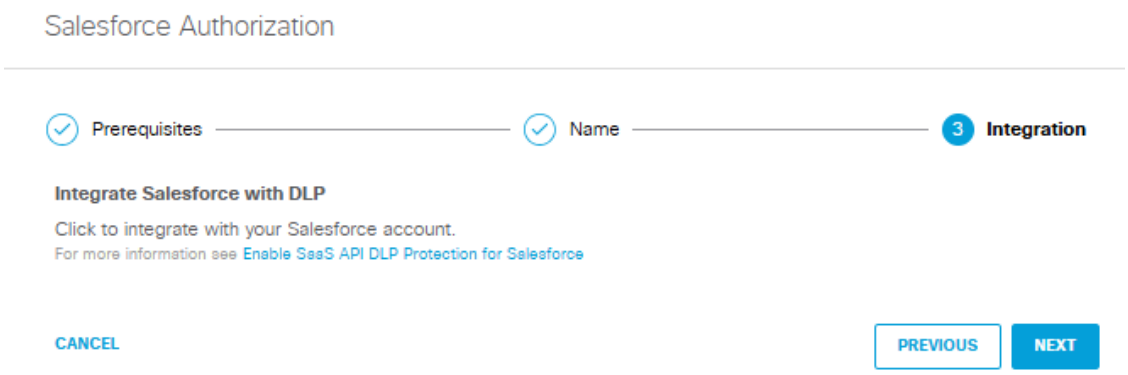
3. In the **DLP** subsection, click **Authorize New Tenant** to add a Salesforce tenant to your Secure Access environment.
4. In the **Salesforce Authorization** dialog, click the **Salesforce Quarantine Package** link and deploy the Salesforce quarantine package to your Salesforce tenant. This enables Secure Access to support the quarantine response action for Salesforce. (If you have already deployed the package to support Cloud Malware Protection for this tenant, you need not do it again.)



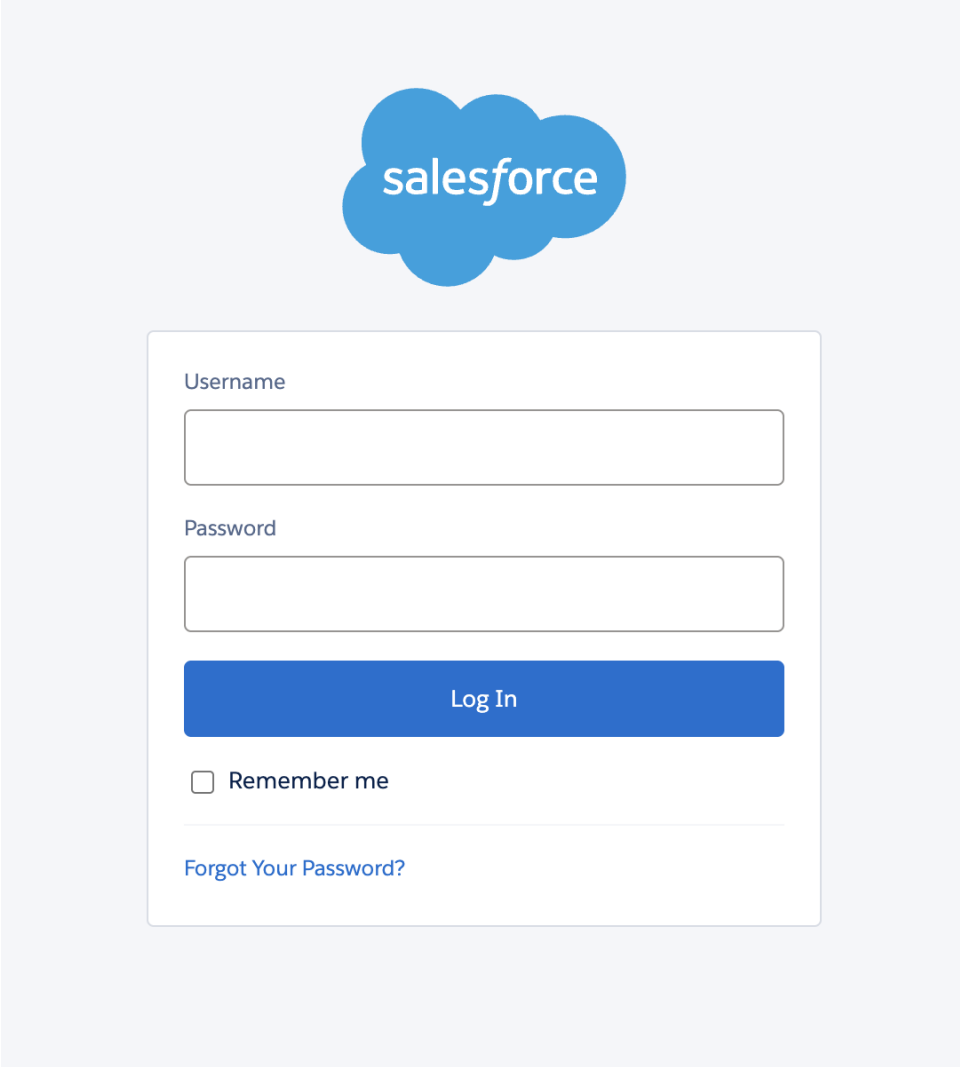
5. In the **Salesforce Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.
6. Enter the **Tenant Name**. If the tenant is a Salesforce sandbox, check **Salesforce Sandbox**. Click **Next**.



7. Click **Next** to be redirected to the **Salesforce** login page.

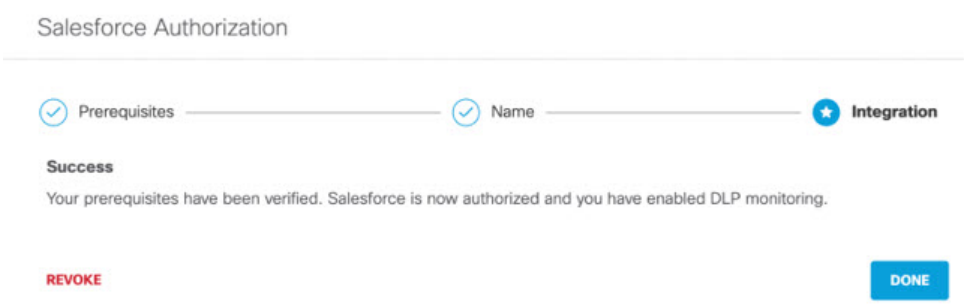


8. Log in to Salesforce with admin credentials to grant access.



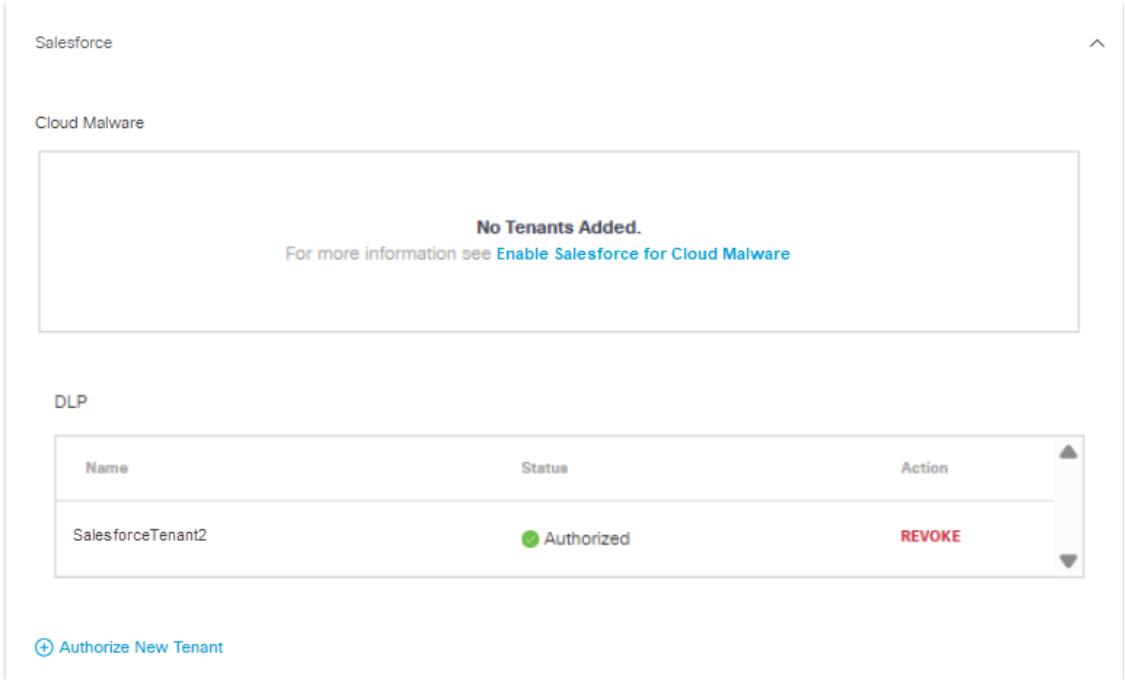
You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized.

9. Click **Done** to complete.



10. The new tenant will appear on the Authorization page in the list under **Salesforce**.

    If you checked **Salesforce Sandbox** in Step 6, the tenant name will have `[Sandbox]` appended to it.



Enable SaaS API Data Loss Prevention for Salesforce Commerce Tenants

Provides instructions for completing the Enable SaaS API Data Loss Prevention for Salesforce Commerce Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports SaaS API DLP protection in Salesforce Commerce deployments for both production and sandbox development for:

Table 24: Scanning cadence and object coverage

Scan Type	Cadence	Object Coverage	Cursor
DLP	Every 7 minutes	product, catalog, category, campaign, gift_certificate	Yes
DLP Discovery	Periodic / on-demand	product, catalog, category, campaign, gift_certificate, promotion, and coupon	No (full poll)

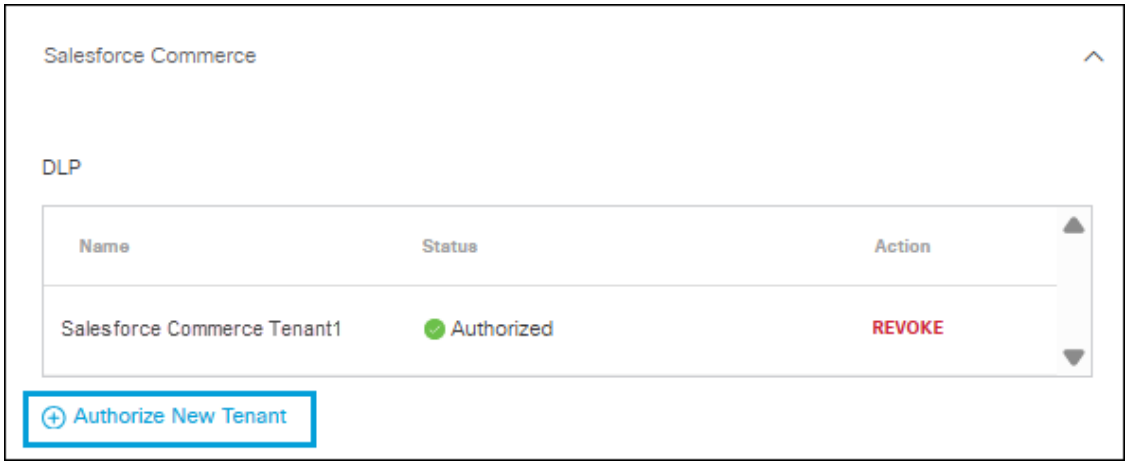
To use this feature you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each item from the list above residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Before you begin

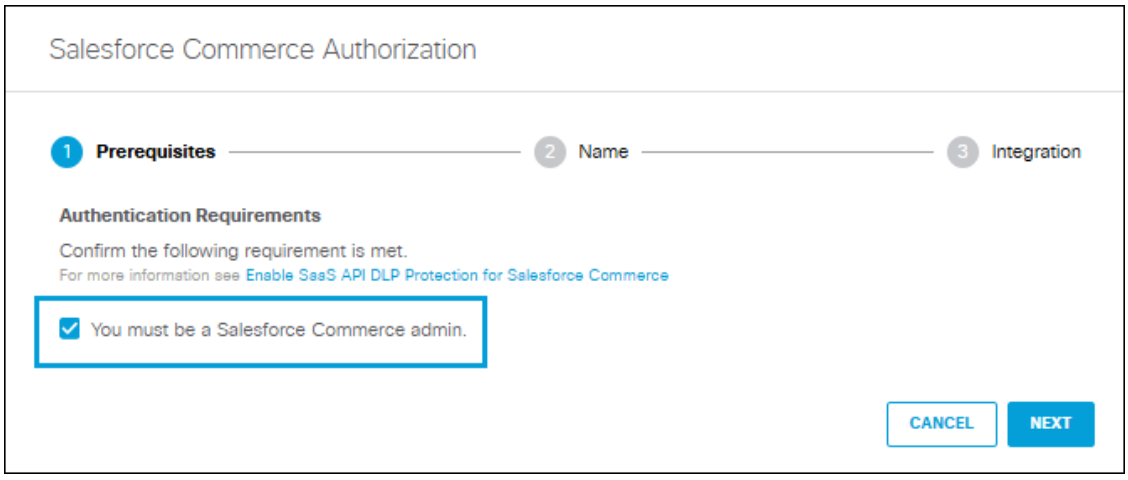
- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Salesforce Commerce account.

Procedure

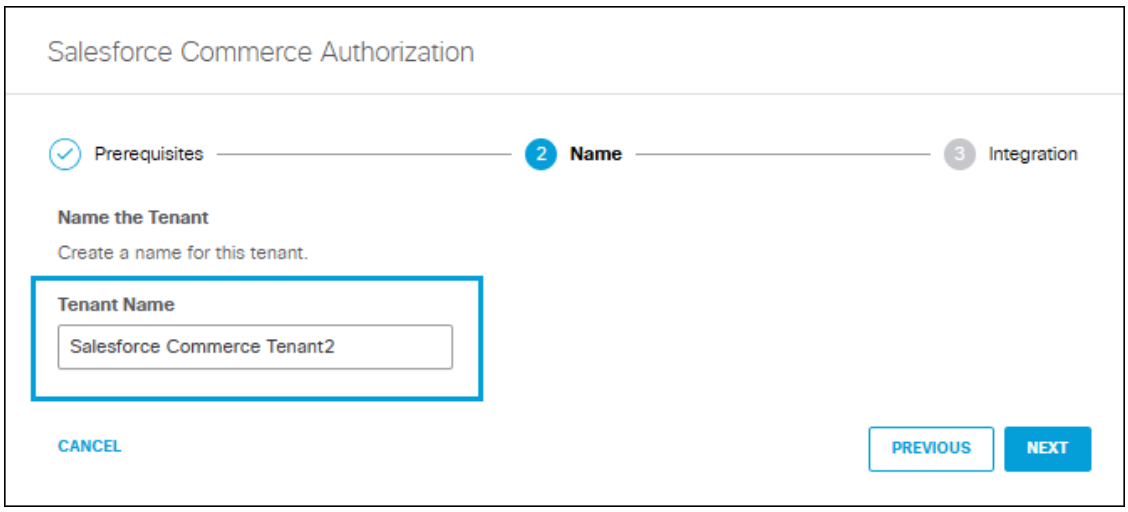
1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click to expand **Salesforce Commerce**.
3. In the **DLP** subsection, click **Authorize New Tenant** to add a Salesforce Commerce tenant to your Secure Access environment.



4. In the **Salesforce Authorization** dialog, check the checkbox to verify you meet the prerequisites, then click **Next**.



5. Enter the **Tenant Name**. Click **Next**.



6. Enter values for for following information associated with your Salesforce Commerce Deployment (See Salesforce :
   - SCAPI Client
     - **Role**: Assign the `Salesforce Commerce API` (realm-scoped) role.
     - **Token Auth**: Set to client_secret_post.
     - **Scopes**: Ensure the following scopes are enabled: `sfcc.products.rw`, `sfcc.products`, `sfcc.catalogs.rw`, `sfcc.catalogs`, `sfcc.campaigns.rw`, `sfcc.campaigns`, `sfcc.gift-certificates`, `sfcc.gift-certificates.rw`, `sfcc.promotions.rw`, `sfcc.promotions`, `sfcc.coupons.rw`, `sfcc.coupons`, `sfcc.sites`, `sfcc.customers`, `sfcc.customers.rw`, `roles`, `profile`, `tenantFilter`, `sfcc.orders`, `sfcc.orders.rw`, `sfcc.preferences`, `sfcc.consents`, `sfcc.experiences`.

     Find this in the Salesforce Commerce Account Manager under **API Client**. See Salesforce documentation for more information.
   - OCAPI API Client
     - **Role**: Assign the `Sandbox API User` (for sandbox) or the equivalent production role defined by your tenant policy.
     - **Token Auth**: Set to `client_secret_post`.

     Find this in the Salesforce Commerce Account Manager under **API Client**. See Salesforce documentation for more information.

     > **Note**
     >
     > Do not assign the `Salesforce Commerce API` role to the OCAPI API client. The OCAPI service does not support this role and will reject the configuration.

   - OCAPI Settings
     - Apply these settings independently for each of your SFCC instances (production, staging, and sandbox).
     - Use Ant-style resource IDs (e.g., `/sites, /libraries/*`) to define access.
     - Use the configuration template provided in the reference section below.

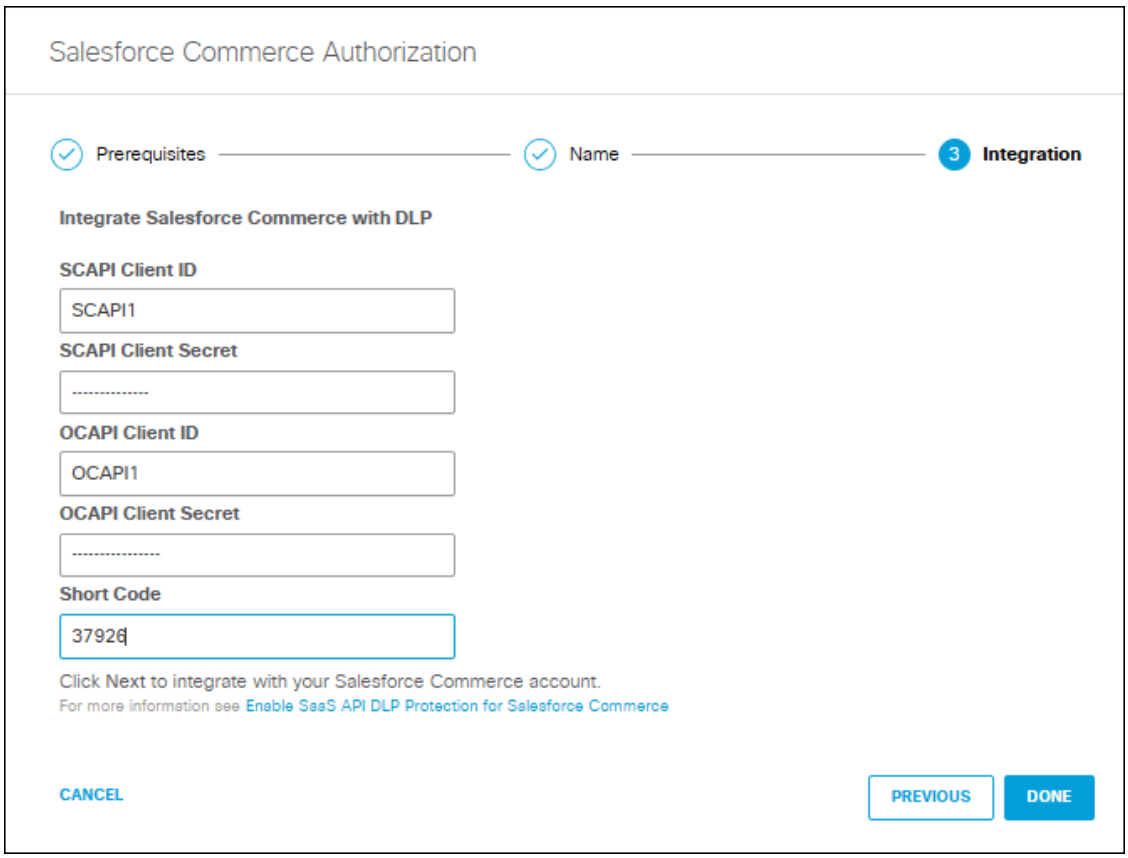
Find this under the Salesforce Commerce Business Manager under **Administration** > **Site Development** > **Open Commerce API Settings**. See Salesforce documentation for more information.

- Short code

  Find this under the Salesforce Commerce Business Manager under **Administration** > **Salesforce Commerce API Settings**. See Salesforce documentation for more information.

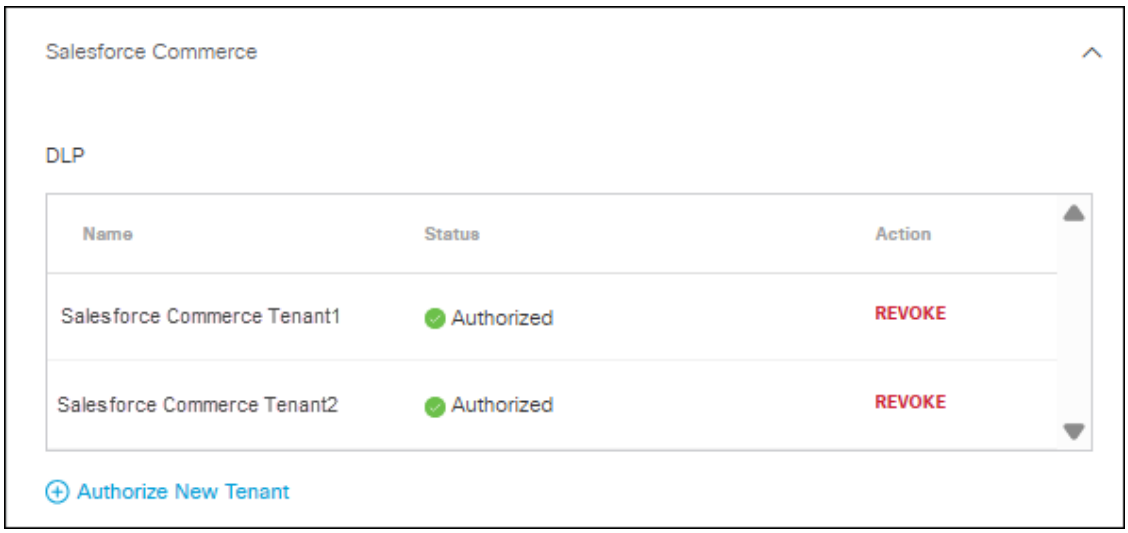
Use the following JSON structure to configure your OCAPI settings within the Business Manager:

```
{
    "_v": "23.2",
    "clients": [
        {
            "client_id": "dad7794b-a60c-440d-b21a-c73874b58387",
            "resources": [
                {
                    "resource_id": "/sites",
                    "methods": ["get"],
                    "read_attributes": "(**)"
                },
                {
                    "resource_id": "/sites/*",
                    "methods": ["get"],
                    "read_attributes": "(**)"
                }
            ]
        }
    ]
}
```



7. Click **Done** to complete.

8. The new tenant will appear on the Authorization page in the list under **Salesforce Commerce**.



Enable SaaS API Data Loss Prevention for ServiceNow Tenants

Describes Enable SaaS API Data Loss Prevention for ServiceNow Tenants in Cisco Secure Access. To apply DLP SaaS API rules to files in a ServiceNow tenant, you must authorize the tenant using the procedure described below.

To apply DLP SaaS API rules to files in a ServiceNow tenant, you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Once you have authorized a ServiceNow tenant for Cloud Malware protection, you can create an app in ServiceNow to view the Cisco Quarantine table maintained in ServiceNow.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).
- The application scope in your ServiceNow deployment must be set to Global.
- You must obtain the Instance Name for your ServiceNow account.
- The user performing the installation must use a ServiceNow account with the **ais_high_security_admin** role and the **oauth_user** role.
- You must add an OAuth Client to your ServiceNow deployment

Limitation

- A tenant that fails to authenticate cannot be deleted.

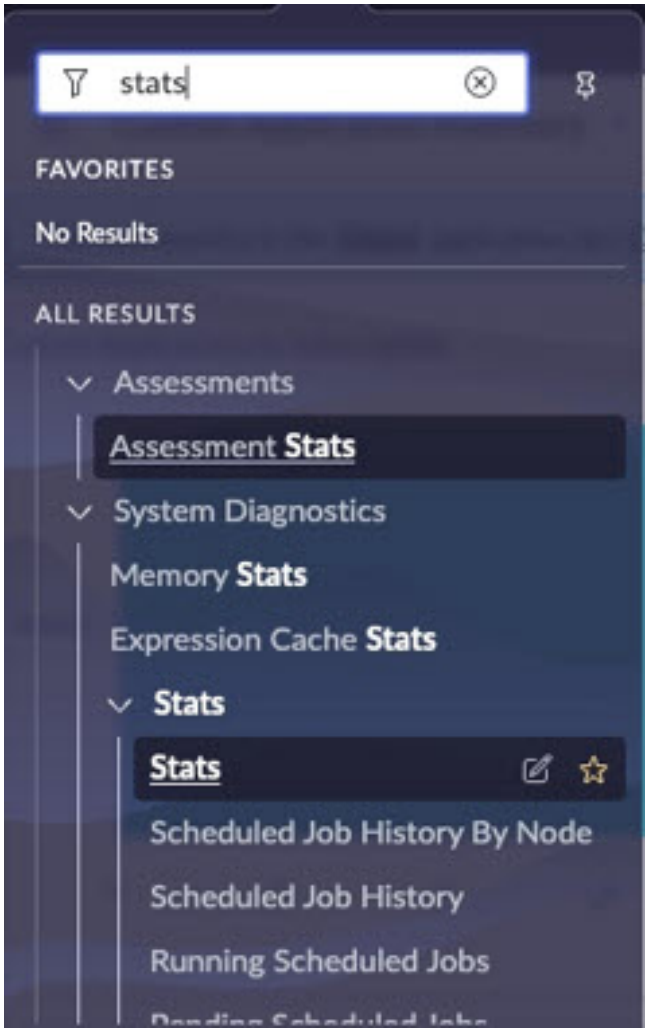
Find the Instance Name for your ServiceNow admin Account

Provides instructions for completing the Find the Instance Name for your ServiceNow admin Account workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal.

Procedure

1. Navigate to the **All** tab.
2. Filter for **Stats**. Under **System Diagnostics** > **Stats** click on **Stats**.



3. In the **Servlet Statistics** page that appears, note the value of the **Instance name**.

Assign the oauth_user role to the ServiceNow admin Account

Provides instructions for completing the Assign the oauth_user role to the ServiceNow admin Account workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal. Make sure your account has the **ais_high_security_admin** role and the application scope is set to **Global**.

Procedure

1. Navigate to **All** > **User Administration** > **Users**.
2. Search for the User ID of the admin account and click on it.
3. Click on the **Roles** tab.
4. Click **Edit**.

5. Under **Collection** search for the role **oauth_user**, select it, and click **>** to move it to the **Roles List**.
6. Click **Save**.

Add an OAuth Client to Your ServiceNow Deployment

Provides instructions for completing the Add an OAuth Client to Your ServiceNow Deployment workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal. Make sure your account has the **ais_high_security_admin** role and the **oauth_user** role, and the application scope is set to **Global**.

Procedure

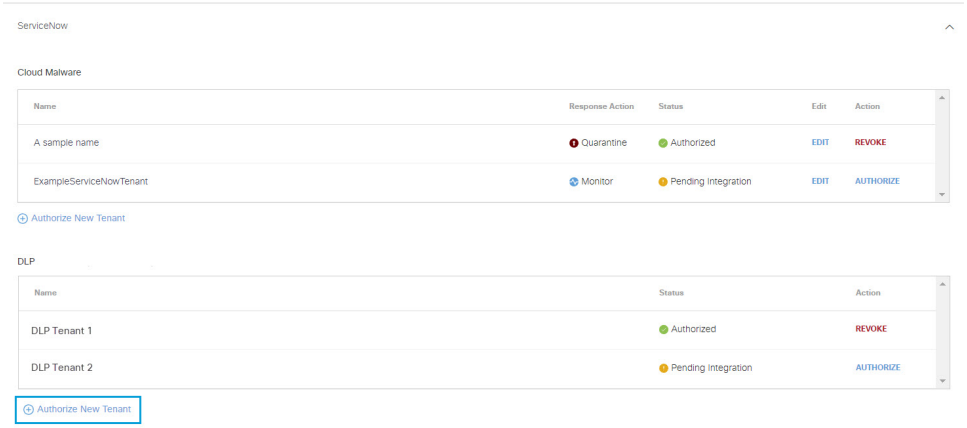
1. Navigate to **All** > **System OAuth** > **Application Registries**
2. Click on **New** and select **Create an OAuth API endpoint for external clients.**
3. Fill out the form that appears with the following required values (other fields are optional):
   - **Name:** Enter a name that will be used by the Secure Access ServiceNow Connector as a Client Id.
   - **Client Secret:** Enter a secret value compliant with your org policy. Take note of this value, as you will need it again when authorizing your ServiceNow tenant with Umbrella.
   - **Redirect URL:** https://management.api.umbrella.com/admin/v2/cloudApplicationInstances/oauth2/callback
   - **Refresh Token Live Span:** We recommend entering 31,536,000 seconds, which is one year. Once the refresh token expires, the ServiceNow tenant will need to be re-authorized with Secure Access.
   - **Application:** Global.
4. Click **Submit**.

Authorize a Tenant

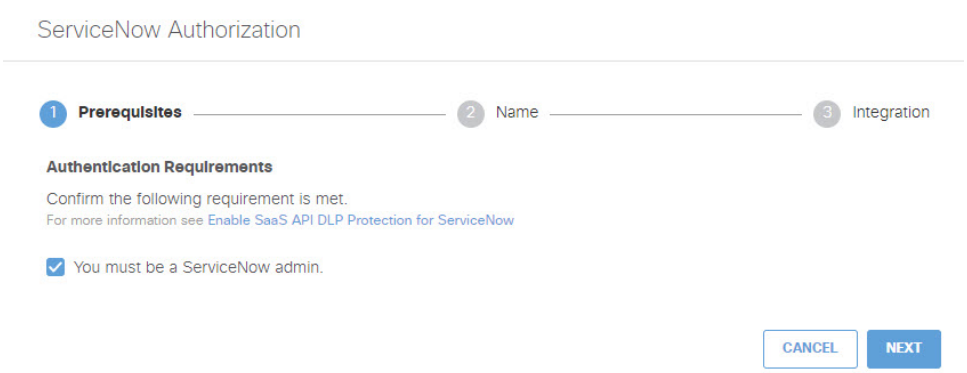
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

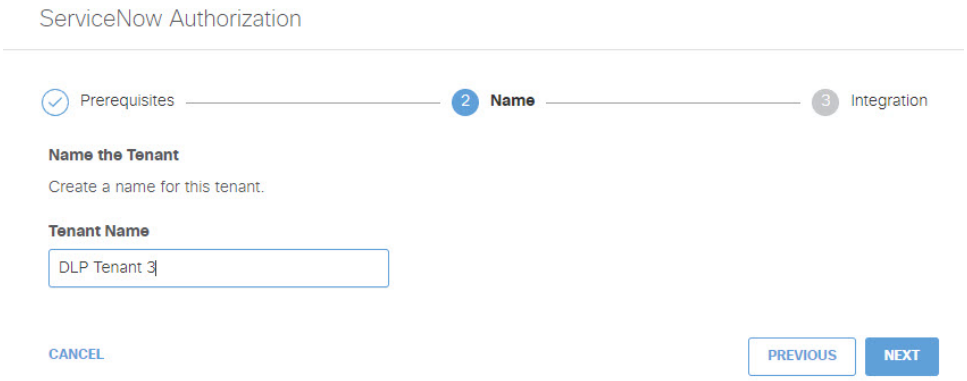
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **ServiceNow**.
3. In the **DLP** subsection, click **Authorize New Tenant** to add a ServiceNow tenant to your Secure Access environment.



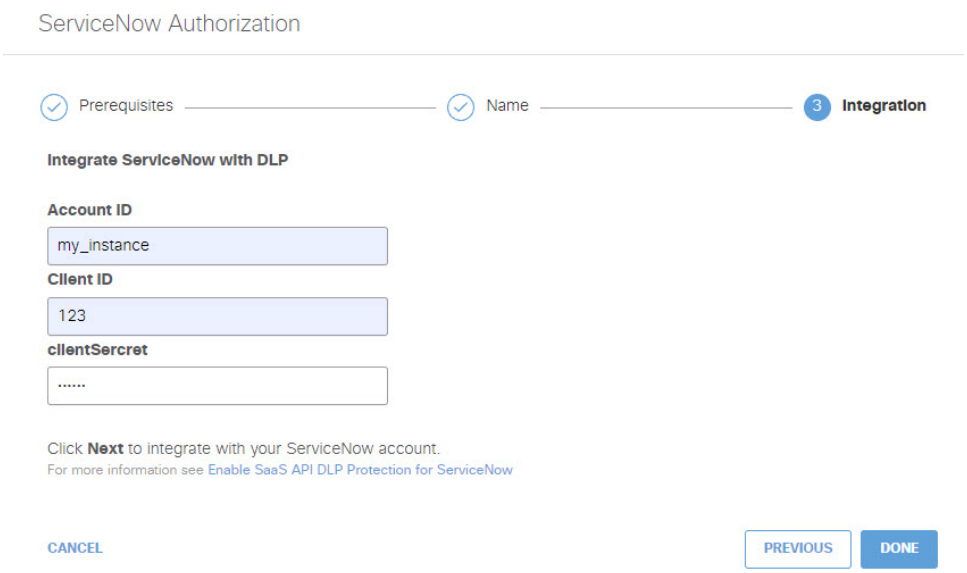
4. In the **ServiceNow Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



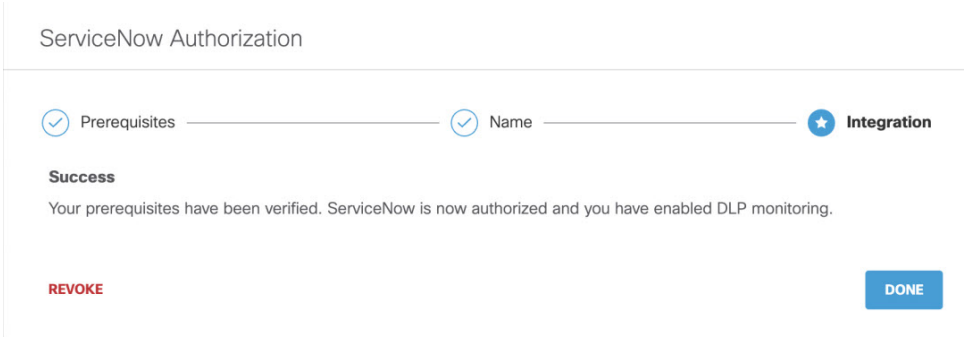
5. Provide a name for your tenant, then click **Next**.



6. Enter the following and then click **Done**.
   - **Account ID**: Enter the Instance Name for your ServiceNow account.
   - **Client ID**: Enter the **Name** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.
   - **Client Secret**: Enter the **Client Secret** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.



7. You are redirected to the ServiceNow OAuth login page and a message will appear notifying you that secure-access-oauth would like to connect to your ServiceNow account. Click **Allow**.
8. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

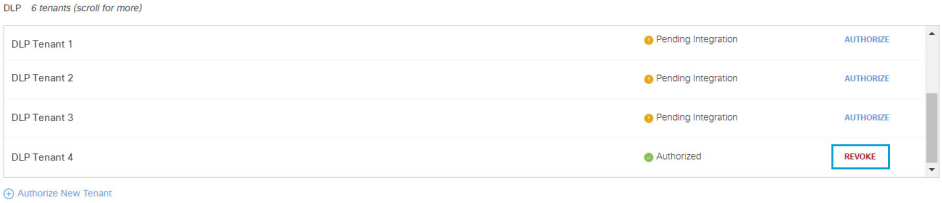


Revoke Authorization

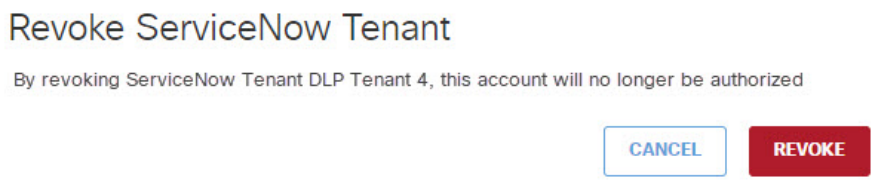
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



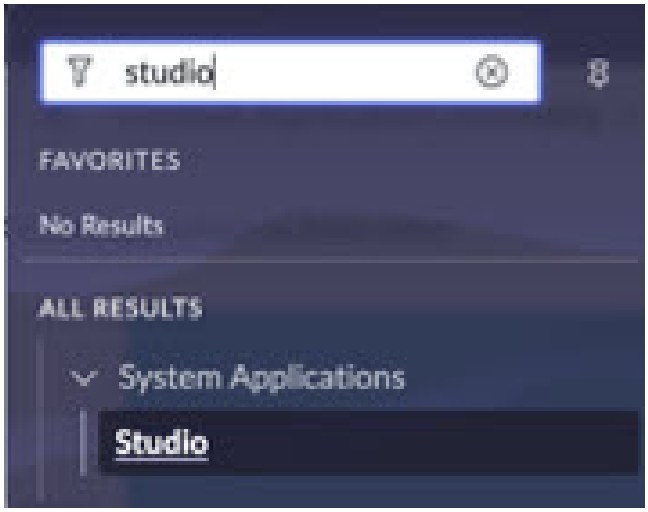
View the Cisco Quarantine Table in Service Now

Provides instructions for completing the View the Cisco Quarantine Table in Service Now workflow in Cisco Secure Access. ServiceNow maintains information about quarantined files in a table called Cisco Quarantine.

ServiceNow maintains information about quarantined files in a table called **Cisco Quarantine**. Perform these steps in your ServiceNow IT Service Management portal to create an application you can use to view that table:

Procedure

1. Filter for **Studio**. Under **System Applications** click on **Studio**.



2. In the Studio interface, click **Create Application**.
3. In the screens that follow, choose the following characteristics for your new application:
   a. Provide an application **Name** and **Description**.

      Under **Advanced settings** choose **Global**.

      Click **Create**.

   b. Under **Roles**, select **ais_high_security_admin**.

      Click **Continue**.

   c. For **Format** select **Classic**.

      Click **Continue**.

   d. For **Data tables** select **Cisco Quarantine [u_cisco_quarantine]**.

      Click **Done with tables**.

4. On the page titled **It's time to design your apps**, click **Start** to the right of the listing for your new application.
5. On the page titled **Let's customize the design of your Classic App**, click **Create**.

Enable SaaS API Data Loss Prevention for Slack Tenants

Describes Enable SaaS API Data Loss Prevention for Slack Tenants in Cisco Secure Access. To apply DLP SaaS API rules to files in a Slack tenant, you must authorize the tenant using the procedure described below.

To apply DLP SaaS API rules to files in a Slack tenant, you must authorize the tenant using the procedure described below. Once the tenant is authorized, for each file residing in the tenant, when Secure Access finds data in violation of an enabled SaaS API rule it will enforce the action of that rule.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).
- You must have a Slack Enterprise Grid account with an active Slack tenant and Slack admin privileges (co-admin does not have sufficient privileges).

Limitations

- A tenant that fails to authenticate cannot be deleted.

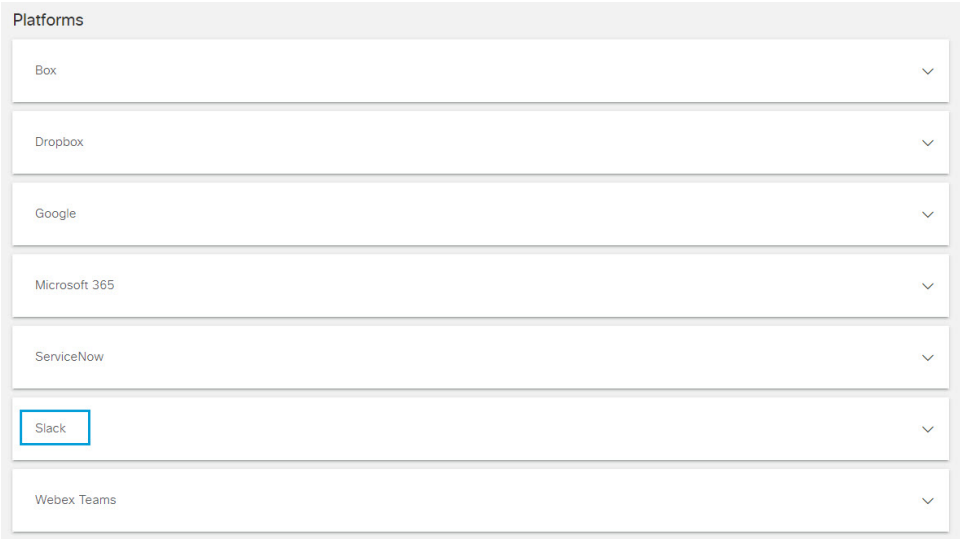
Authorize a Tenant

Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

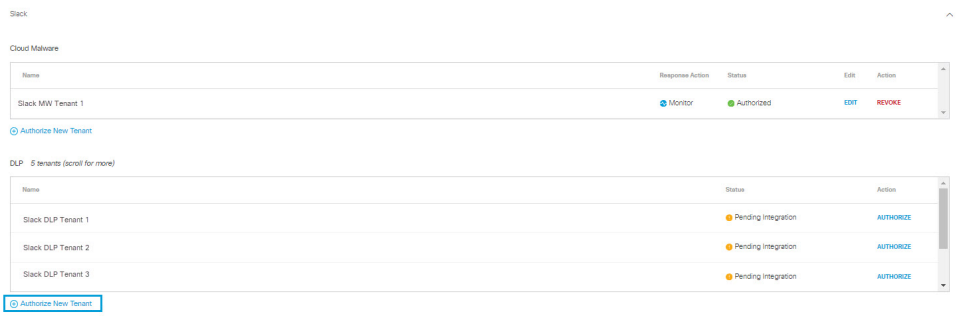
Procedure

---

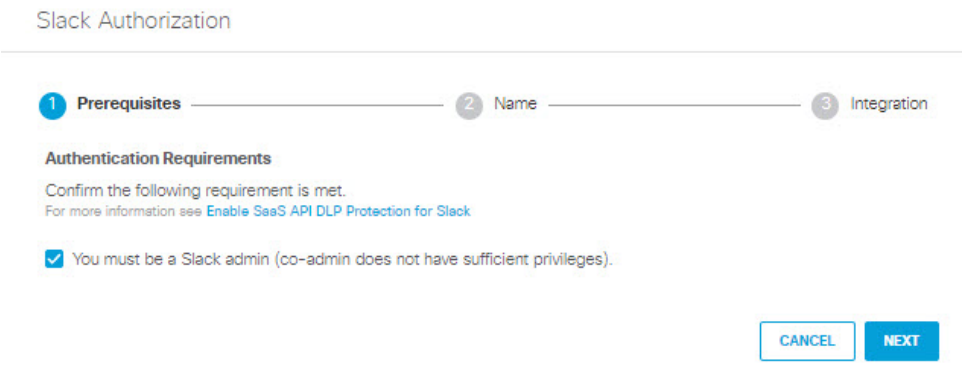
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Slack**.



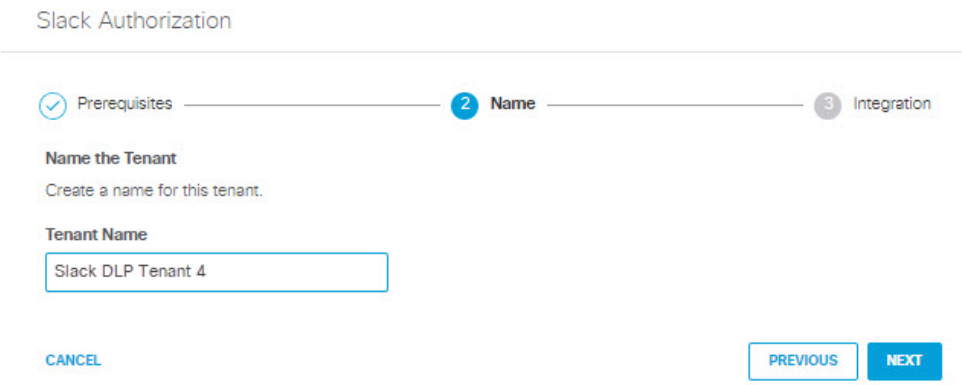
3. In the **DLP** subsection, click **Authorize New Tenant** to add a Slack tenant to your Secure Access environment.



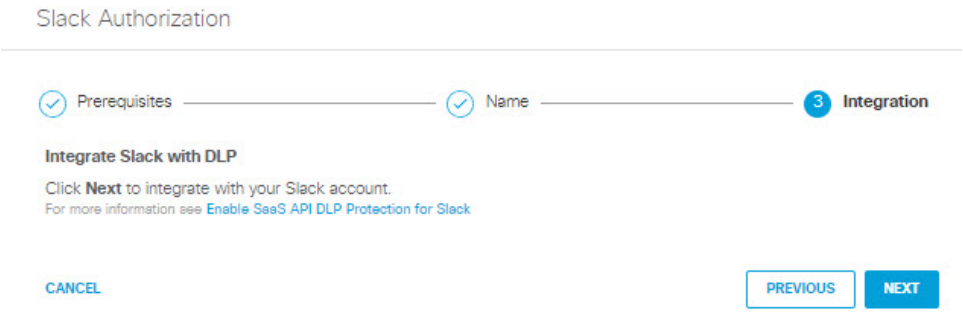
4. In the **Slack Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



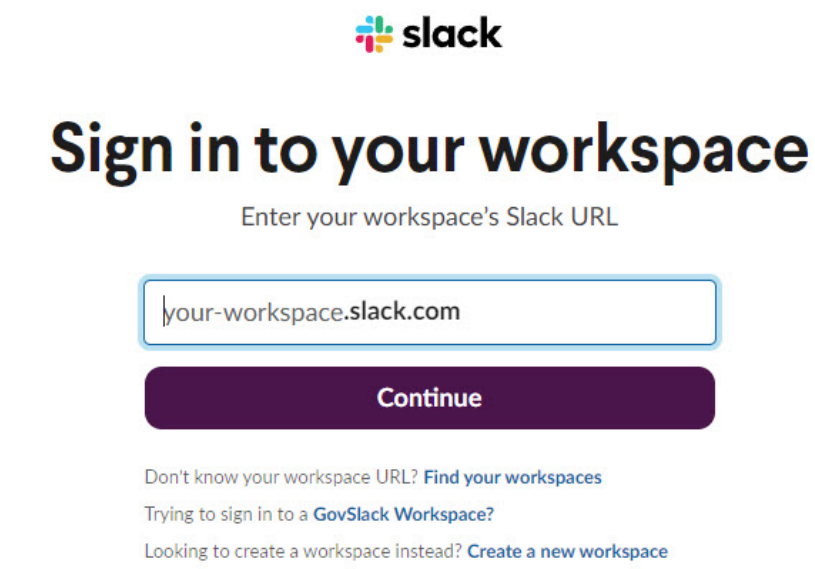
5. Provide a name for your tenant, then click **Next**.



6. Click **Next** to integrate with Slack.



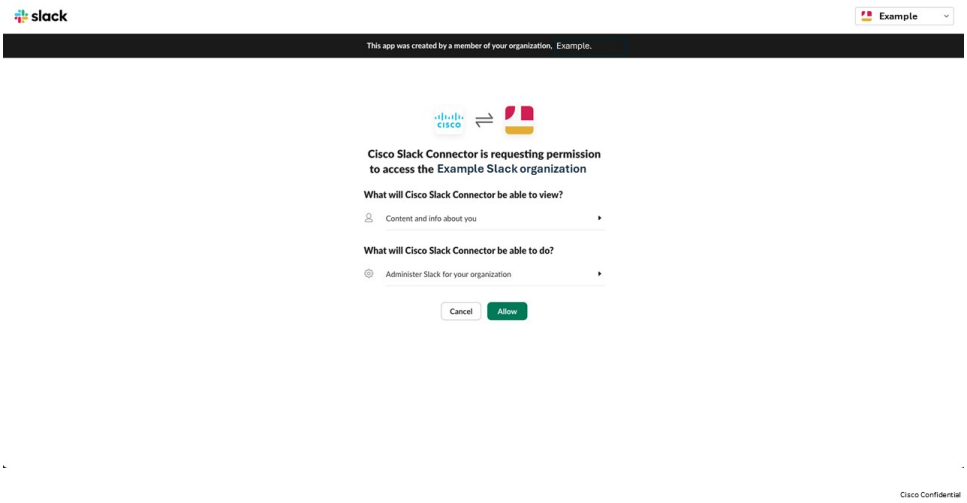
7. If you are not already logged in, the Slack login page will appear; log int to Slack with admin credentials to grant access.



If you are not already logged in to Slack with admin credentials, the Slack login page does not appear; proceed to Step 8.

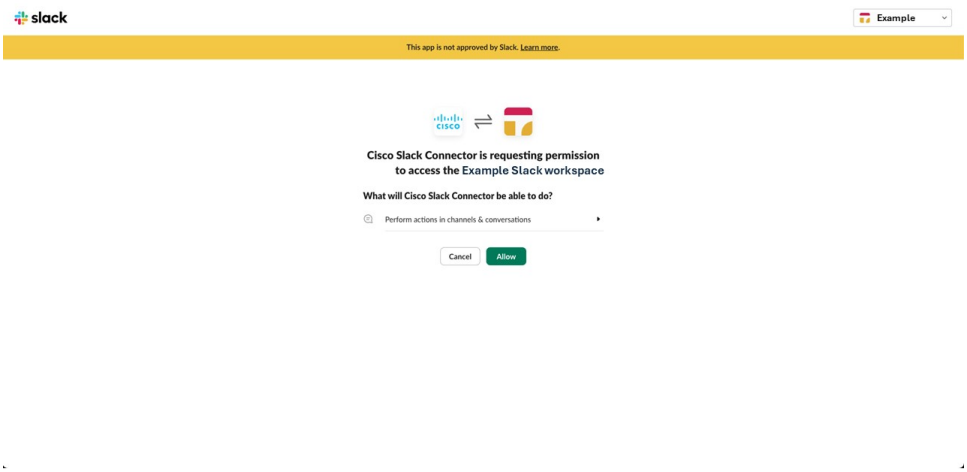
8. Screens with prompts from Slack will appear .

   a. Click **Allow** to authorize the Cisco Slack Connector to view content and information about your Slack account, and to administer Slack for your account.



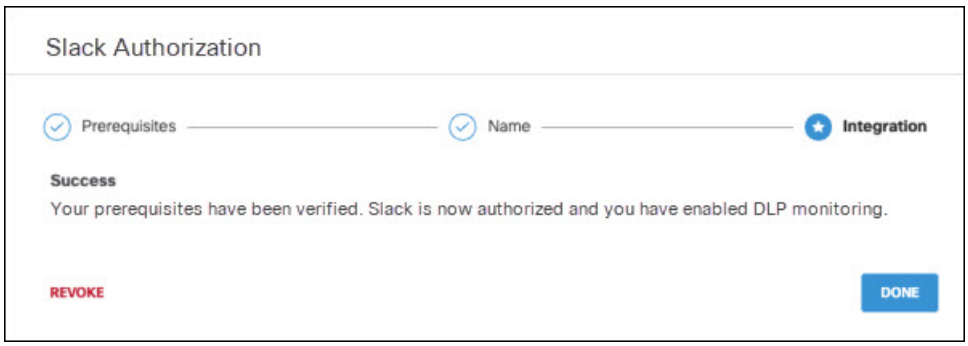
Cisco Confidential

   b. Click **Allow** to authorize the Cisco Slack Connector to perform actions in channels and conversations associated with your Slack account.



Cisco Confidential

9. You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

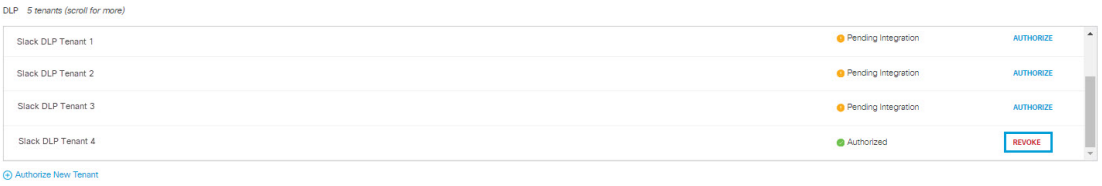


Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account will no longer be authorized.



Enable SaaS API Data Loss Prevention for Webex Teams

Describes Enable SaaS API Data Loss Prevention for Webex Teams in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

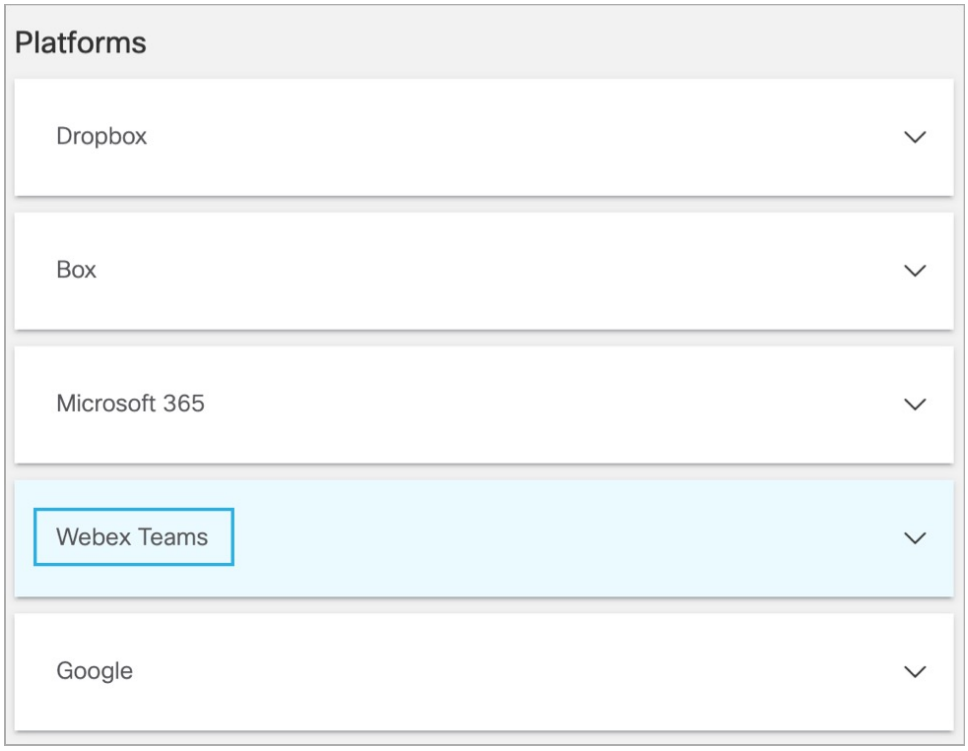
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Full Administrator Privileges in Webex Teams and the Compliance Officer role
- The `EventsAPI` in your Webex Teams instance must be enabled. Contact your Webex Teams support team to ensure that the `EventsAPI` is turned on.

Authorize a Tenant

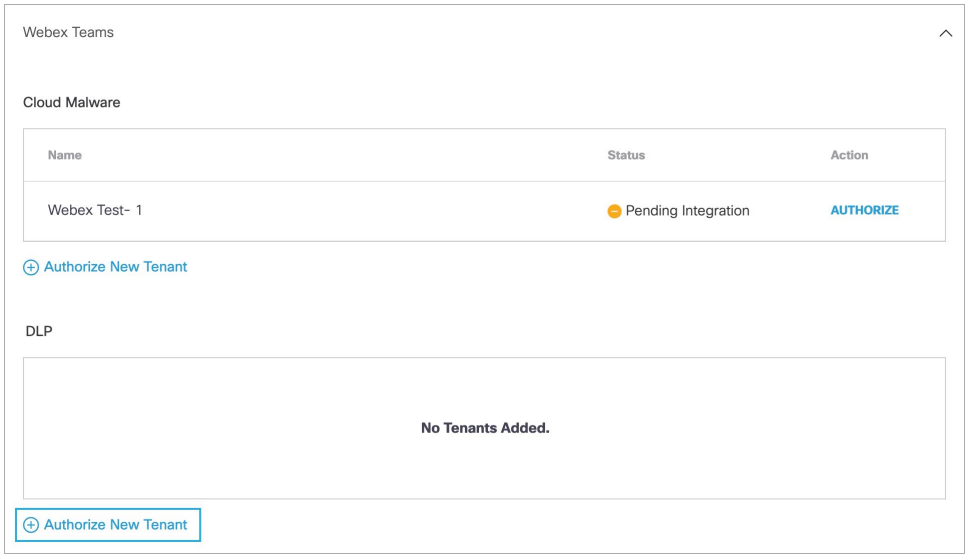
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

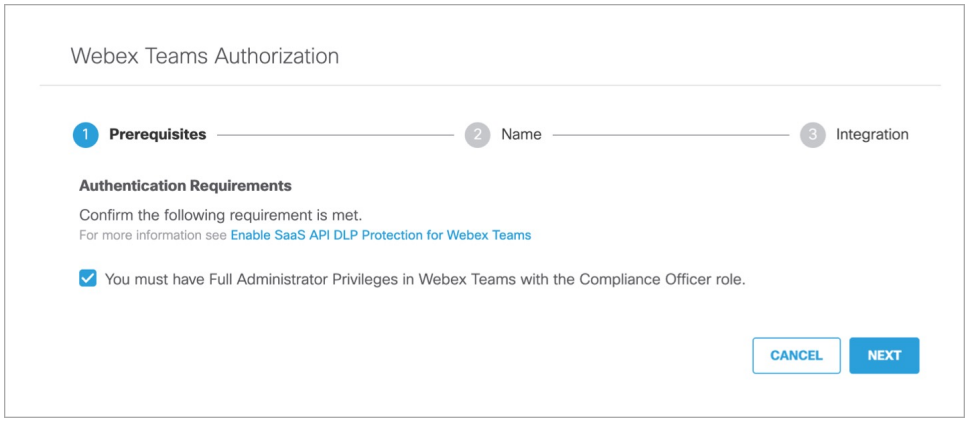
1. Navigate to **Admin** > **Authentication**.
2. Under **Platforms**, click **Webex Teams**.



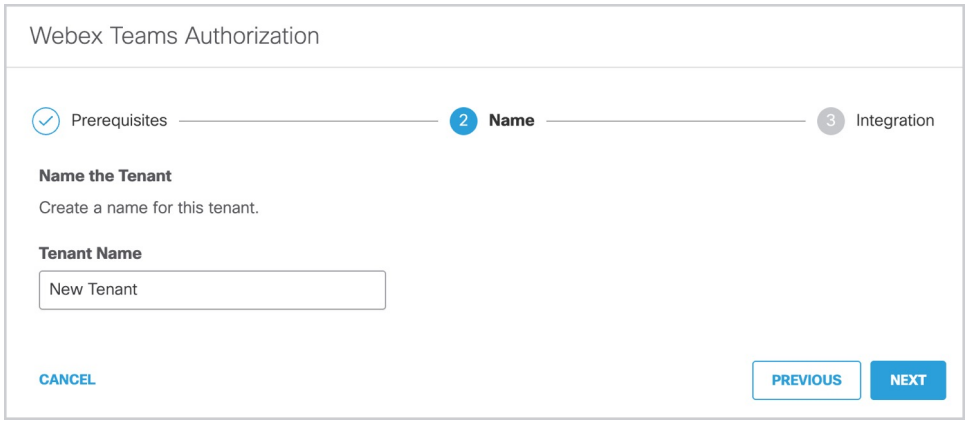
3. In the DLP subsection, click **Authorize New Tenant** to add a Webex Teams tenant to your Secure Access environment.



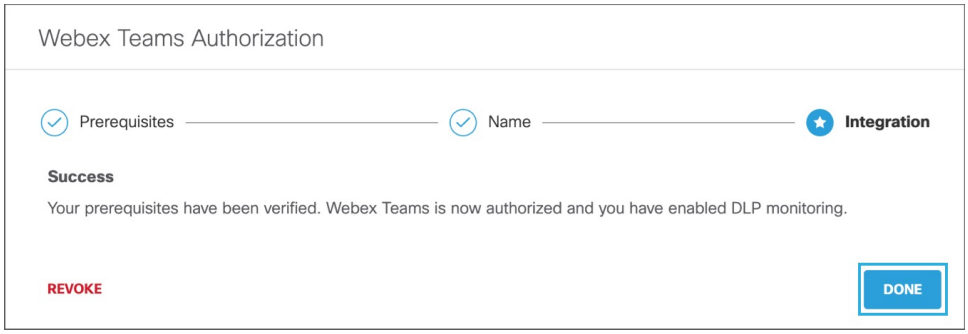
4. In the **Webex Teams Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



5. Enter the name of your tenant, then click **Next**.



6. Click **Next** to complete the integration.
7. Click **Accept** to complete the authorization.
8. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.

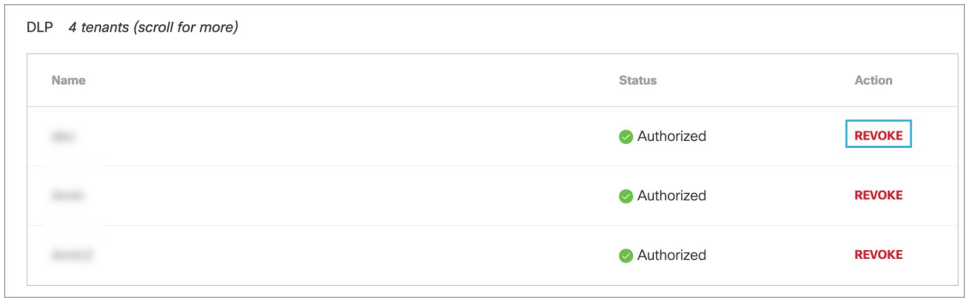


Revoke Authorization

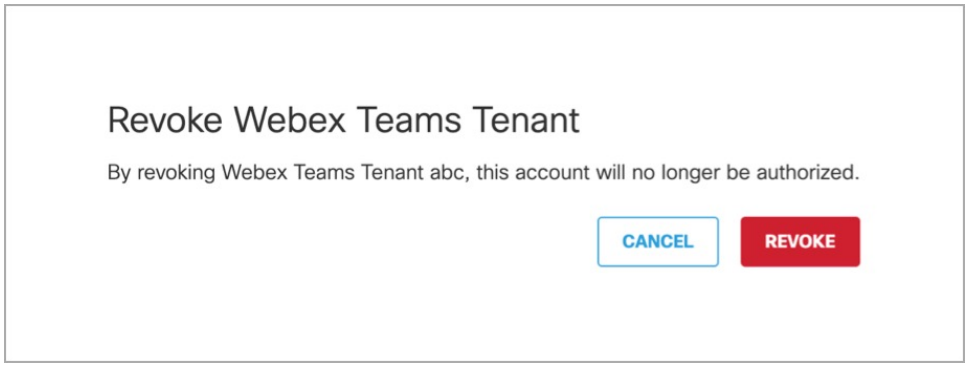
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



51 Cloud Malware Protection

Topics:

- Manage Cloud Malware Protection
- Enable Cloud Malware Protection for AWS Tenants
- Enable Cloud Malware Protection for Azure Tenants
- Enable Cloud Malware Protection for Box Tenants
- Enable Cloud Malware Protection for Confluence Tenants
- Enable Cloud Malware Protection for Dropbox Tenants
- Enable Cloud Malware Protection for GitHub Tenants
- Enable Cloud Malware Protection for Jira Tenants
- Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants
- Enable Cloud Malware Protection for Salesforce Tenants
- Enable Cloud Malware Protection for ServiceNow Tenants
- Enable Cloud Malware Protection for Slack Tenants
- Enable Cloud Malware Protection for Webex Teams
- Cloud Access Security Broker Protection for Google Drive and Microsoft 365
- Enable Cloud Access Security Broker Features for Google Drive

Provides an overview of Cloud Malware Protection in Cisco Secure Access, including Manage Cloud Malware Protection, Cloud Access Security Broker Protection for Google Drive and Microsoft 365, and Enable Cloud Malware Protection. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Cloud Malware Protection

Describes Manage Cloud Malware Protection in Cisco Secure Access. Cloud Malware Protection scans your environment's cloud platforms for malicious files and any other risks.

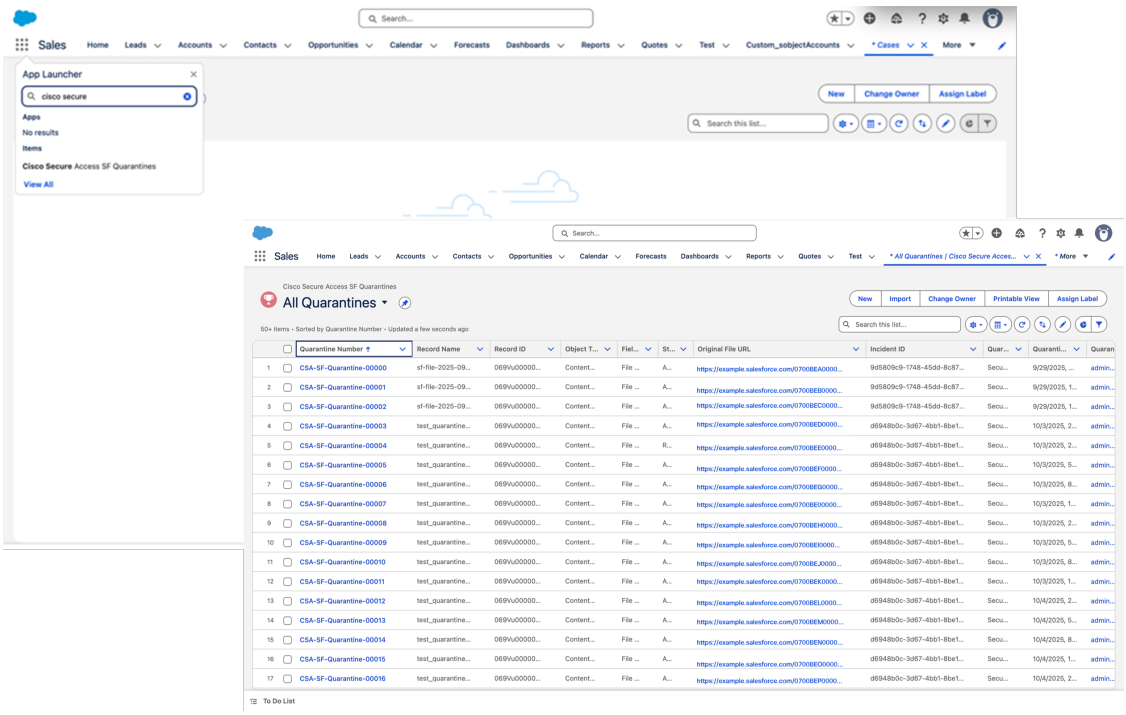
Cloud Malware Protection scans your environment's cloud platforms for malicious files and any other risks. You can enable more than one instance of a platform. For example, a school administration with an instance of Box for teachers and faculty and another for students can enable both instances, the result being complete malware protection for Box.

When you authenticate a tenant for Cloud Malware protection, the scan begins immediately and inspects new and updated files as changes occur. Additionally, one week after the tenant is authenticated Cloud Malware also initiates a retroactive scan of all existing files for the tenant going back in time as far as recorded. The time it takes to complete the retroactive scan depends on the number of files in the tenants and their size and on the API rate limit of the platform vendor.

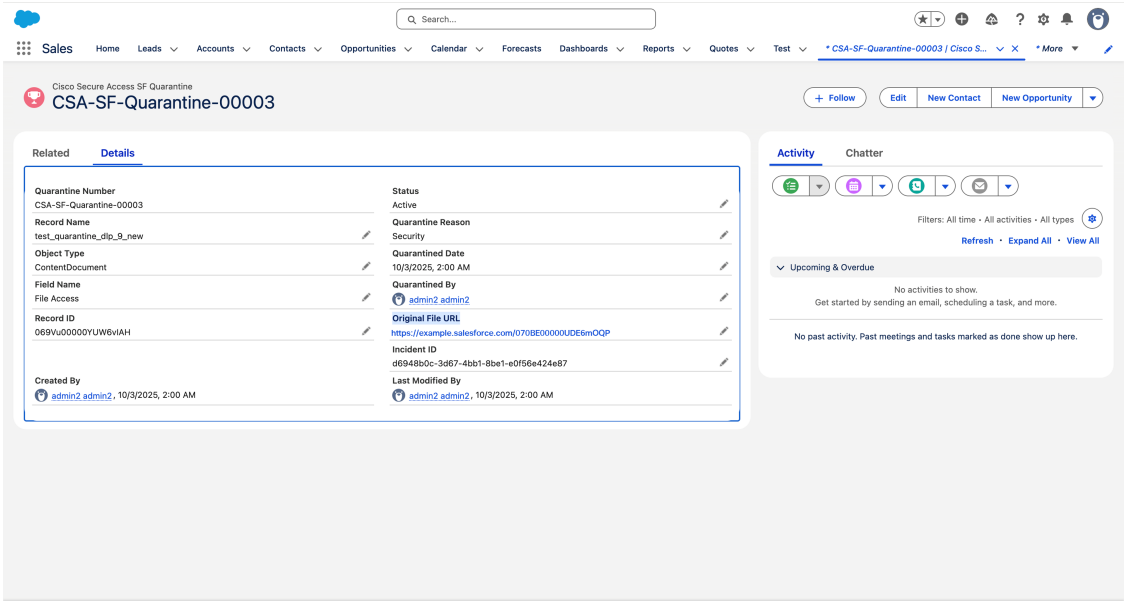
> **Note**
>
> For Microsoft Outlook, Cloud Malware protection applies to the primary inbox only. For outgoing mail you can enable Data Loss Prevention; see Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants.

When Cloud Malware Protection finds malicious files, the information is presented in the Cloud Malware Report. You can remediate potential risk by configuring a response action that Secure Access will automatically apply for malicious files detected within the tenant:

- For all platforms you can choose to monitor the file.
- For Webex Teams and Slack you can choose to delete the file.
- For Dropbox, Box, Microsoft 365, SharePoint, Microsoft 365 OneDrive, and Google you can quarantine the file.
  - The quarantined file is moved into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, removes all collaborators, and changes the file owner to the platform admin.
  - A text file is left in the original location of the quarantined file with the name *`filename`*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware or exposing sensitive data, and for more information to contact their organization administrator.
- For ServiceNow you can choose to quarantine the file.
  - The file is moved into a table named **Cisco_Quarantine_Malware** which can be access only by the admin user who authorized the ServiceNow tenant.
  - A footprint is attached to the notes\activities area of the table the file is attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.
- For Salesforce (uploaded files as well as files attached to chatter posts) you can choose to quarantine the file.
  - The system will remove all collaborators and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.



Click on the listing for an individual file to see the information about it:



- The system replaces the file in its original location with a text file named *filename*_Cisco_Quarantined.txt explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

- Quarantine attempts may fail if the files have been locked or blocked by settings within their native platforms. Settings local to the platform where a file resides take precedence over Secure Access' ability to detect or remediate DLP violations or malware.

You can configure each Cloud Malware instance to automatically apply a response action to malicious files when they are detected, or you can manually trigger a response action from the Cloud Malware report. For more information, see Cloud Malware Report.

Enable Cloud Malware Protection

Provides instructions for completing the Enable Cloud Malware Protection workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

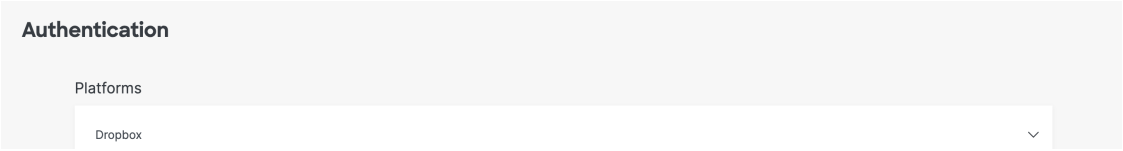
Enable Cloud Malware Protection so that Secure Access scans your environment's cloud platforms for malicious files and any other risks. When Cloud Malware Protection finds malicious files, the information is presented in the Cloud Malware Report.

Before you begin

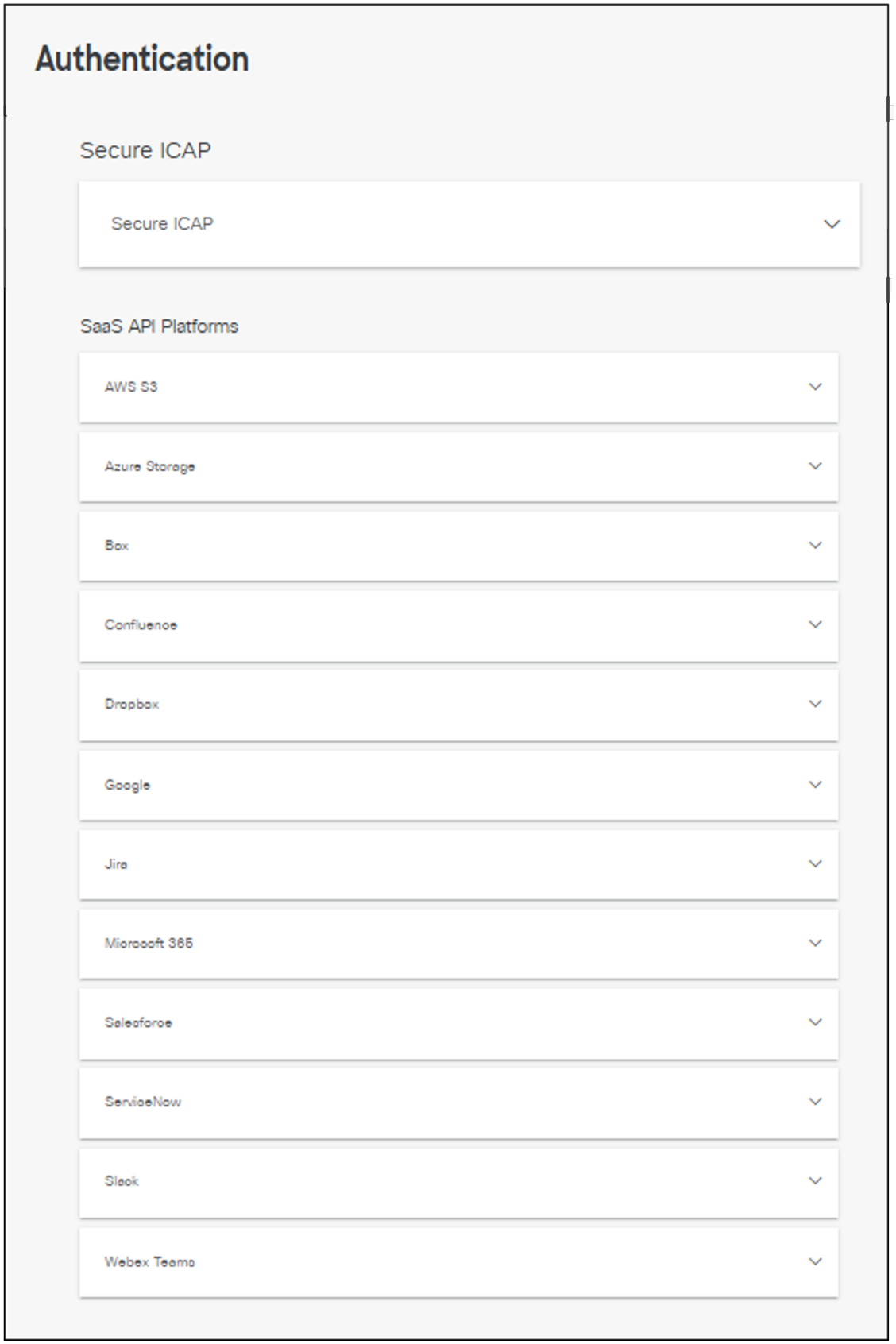
- Full Admin user role. For more information, see Manage Accounts.

Procedure

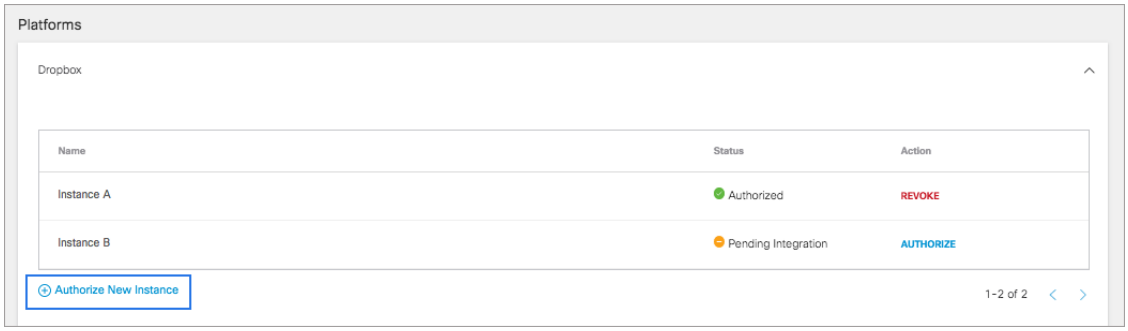
1. Navigate to **Admin** > **Authentication**.



2. In the **Platforms** section, expand a platform.



3. Click **Authorize New Instance** to add an instance of this platform to your Secure Access environment. You can authorize more than one instance of the same platform.



What to do next

Secure Access redirects you to the platform's OAuth login page. Follow the instructions for the platform that you selected to authorize access to Secure Access:

- AWS S3
- Azure Storage
- Box
- Confluence
- Dropbox
- Google
- Jira
- Microsoft 365
- Salesforce
- ServiceNow
- Slack
- Webex Teams

Revoke Authorization for a Platform

Provides instructions for completing the Revoke Authorization for a Platform workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

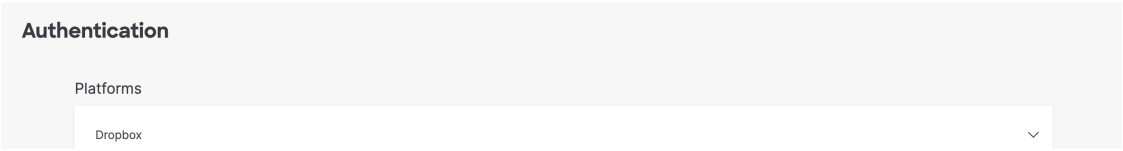
After authorizing a platform in your Secure Access environment, you can revoke authorization at any time.

Before you begin

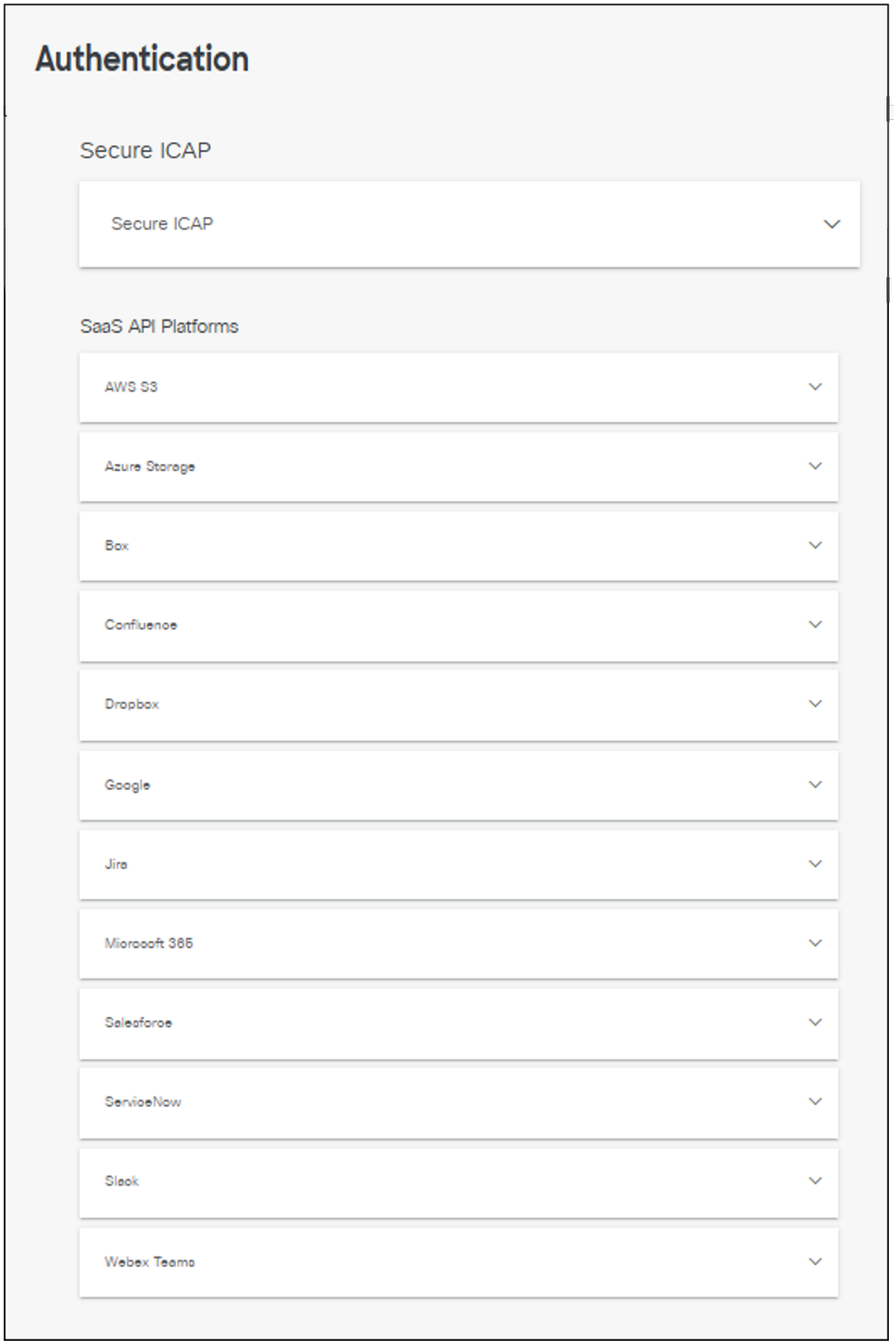
- Full Admin user role. For more information, see Manage Accounts.

Procedure

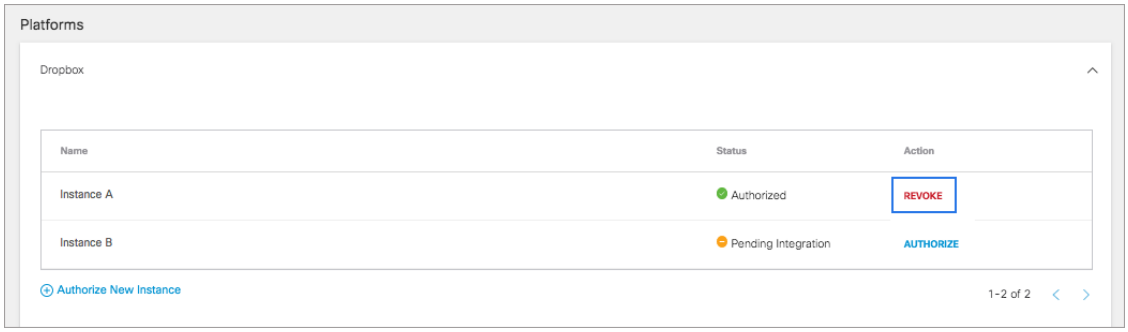
1. Navigate to **Admin** > **Authentication**.



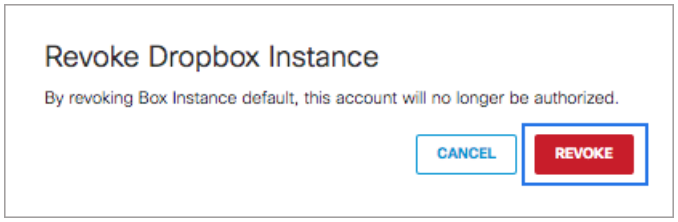
2. Under **Platforms**, click the platform that you wish to revoke.



3. Choose the instance to revoke and click **Revoke**.



4. Click **Revoke** again to complete the process.



Enable Cloud Malware Protection for AWS Tenants

Provides instructions for completing the Enable Cloud Malware Protection for AWS Tenants workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access supports Cloud Malware protection for files within your AWS deployment. To enable this feature:

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- You must have an active AWS tenant and the person doing the installation must be an AWS Administrator.
- You must Enable CloudTrail Event Logging for S3 Buckets and Objects for your AWS account. (You need enable this feature only once for your account; you need not do it for each AWS tenant you authorize.)
- You must Obtain your AWS Account ID.
- Chrome or Firefox is recommended with pop-up blockers/ad blockers disabled (only for the duration of authorization).

Procedure

1. Enable CloudTrail Event Logging for S3 Buckets and Objects from the AWS console. (You need only enable this feature once for your account; you need not do it for each AWS tenant you authorize.)
2. Authorize an AWS Tenant in Secure Access.
3. For each region within which your tenant has resources deployed, Create an AWS Stack from the AWS console.

What to do next

An AWS account can support at most one SaaS API DLP tenant and one Cloud Malware tenant at the same time. You cannot authorize multiple Cloud Malware tenants for a single AWS account.

- A tenant that fails to authenticate cannot be deleted.

Enable CloudTrail Event Logging for S3 Buckets and Objects

Provides instructions for completing the Enable CloudTrail Event Logging for S3 Buckets and Objects workflow in Cisco Secure Access. You must enable CloudTrail event logging to provide you with a record of activities in your AWS account.

You must enable CloudTrail event logging to provide you with a record of activities in your AWS account. You need enable this feature only once for your account; you need not do it for each AWS tenant you authorize.

Procedure

1. In the AWS console, navigate to **CloudTrail** and choose **Create Trail**.



2. Provide a meaningful **Trail name** for your trail.
3. Under **Events**, choose **Data Events** to log data events.
4. For **Storage location**, choose **Use existing S3 bucket**, and choose **Browse** to choose an S3 bucket in your account.
5. You may optionally choose to enable **Log file SSE KMS encryption** for your log files. (If you choose this option, see Step 11.)
6. On the**Choose log events** page, choose **Data events**.
7. For **Data event source** choose **S3**.
8. You can choose from:
   - **Log all current and future S3 buckets** (This is the default.)

     Choose to log **Write** events.
   - **Individual bucket selection** (This can be a more economical choice.)

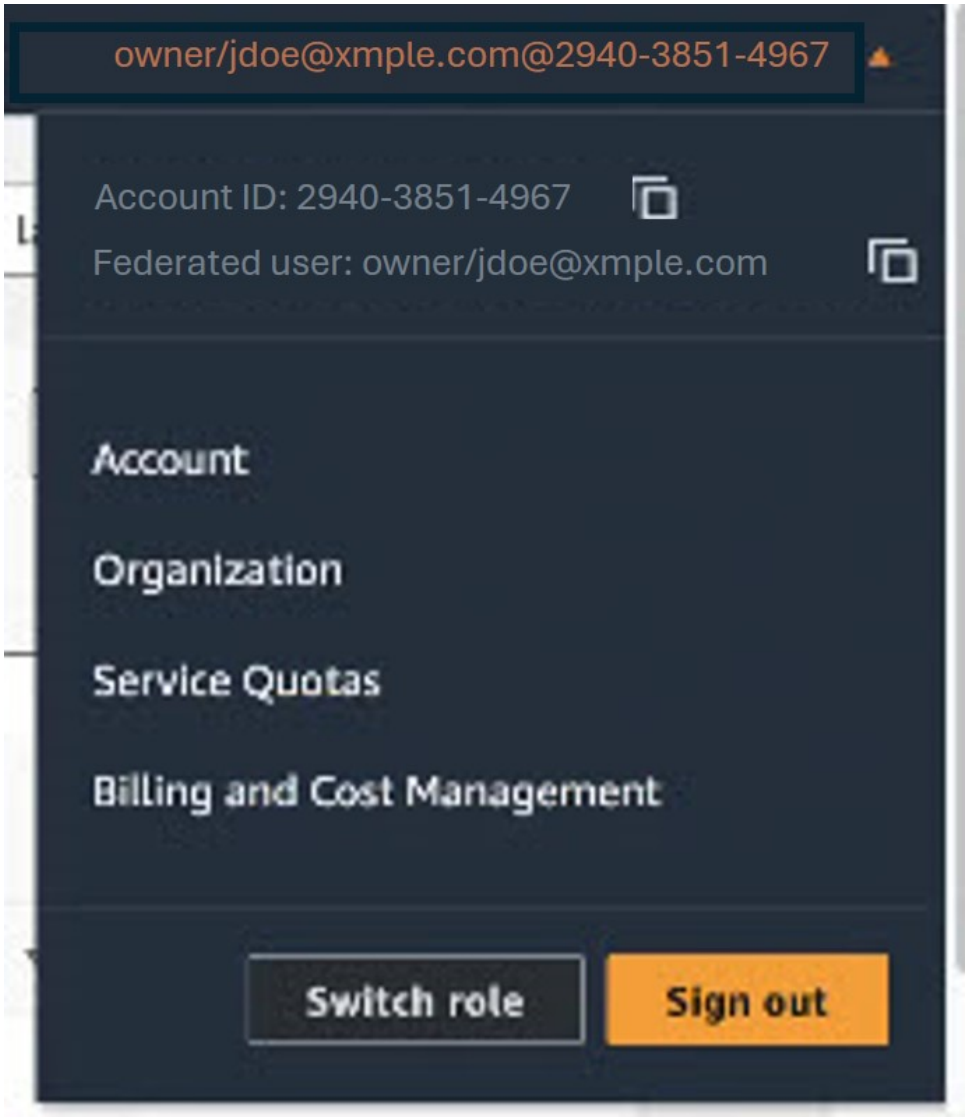
     Browse for existing buckets and click **Add bucket** to log data events for each. Choose to log **Write** events.
9. For the remaining options in the CloudTrail creation wizard, choose the settings appropriate to your environment.
10. On the **Review and Create** page, review your choices and **Edit** if necessary. Then click **Create Trail**.
11. If in Step 5 you chose to enable **Log file SSE KMS encryption** for your log files, grant permission for the encryption key to the role **CiscoSecureAccessScanner**. In the AWS console, under **Key Management Service (KMS)** > **Customer managed keys** > **Key ID** > **Edit key policy**, add a statement to grant permission for the role **CiscoSecureAccessScanner**.
12. If your S3 buckets have restrictive policies associated with them, add statements to those policies to grant the role **CiscoSecureAccessScanner** access to those buckets. In the AWS console, see **Amazon S3** > **Buckets** > **Bucket Name** > **Permissions** > **Bucket Policy**.

Obtain Your AWS Account ID

Provides instructions for completing the Obtain Your AWS Account ID workflow in Cisco Secure Access. Log in to the AWS Management Console with an Admin account.

Procedure

1. Log in to the AWS Management Console with an Admin account.
2. In the navigation bar at the upper right, click on your user name. The account ID is displayed above your user name.
3. Click the **Copy** icon to the right of the Account ID to copy it.

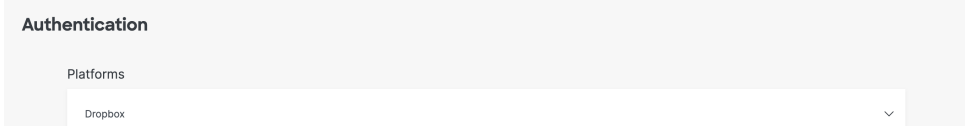


Authorize an AWS Tenant

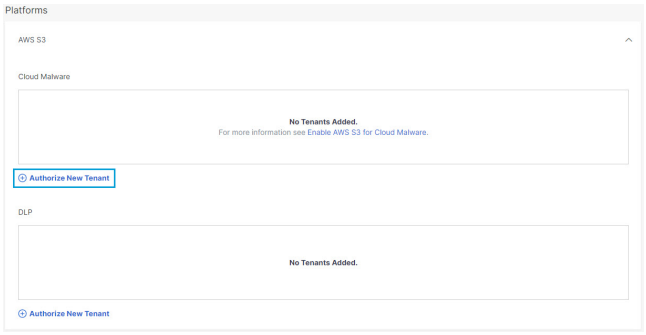
Provides instructions for completing the Authorize an AWS Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

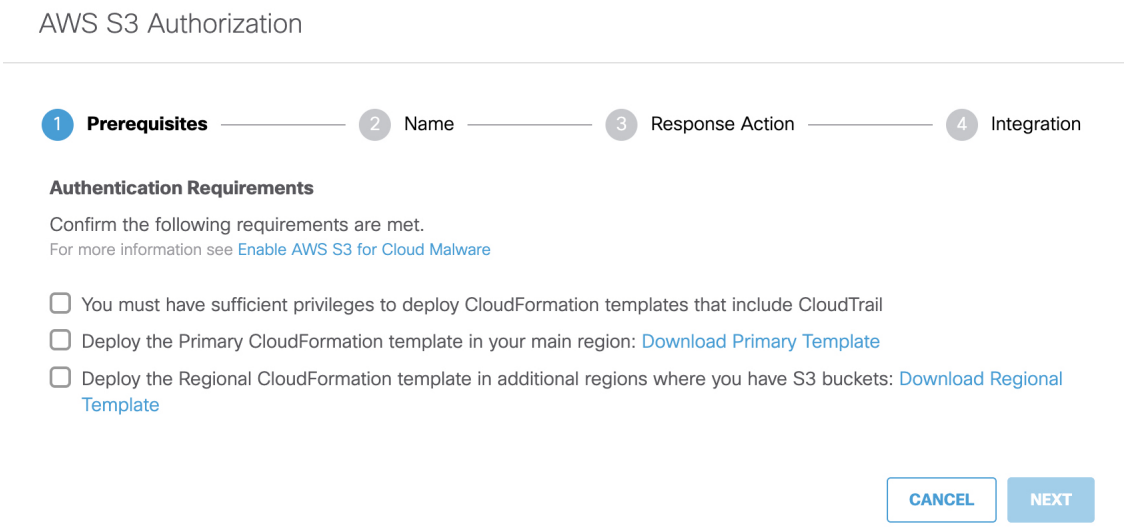
1. Navigate to **Admin** > **Authentication**.



2. Under **Platforms**, click to expand **AWS S3**.
3. Under **Cloud Malware** click **Authorize New Tenant** to add an AWS S3 tenant to your Secure Access environment.

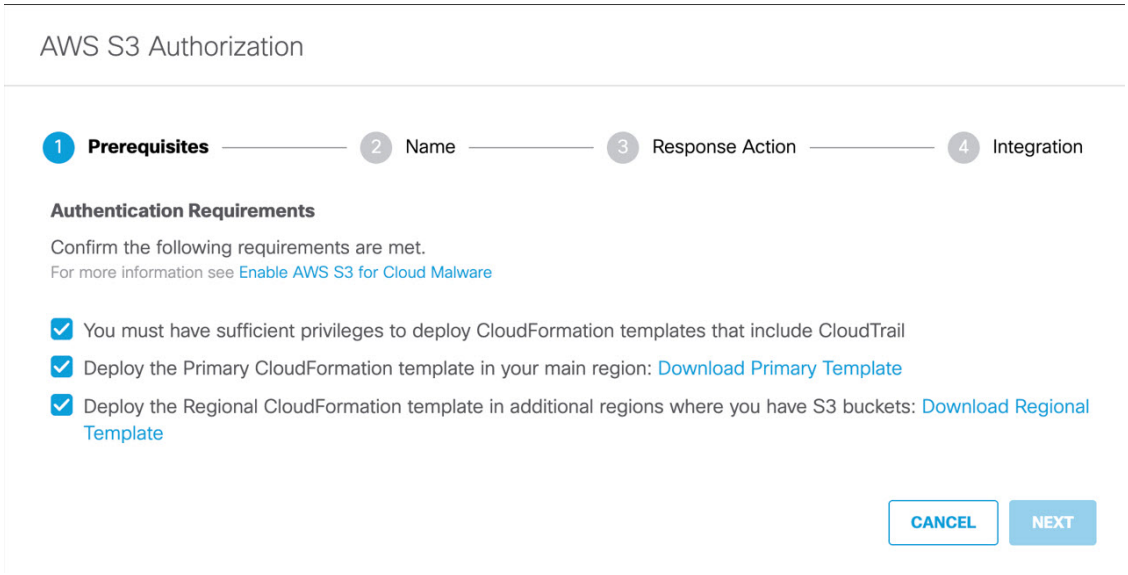


4. In the **AWS S3 Authorization** dialog box, click **Download Primary Template** to download an AWS CloudFormation template for your main region (**primary-cloudformation-template.json**). If you have S3 buckets in additional regions, click **Download Regional Template** to download an AWS CloudFormation template for those regions (**regional-cloudformation-template.json**). Save the templates to your local machine, then for each of the regions where you have S3 buckets, Create an AWS Stack before proceeding to the next step.

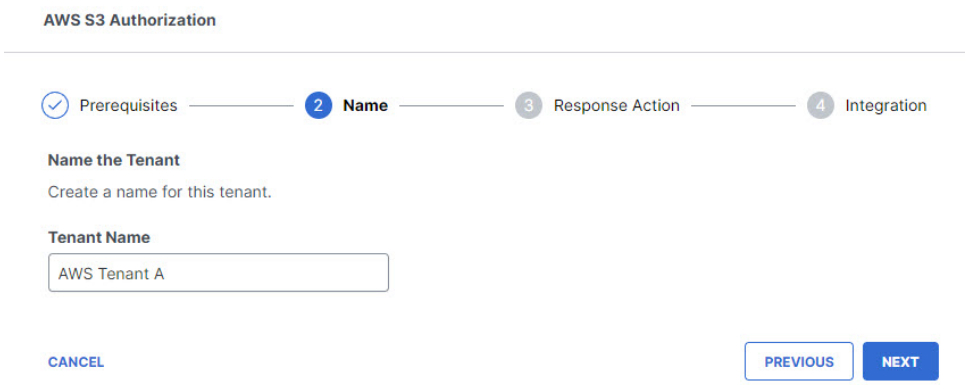


> **Note**
>
> If you enable both Cloud Malware and DLP protection for a region, a single stack can serve for both purposes. If you have already created an AWS stack for DLP protection for a region, you need not create another for Cloud Malware.

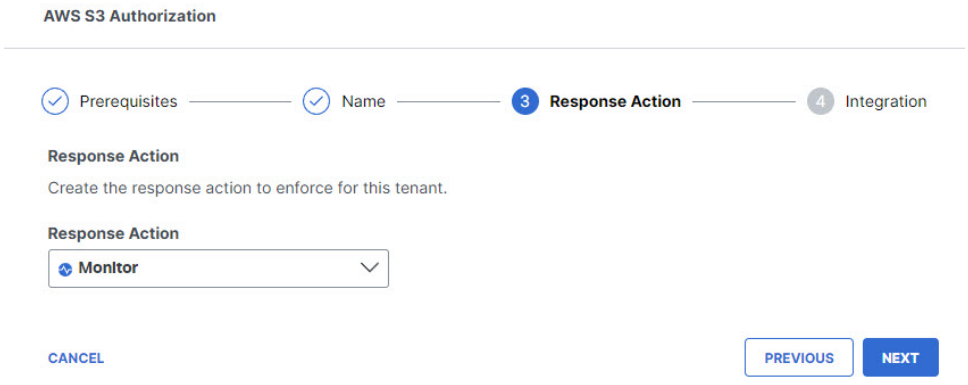
5. In the **AWS S3Authorization** dialog box, check the checkboxes to verify you meet the prerequisites, then click **Next**.



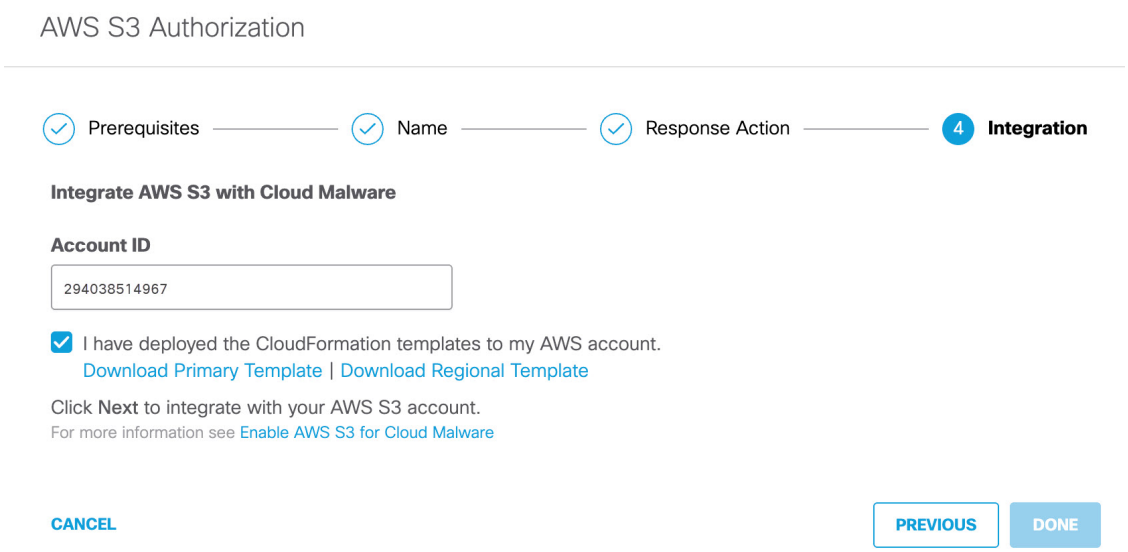
6. Provide a name for your tenant that is meaningful within your environment, then click **Next**.



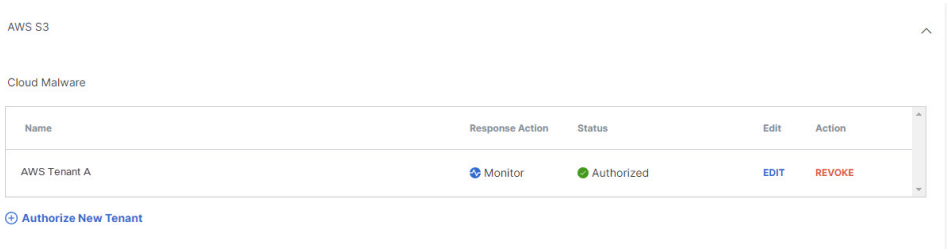
7. Choose **Monitor** for the **Response Action** for Secure Access to apply to AWS S3files found with malware, then click **Next**.



8. Paste your AWS Account ID in the text box, confirm that you have deployed template(s) to create the necessary AWS stack(s), then click **Done**. (It may take up to 24 hours for the integration to be confirmed and appear as Authorized on the Authentication page).



9. The new tenant will appear on the Authorization page in the list under **AWS S3**.



Create an AWS Stack

Provides instructions for completing the Create an AWS Stack workflow in Cisco Secure Access. Secure Access requires an AWS stack for each AWS region where you have S3 resources, to monitor and communicate with those resources.

Secure Access requires an AWS stack for each AWS region where you have S3 resources, to monitor and communicate with those resources. If you have more than one AWS tenant, you will need a stack for each region within which each tenant has resources deployed. If you enable both Cloud Malware and DLP protection for a region, a single stack can serve for both purposes.

Note

If you enable both Cloud Malware and DLP protection for an AWS region, then disable one of those two forms of protection, you must leave the stack intact to support the remaining protection.

Important

Perform this task for each region your tenant accesses, after you have downloaded CloudFormation Templates in Step 4 of Authorize an AWS Tenant. Once you have created the stack(s), return to Step 5 of that task.

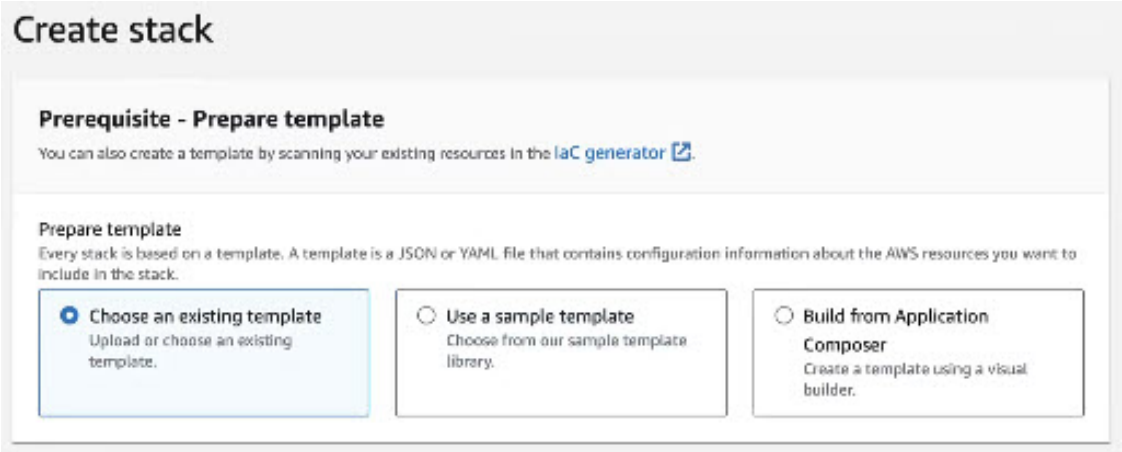
For more information about AWS Stacks, see the Amazon AWS Cloud Formation User Guide.

Procedure

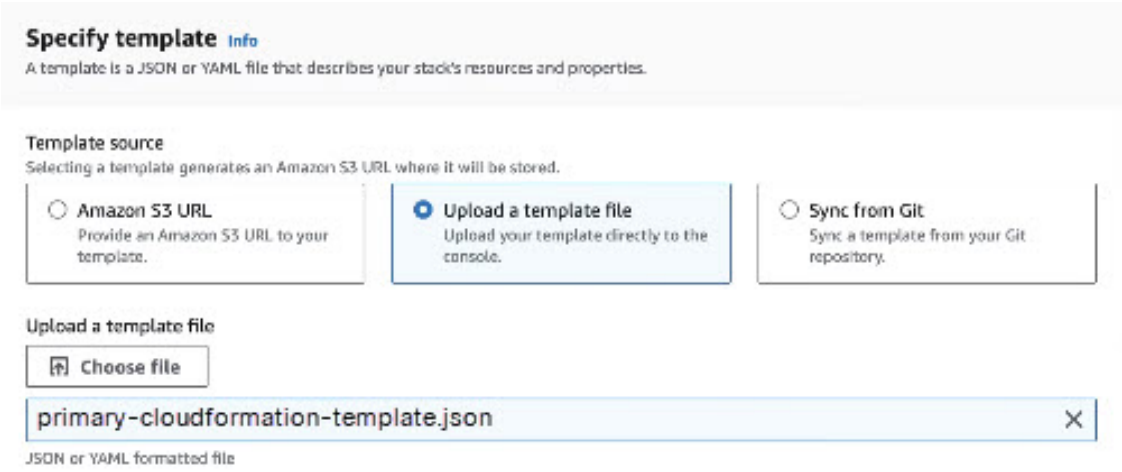
1. Log in to the AWS Management Console with an Admin account.
2. In the AWS console, navigate to **CloudFormation** > **Stacks** and choose **Create new stack** > **With new resources**.



3. On the **Create stack** page, under **Prerequisite – Prepare template**, select **Choose an existing template**.

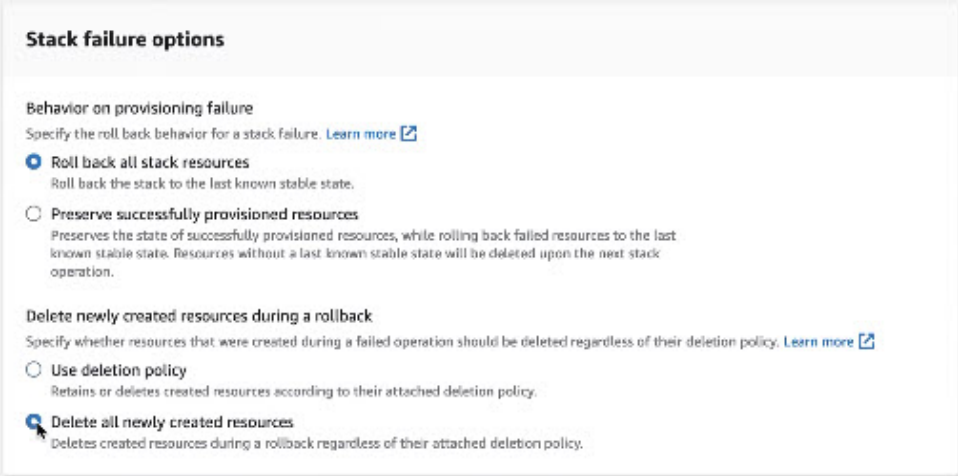


4. On the **Create stack** page, under **Specify template**, select **Upload a template file**, then click **Choose file** and navigate to and select the JSON file on your local system which you downloaded when you authorized the AWS tenant in Secure Access. (**primary-cloudformation-template.json** for your main region, or **regional-cloudformation-template.json** for any additional regions).

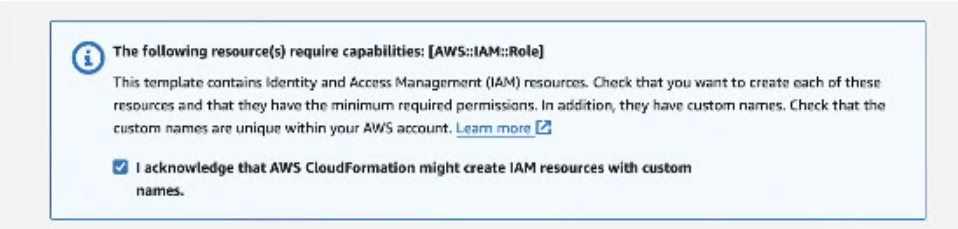


5. (Optional) Click **View in Application Composer** to open a new tab displaying a graphical representation of the stack deployment.
6. Click **Next**.
7. For the remaining options in the stack creation wizard, choose the settings appropriate to your environment. We recommend the following best practices:

- **Provide a stack name** that is meaningful within your environment.
- Under **Stack failure options**, choose **Role back stack resources** and **Delete all newly created resources**.



8. Acknowledge that AWS CloudFormation may create IAM resources with custom names within your AWS account.



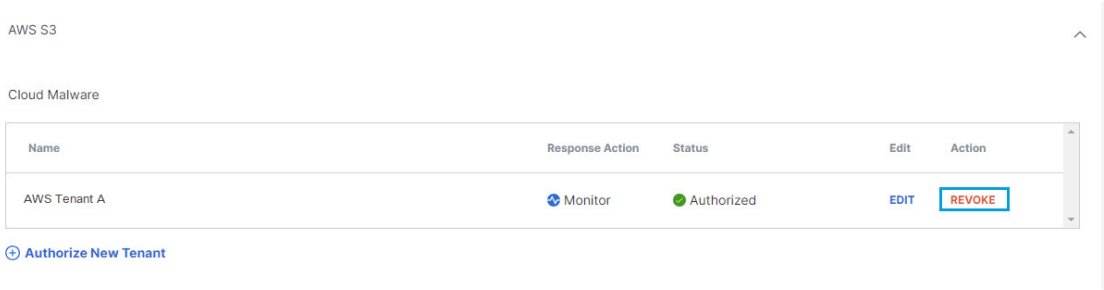
9. Click **Submit**.
10. In the AWS console the status of all stack in your account is displayed under **CloudFormation** > **Stacks**. Wait until the status for your new stack is displayed as **CREATE_COMPLETE**.
11. Continue with Step 5 of Authorize an AWS Tenant.

Revoke Authorization

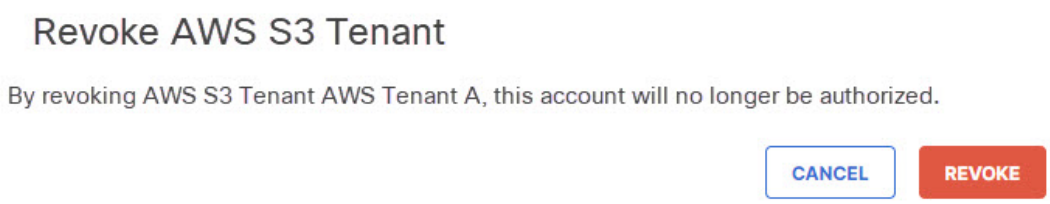
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **AWS S3**.
3. Under the **Action** column, click **Revoke**. You can revoke any authorized tenant.



4. Confirm to proceed. The selected tenant will no longer be authorized.



Consider deleting the AWS stack you created if it is not needed for other purposes.

Enable Cloud Malware Protection for Azure Tenants

Describes Enable Cloud Malware Protection for Azure Tenants in Cisco Secure Access. Secure Access supports Cloud Malware protection for files within your Azure deployment.

Secure Access supports Cloud Malware protection for files within your Azure deployment.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- You must have an active Azure account and the person doing the installation must be an Azure Global Admin.
- Chrome or Firefox is recommended with pop-up blockers/ad blockers disabled (only for the duration of authorization).

Limitation

- A tenant that fails to authenticate cannot be deleted.

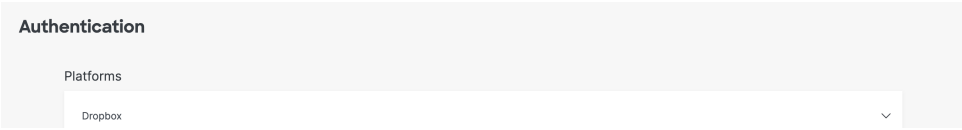
Authorize an Azure Tenant

Provides instructions for completing the Authorize an Azure Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

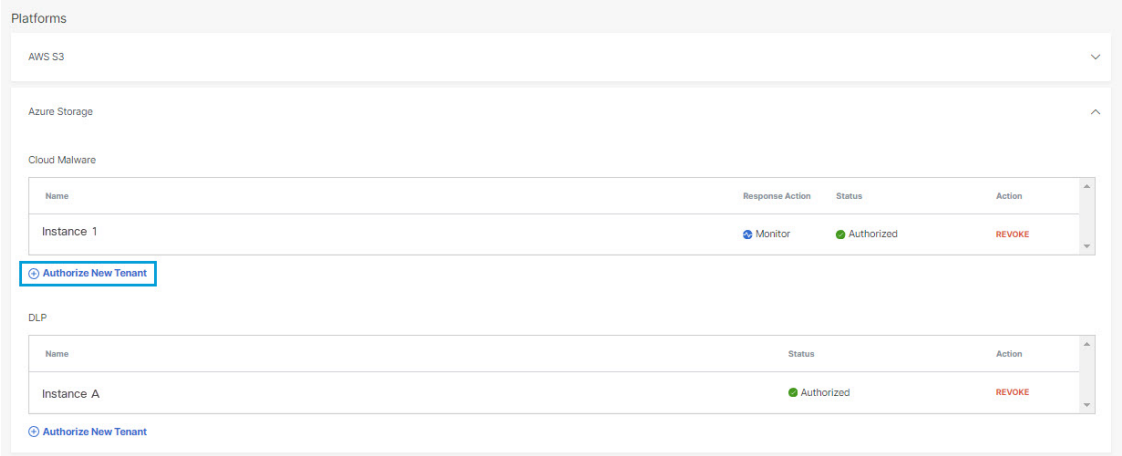
Procedure

---

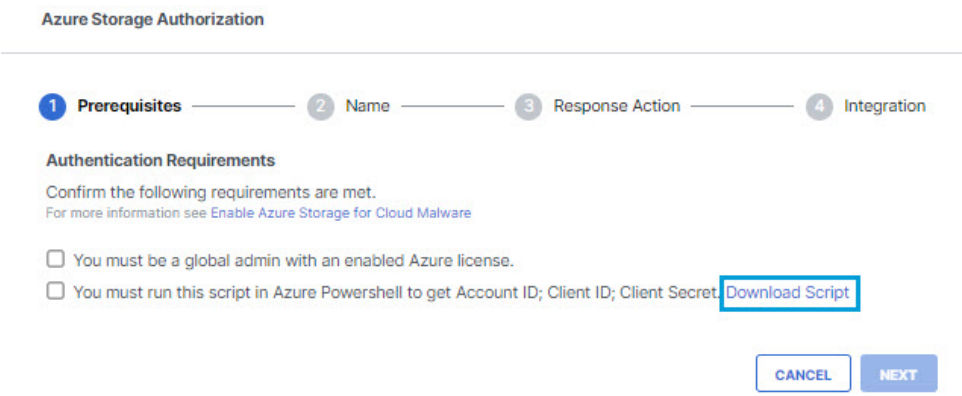
1. Navigate to **Admin** > **Authentication**.



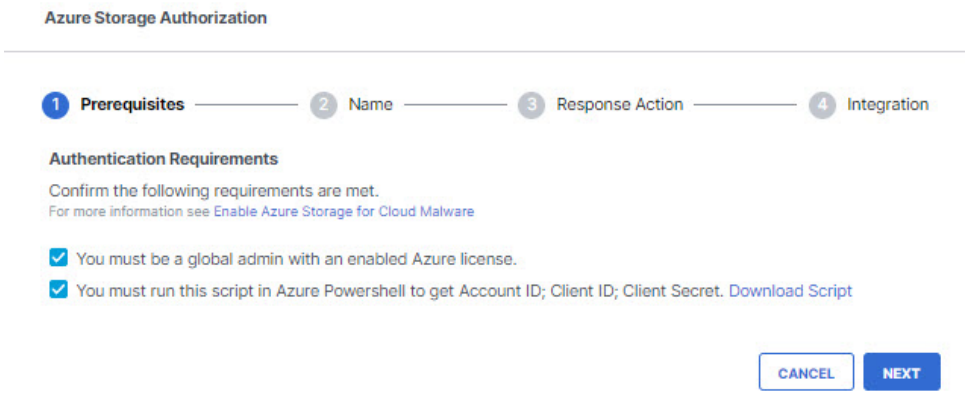
2. Under **Platforms**, click to expand **Azure Storage**.
3. Under **Cloud Malware** click **Authorize New Tenant** to add an Azure tenant to your Secure Access environment.



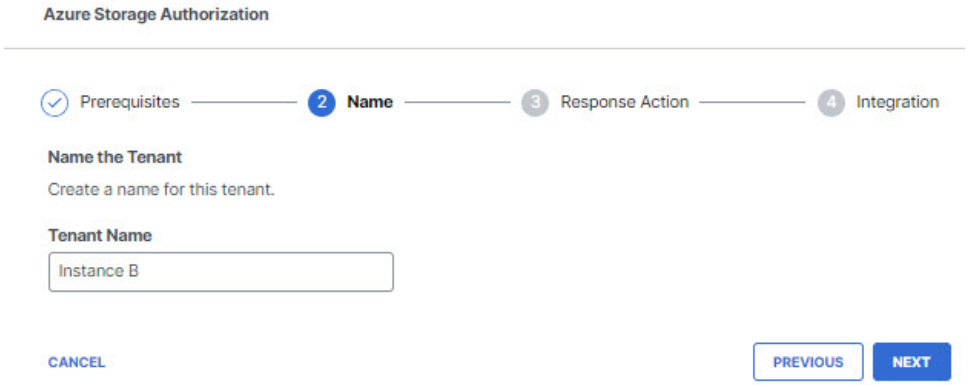
4. In the **Azure Storage Authorization** dialog box, click **Download Script** to download the AWS PowerShell script **AzureOnboarding.ps1**. Save the script to your local machine, then run the script in the Azure PowerShell before proceeding to the next step. Be sure to note the information the script will provide: **Account ID**, **Client ID**, and **Client Secret**.



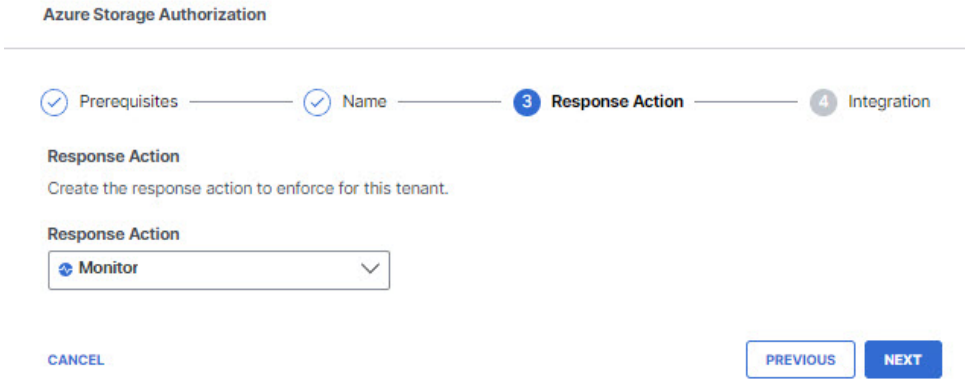
5. In the **Azure Storage Authorization** dialog box, check the checkboxes to verify you have met the prerequisites, then click **Next**.



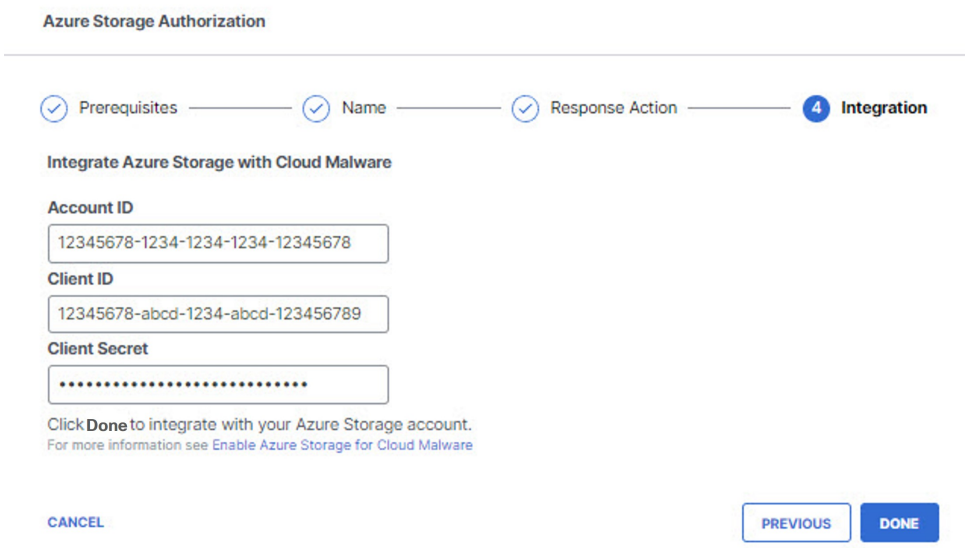
6. Provide a name for your tenant that is meaningful within your environment, then click **Next**.



7. Choose **Monitor** for the **Response Action** for Secure Access to apply to AWS S3 files found with malware, then click **Next**.



8. Paste the **Account ID**, **Client ID**, and **Client Secret** (which you obtained when you ran the PowerShell script in the Azure portal) in the appropriate boxes and Click **Done**. (It may be up to 24 hours for the integration to be confirmed and appear as **Authorized** on the Authentication page).



Run an Azure PowerShell Script to Obtain Account Information

Provides instructions for completing the Run an Azure PowerShell Script to Obtain Account Information workflow in Cisco Secure Access. In the Azure portal, open a terminal window to the PowerShell.

Procedure

1. In the Azure portal, open a terminal window to the PowerShell.
2. Upload the script you downloaded in Step 4 of Authorize a Tenant: In the Azure portal choose **Manage Files** > **Upload**, and choose the file.
3. Azure will display a message reporting **Successfully uploaded a file** and show the location and file name; note this information before dismissing the message.
4. In the terminal window, set your current directory to the location of the uploaded file.
5. To run the script, at the caret prompt (**>**) in the terminal window, enter **./AzureOnboarding.ps1**.
6. The script will prompt you to log into a web browser at https://microsoft.com/deviceLogin, and provide you with a code to authenticate. (If you get an error indicating you are already signed in, log out and log back in again.)
7. After initiating the login process, return to the terminal window.
8. The login process will present you with a numbered list of subscriptions available to you. (The subscription provides the environment where Azure will create resources needed to onboard Azure Storage for Secure Access DLP protection.) Enter the number corresponding to the subscription you want to work in, or press enter to use the default subscription, indicated with an asterisk.
9. The script will present a list of available subscriptions. Enter the name of the same subscription you chose during the login process in the previous step.
10. The script will present a list of Resource Groups available within the subscription you have chosen, and prompt you to enter the name of the Resource Group you want to use. This is where the resources needed for onboarding will reside.
11. For each Storage Account associated your subscription, the script will offer you the chance to add that Storage Account to the list of Storage Accounts with data to be scanned by Secure Access DLP. When presented with each Storage Account name, press Enter to add that account to the list, or Escape to skip that account. Azure will display messages confirming your choices. The script then proceeds to create the resources needed to support Secure Access DLP.

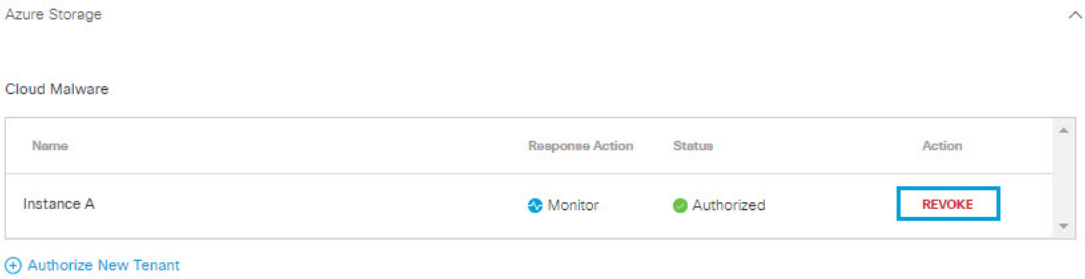
12. When the script has completed processing, it will display an **Account ID**, a **Client ID**, and **Client Secret**. Copy that information and return to Step 5 in Authorize an Azure Tenant .

Revoke Authorization

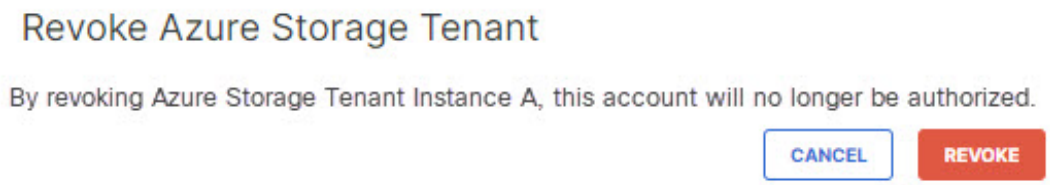
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Azure Storage**.
3. Under the **Action** column, click **Revoke**. You can revoke any authorized tenant.



4. Click **Revoke** to proceed. The selected tenant will no longer be authorized.



Enable Cloud Malware Protection for Box Tenants

Describes Enable Cloud Malware Protection for Box Tenants in Cisco Secure Access. Secure Access supports Cloud Malware protection for all files within your Box deployment.

Secure Access supports Cloud Malware protection for all files within your Box deployment.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- You must have the Box Admin role (not Co-Admin)
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Published and unpublished applications must be enabled in the Box Admin Console (see Verify Box Application Settings.

Limitations

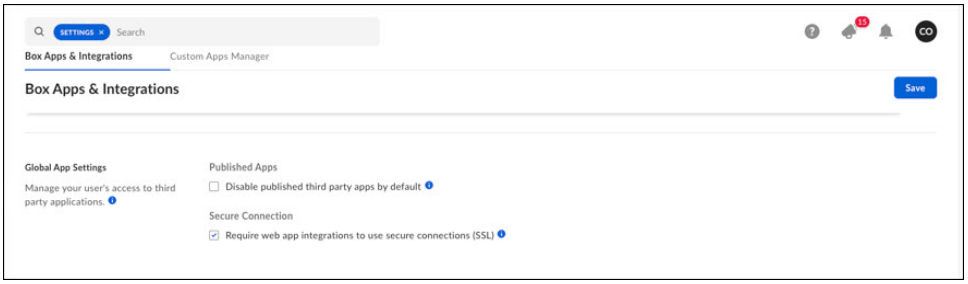
- Secure Access supports Cloud Malware protection only for Box Enterprise accounts.
- A tenant that fails to authenticate cannot be deleted.
- Secure Access attempts to quarantine a file will fail if actions on the file have been blocked by settings in Box Shield policies. In such a case, the block placed by Box takes precedence over Secure Access' ability to detect or remediate DLP violations or malware.

Verify Box Application Settings

Provides instructions for completing the Verify Box Application Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Log into the Box Admin Console.
2. Navigate to **Settings (the Gear icon)** > **Enterprise Settings** > **Apps** .
3. In the **Global App Settings** section:
   - Do *not* check: **Disable published third party apps by default**.
   - Check: **Require web app integrations to user secure connections (SSL)**.



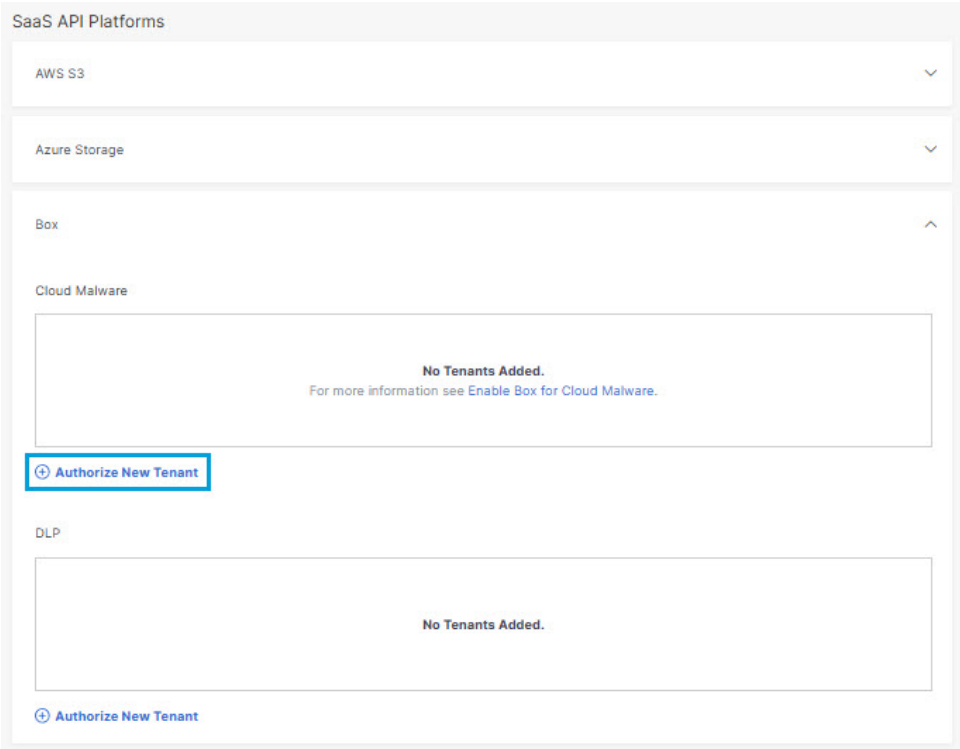
4. Click **Save**.

Authorize a Tenant

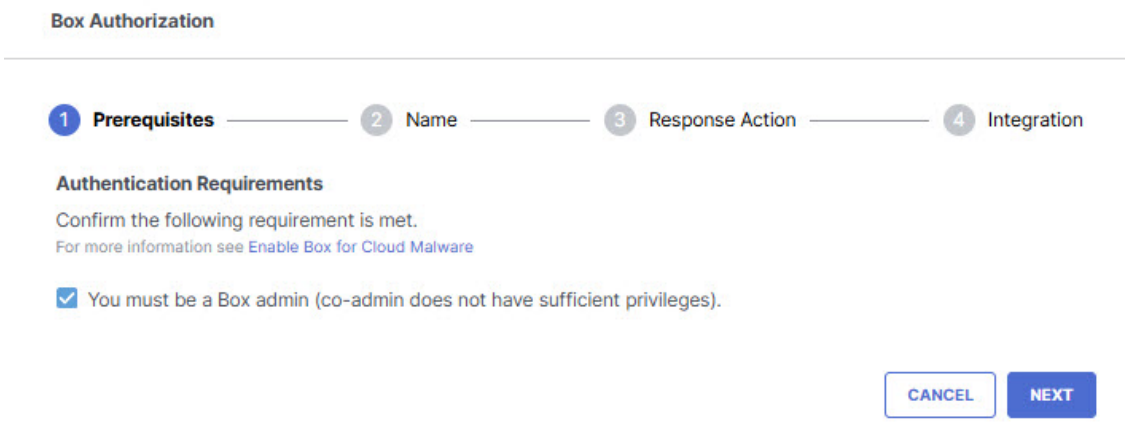
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

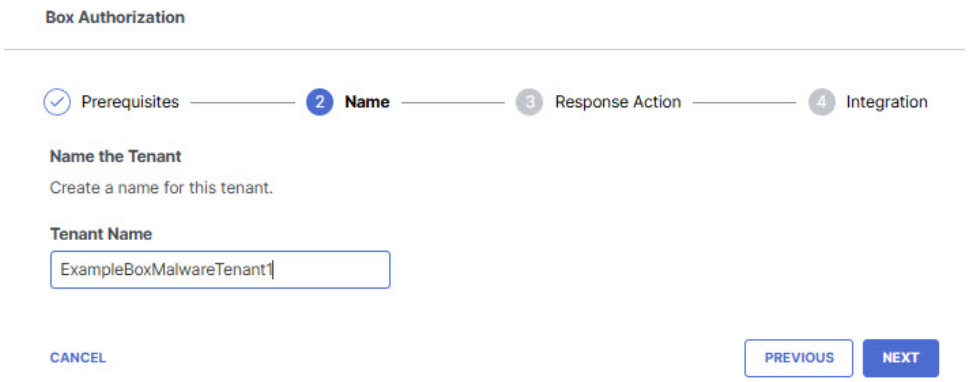
1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click to expand **Box**.



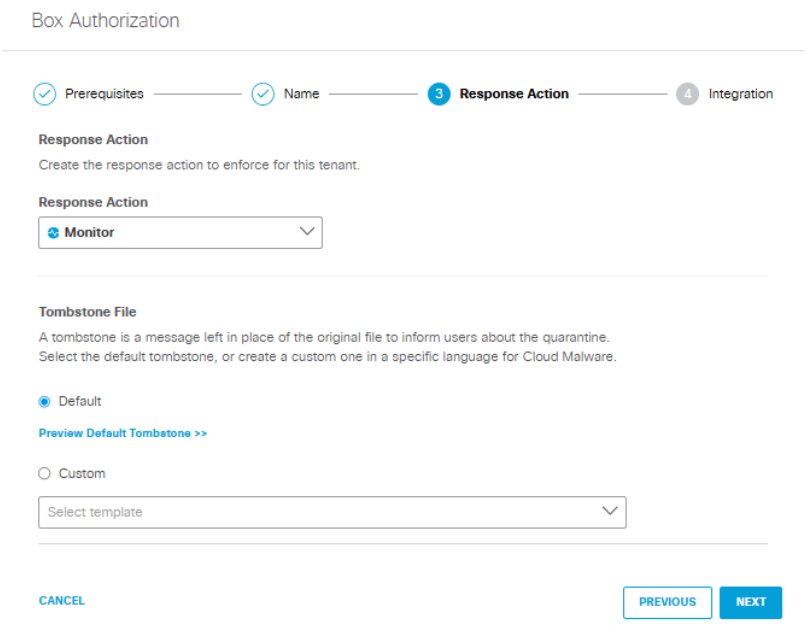
3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Box tenant to your Secure Access environment.
4. In the **Box Authorization** dialog box, check the checkbox to verify you meet the prerequisites, then click **Next**.



5. Enter the tenant name, then click **Next**.



6. Select a **Response Action** for Secure Access to apply to Box files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Box admin.
     - Replace the file in its original location with a text file named *filename*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



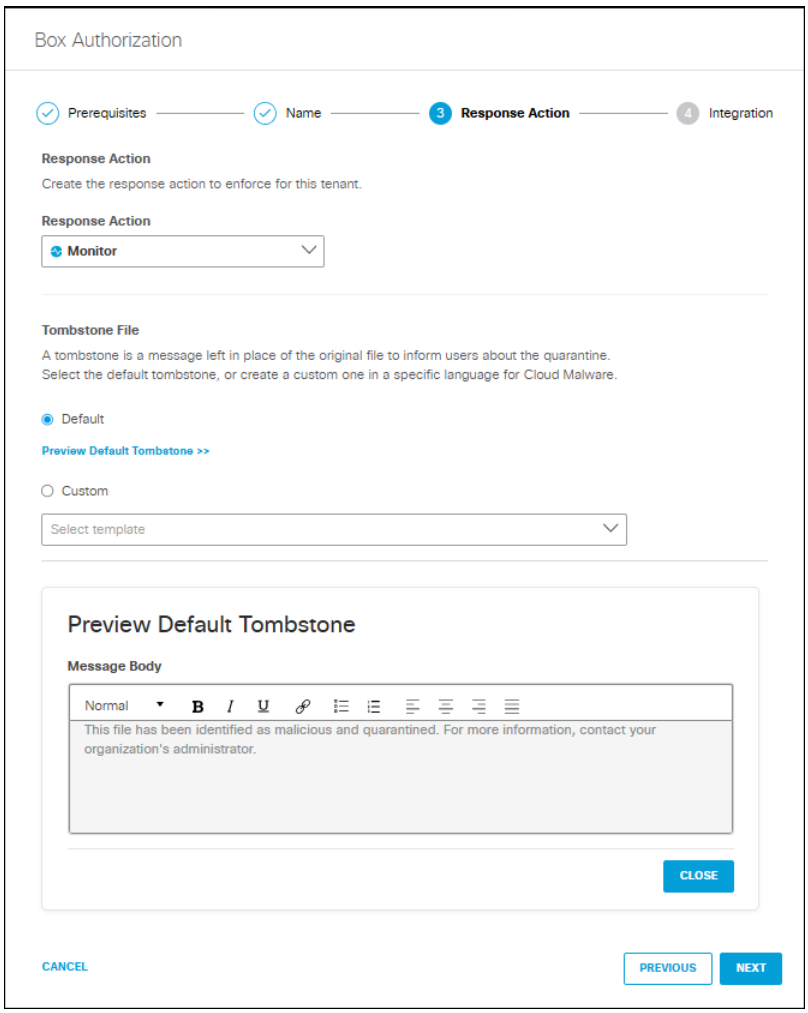
7. Define the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

b. To preview the content of tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

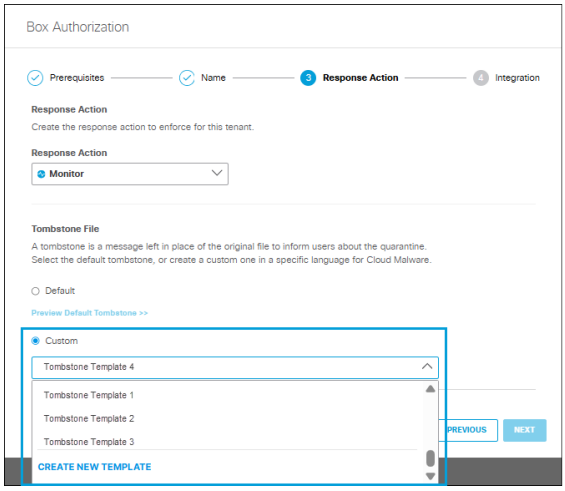


c. Click **CLOSE** to close the preview.

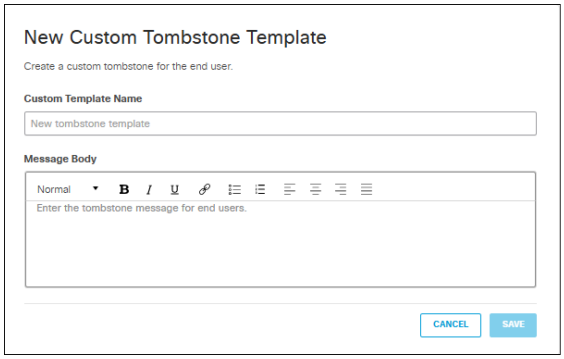
- **To Use a Custom Tombstone Template:**

a. Click **Custom**.

b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

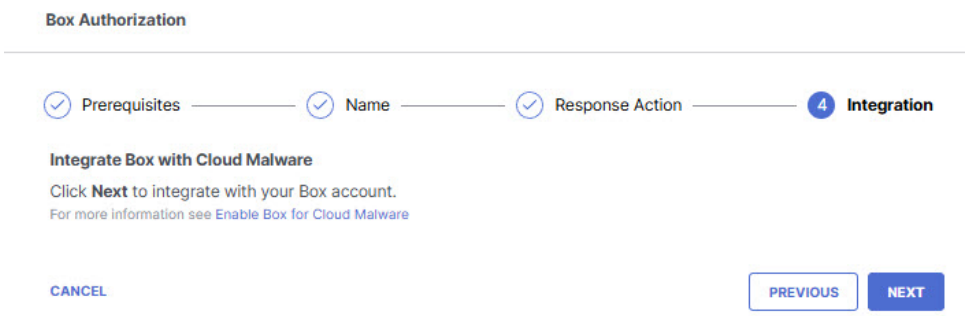
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

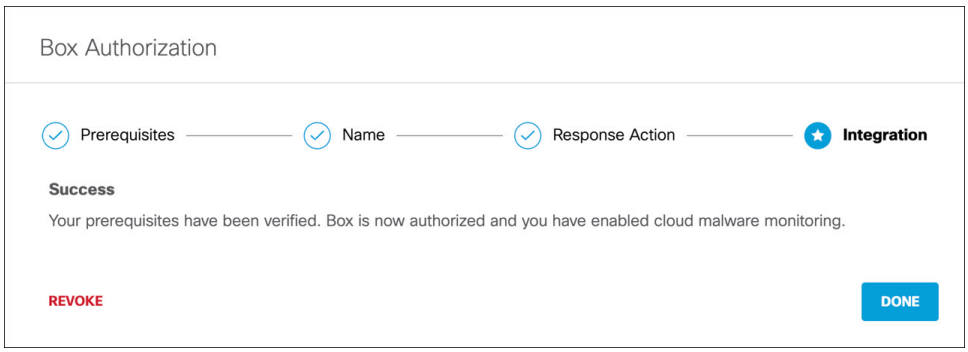
8. Click **Next** to proceed to **Integration**.
9. Click **Next** to be redirected to the Box login page.



10. Log in to Box with admin credentials to grant access.

    You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized.

11. Click **Done** to complete.



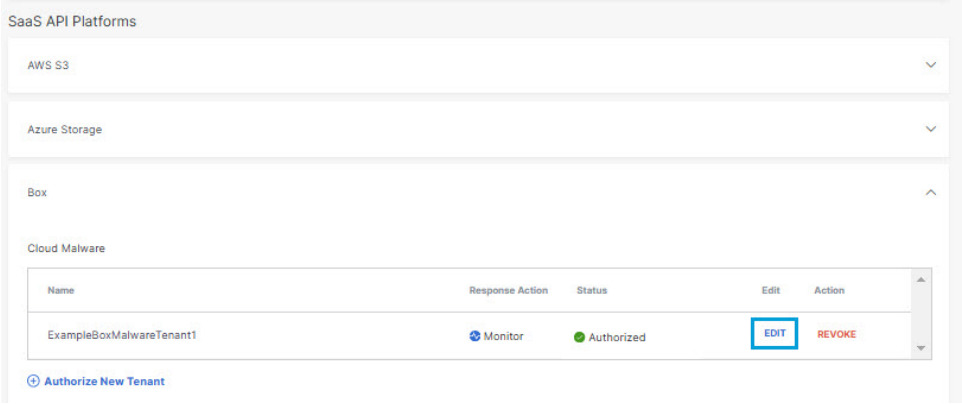
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the Response Action you have selected for a tenant.

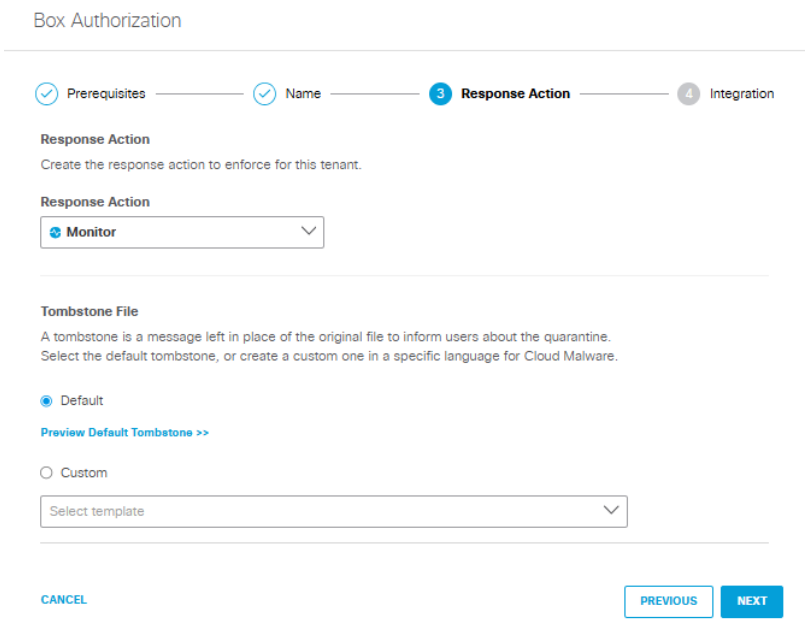
You can change the Response Action you have selected for a tenant.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **SaaS API Platforms** section, click **Box**.
3. In the **Cloud Malware** section , from the **Edit** column, click **Edit**. You can edit any tenant.



4. Select a **Response Action** for Secure Access to apply to Box files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Box admin.
     - Replace the file in its original location with a text file named *filename*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



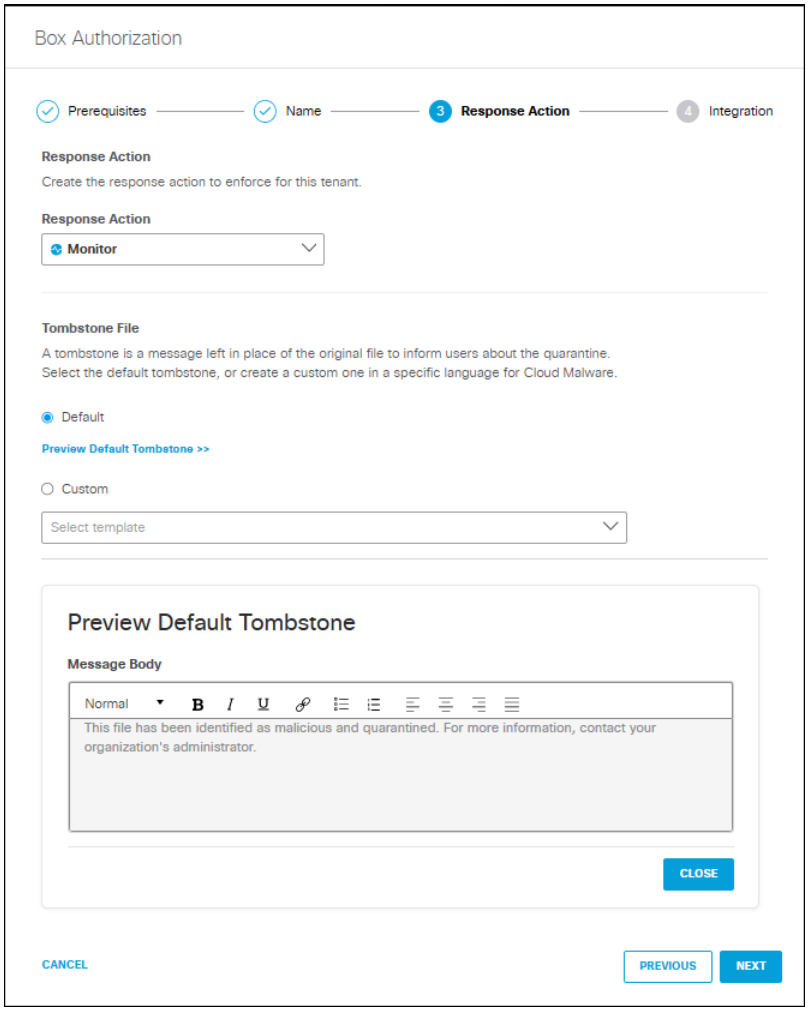
5. Change the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

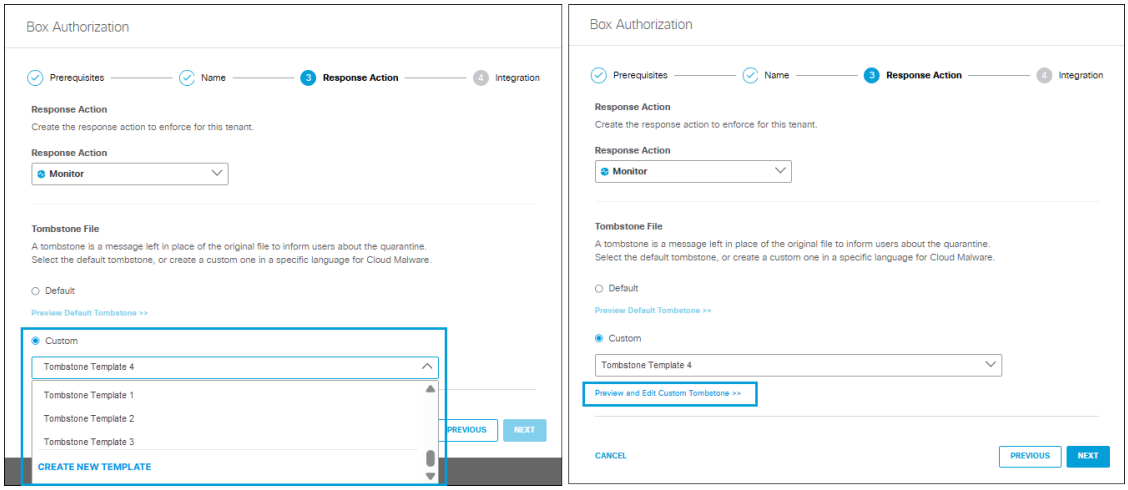


c. Click **CLOSE** to close the preview.

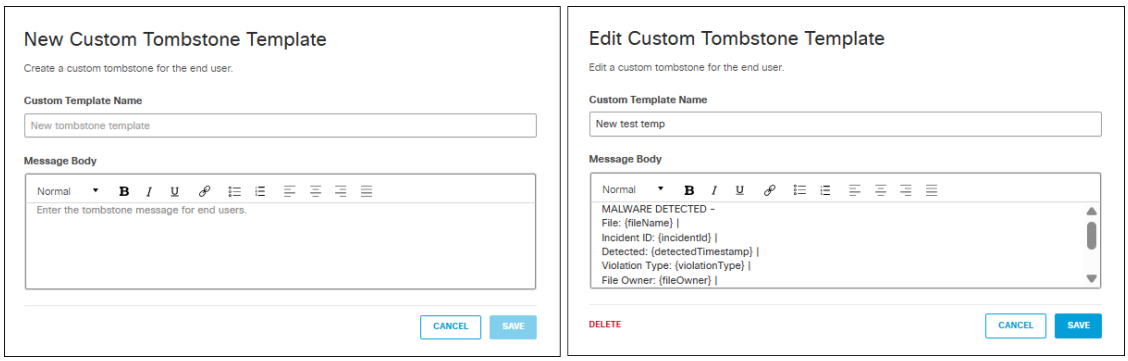
- **To Use a Custom Tombstone Template:**

  a. Click **Custom**.

  b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

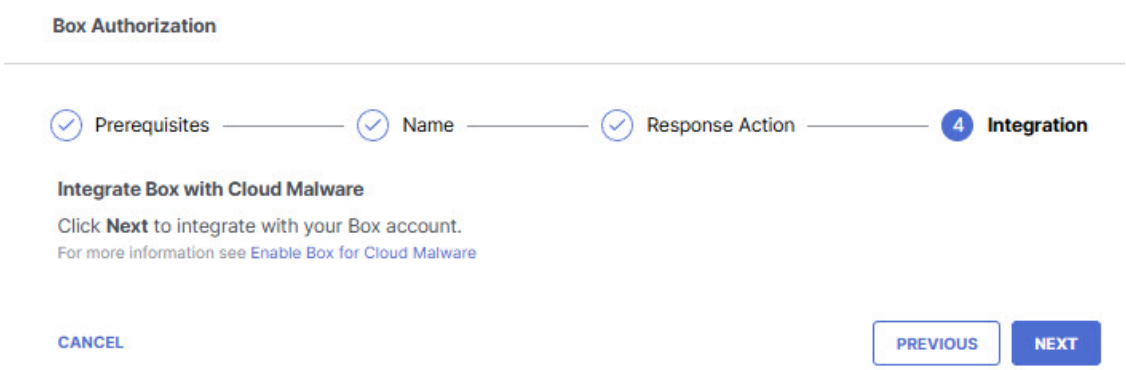
   The text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (SeeManage Data Classifications.)
   - **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileLocation}** - The file URL.

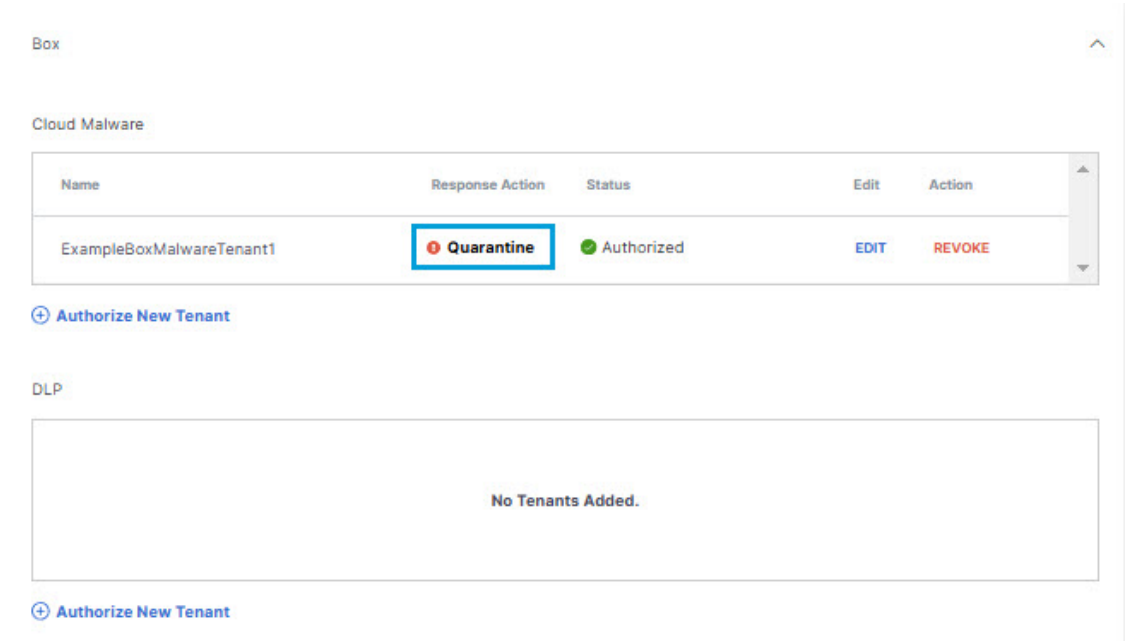
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

6. Click **Next** to proceed to **Integration**.
7. Click **Next**.



The new **Response Action** is displayed.

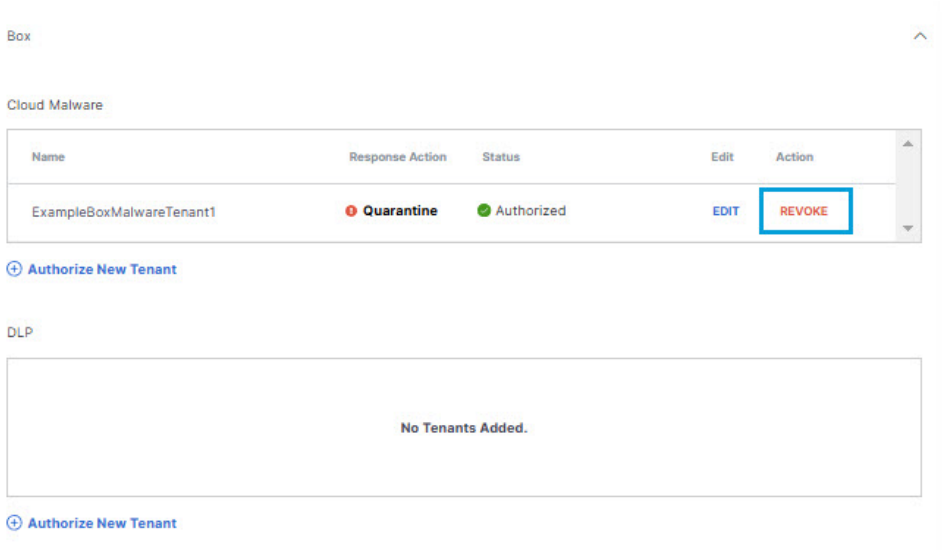


Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is no longer authorized.



Enable Cloud Malware Protection for Confluence Tenants

Provides instructions for completing the Enable Cloud Malware Protection for Confluence Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports Cloud Malware protection in Confluence Enterprise sites only for file attachments to Confluence pages. Secure access does not provide Cloud Malware protection for Confluence page contents, comments, attachments to comments, whiteboards or database tables. A tenant can access only a single Confluence site; to apply Cloud Malware protection to multiple Confluence sites, you must establish a separate tenant for each.

To enable this protection you must first authorize your Confluence tenant with Secure Access as described here.

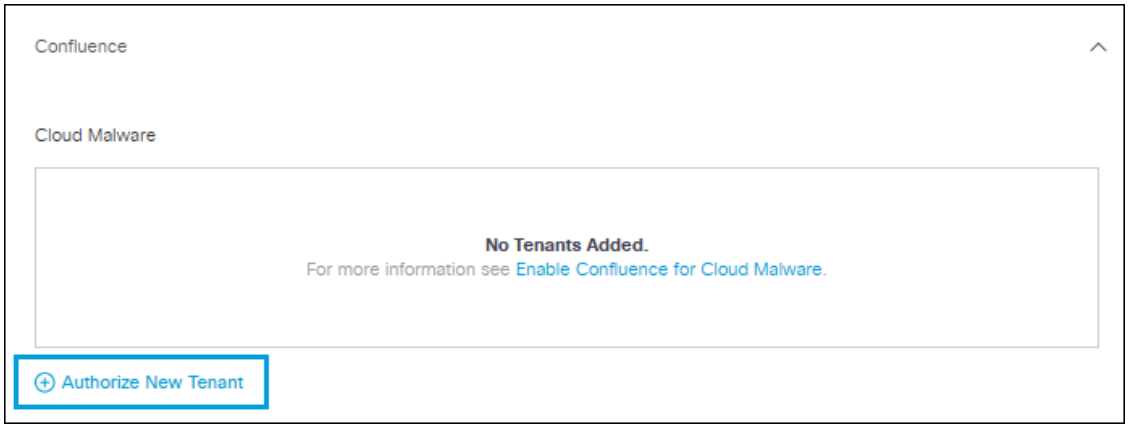
Before you begin

- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Confluence account.

Procedure

1. Navigate to **Admin > Authentication**.

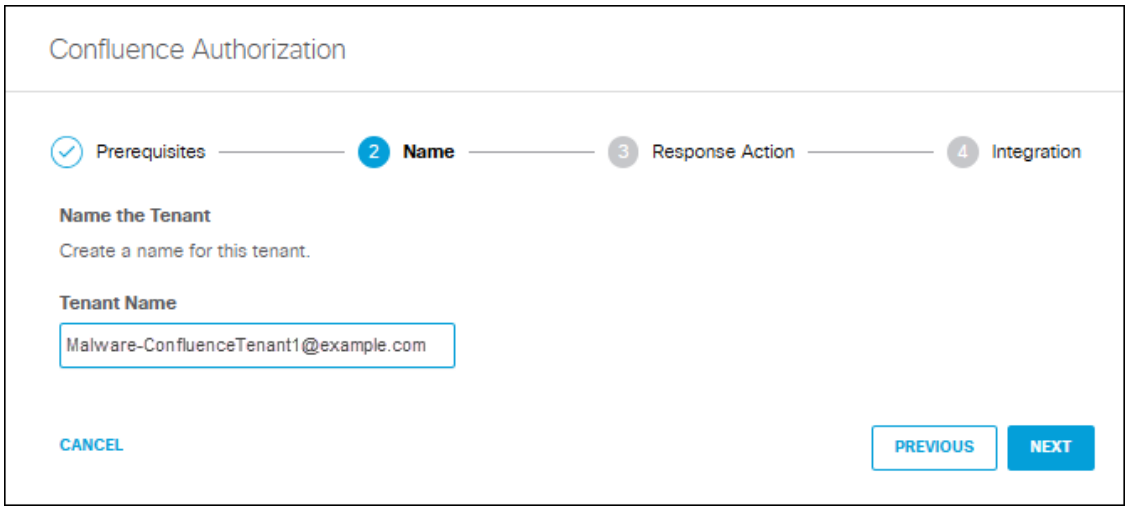
2. Under **Platforms**, click to expand **Confluence**.
3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Confluence tenant to your Secure Access environment.



4. In the **Confluence Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.



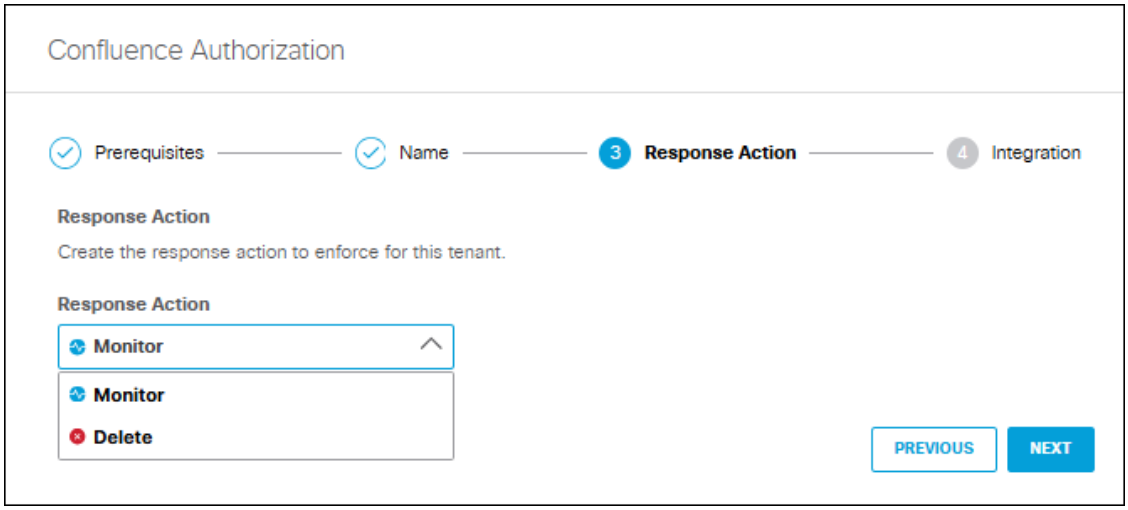
5. Enter the **Tenant Name**. Click **Next**.



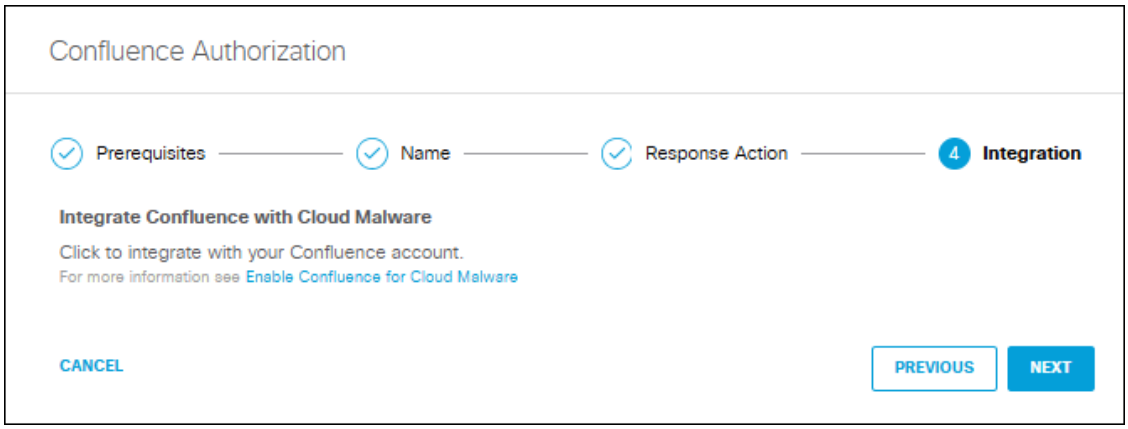
6. Select a **Response Action** for Secure Access to apply to Confluence page attachment files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log Confluence attachment files detected with malware.

- Choose **Delete** to cause Secure Access to delete attachment files detected with malware.

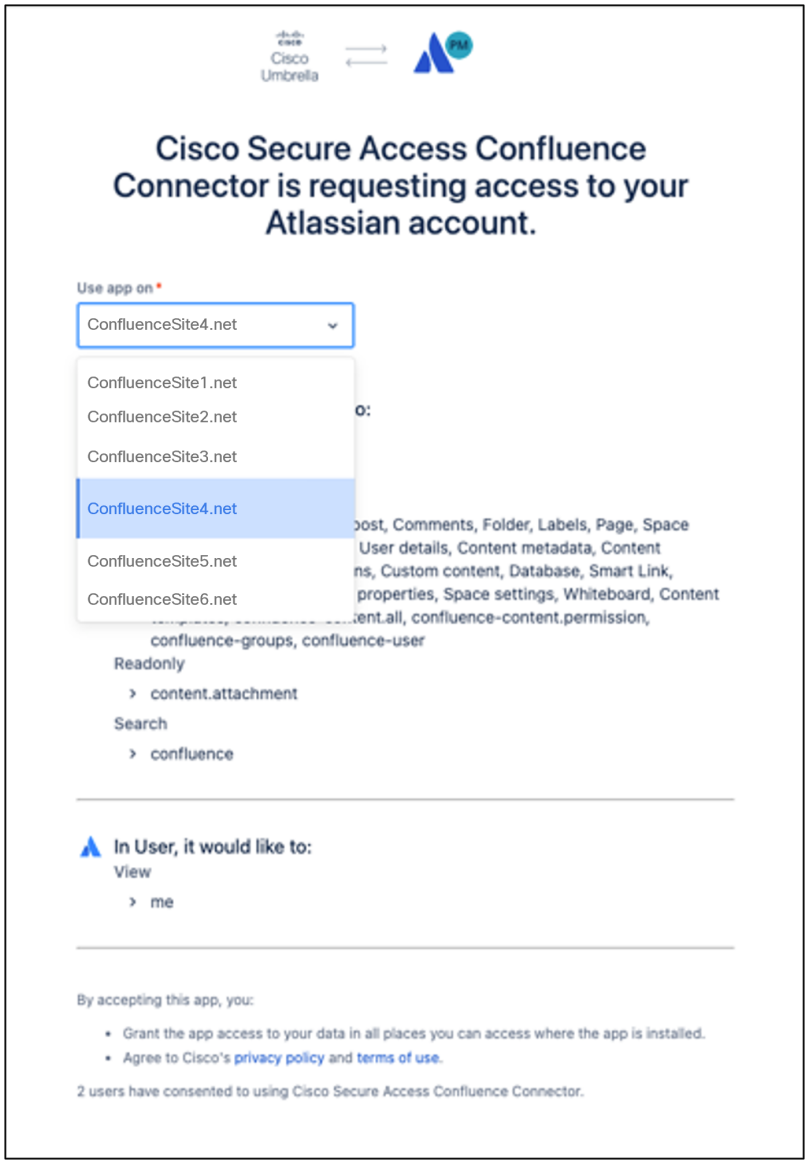
> **Note**
>
> Secure Access leaves no indication in the Confluence page of the attachment deletion.



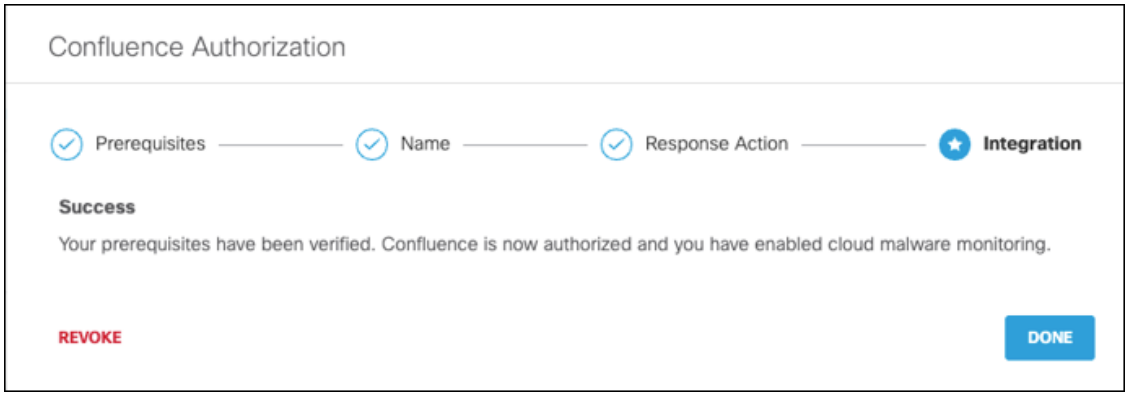
7. Click **Next** to be redirected to the Atalassian login page.



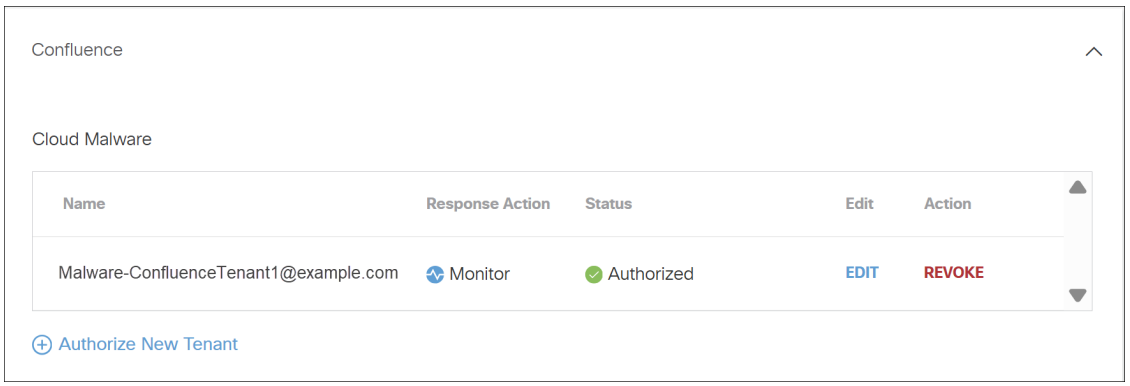
8. Log in with Confluence admin credentials. The Confluence Access Authorization page will appear.
9. From the **Use app on** drop-down, select a Confluence site for the new tenant to access . (Each tenant can access only one Confluence site.) Click **Accept**.



10. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.



11. The new tenant will appear on the Authorization page in the list under **Confluence**.



Enable Cloud Malware Protection for Dropbox Tenants

Describes Enable Cloud Malware Protection for Dropbox Tenants in Cisco Secure Access and explains Prerequisites and Limitations. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- You must have an active Dropbox tenant
- You must have the Dropbox Team Admin role
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)

Limitations

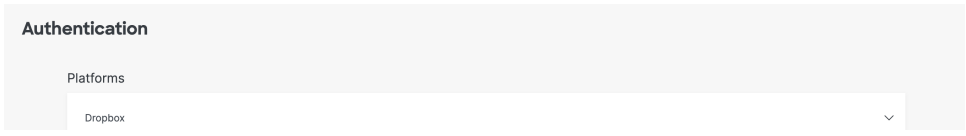
- Secure Access supports Cloud Malware protection only for Dropbox Enterprise accounts.
- Secure Access does not scan team folders on Dropbox.
- Umbrella attempts to quarantine a file will fail if that file has been locked by the Dropbox application. This may occur if Dropbox has detected malware in the file. In such a case, the lock placed by Dropbox takes precedence over Secure Access' ability to detect or remediate DLP violations or malware.

Authorize a Tenant

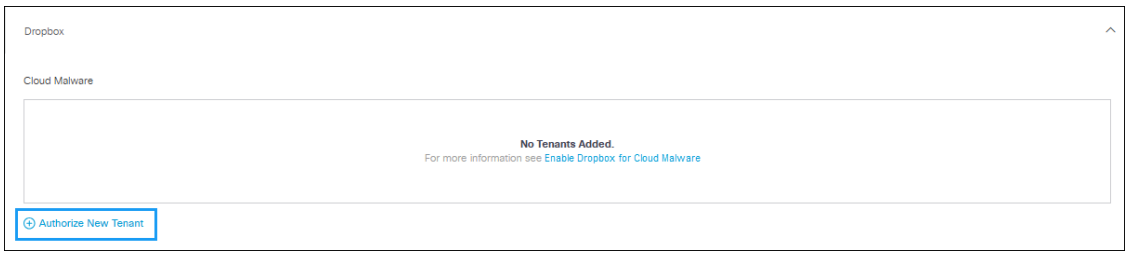
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

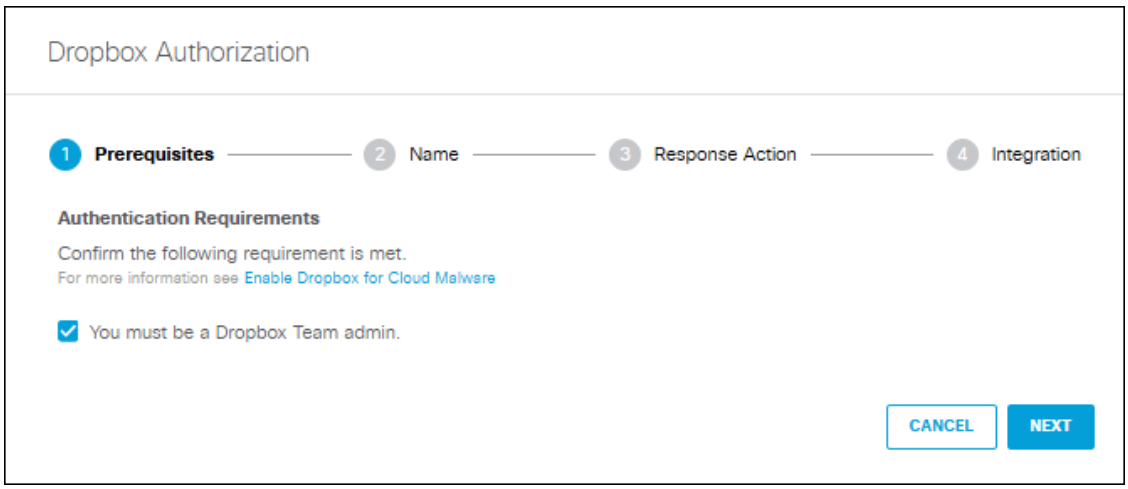
1. Navigate to **Admin** > **Authentication**.



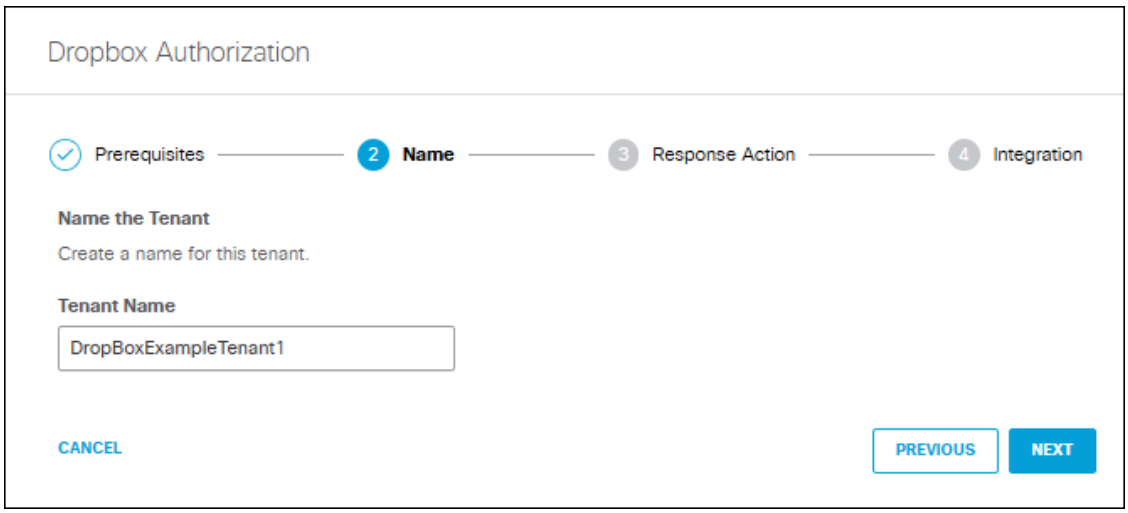
2. Under **Platforms**, click **Dropbox**.
3. Click **Authorize New Tenant** to add a Dropbox tenant to your Secure Access environment.



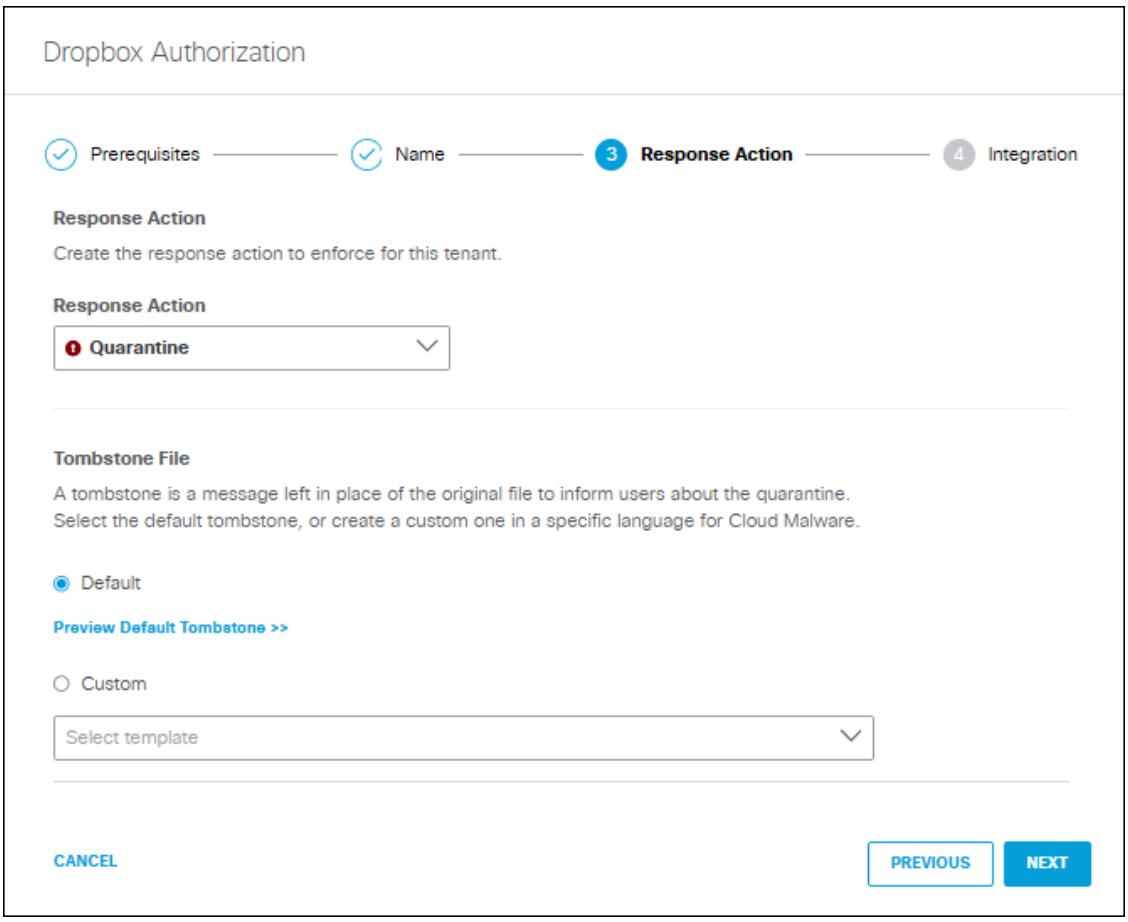
4. In the **Dropbox Authorization** dialog box, check the checkbox to verify you meet the prerequisite, then click **Next**.



5. Enter the tenant name, then click **Next**.



6. Select a **Response Action** for Secure Access to apply to Dropbox files found with malware.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Dropbox admin.
     - Replace the file in its original location with a "tombstone" text file named *filename*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



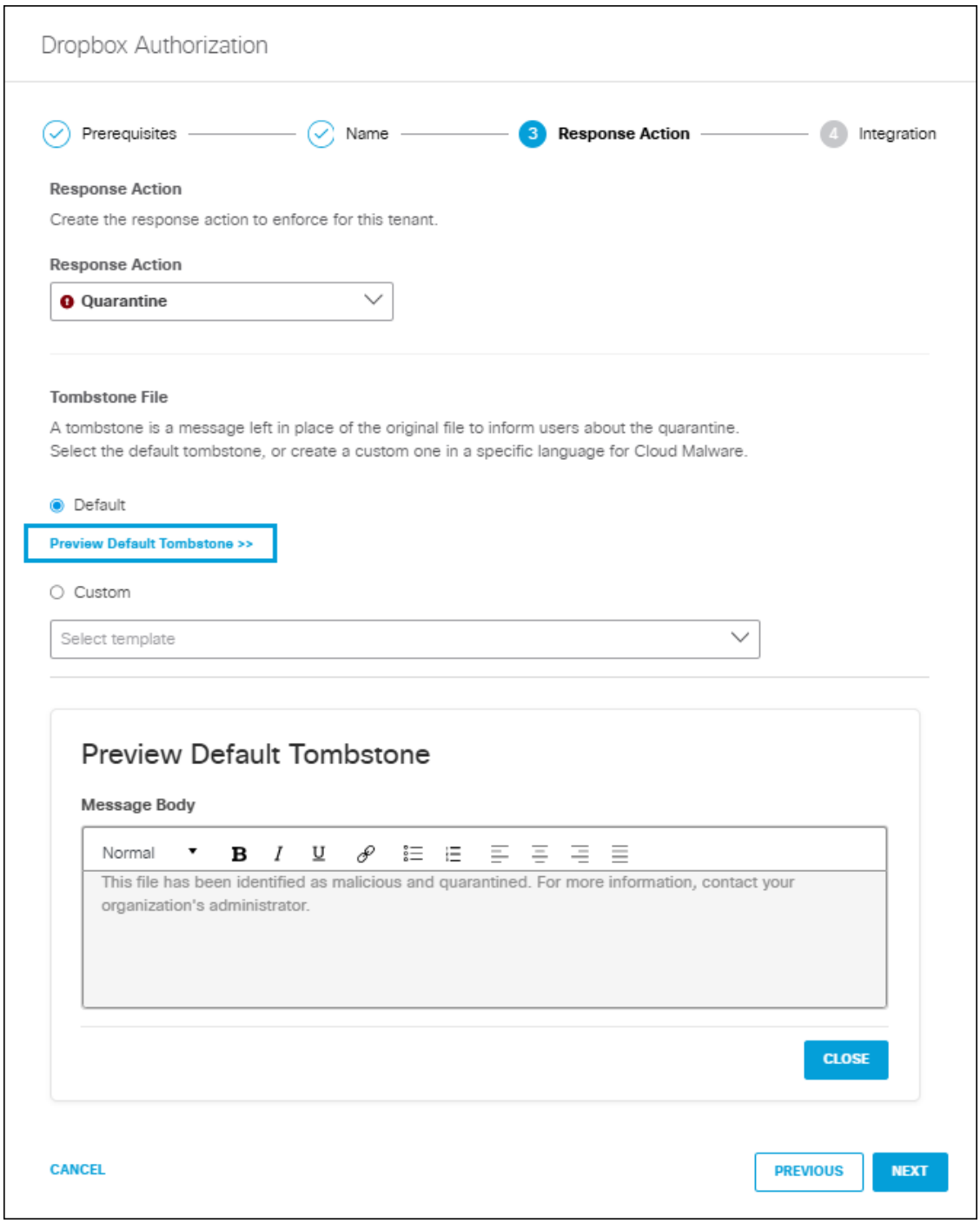
7. Define the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

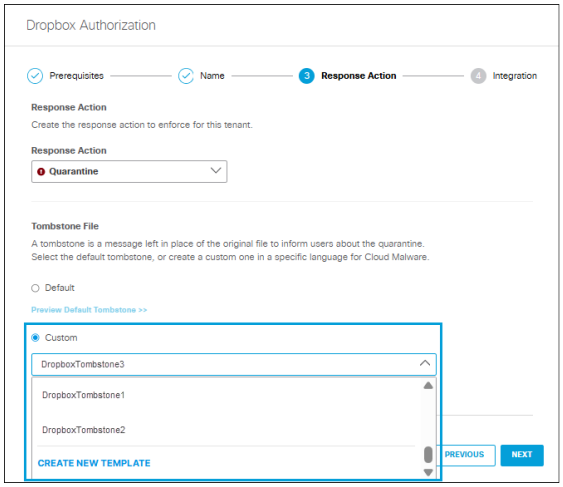


c. Click **CLOSE** to close the preview.

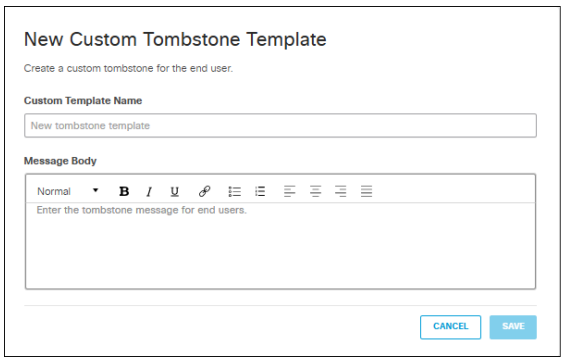
- **To Use a Custom Tombstone Template:**

  a. Click **Custom**.

  b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (SeeManage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

8. Click **Next** to be redirected to the Dropbox's login page.



9. Log in to Dropbox with admin credentials to grant access.

   You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as **Authorized**.

10. Click **Done** to complete.

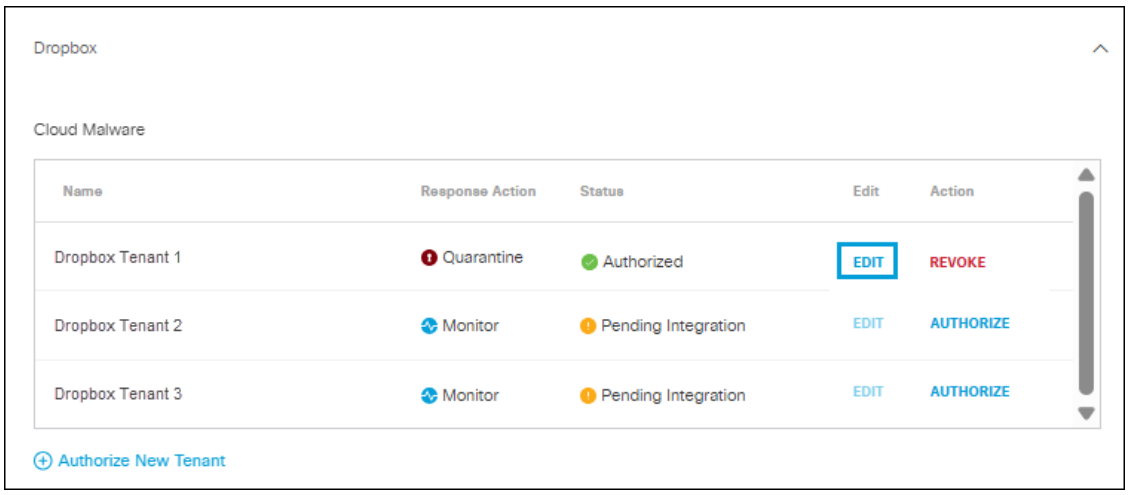
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the Response Action you have selected for a tenant.

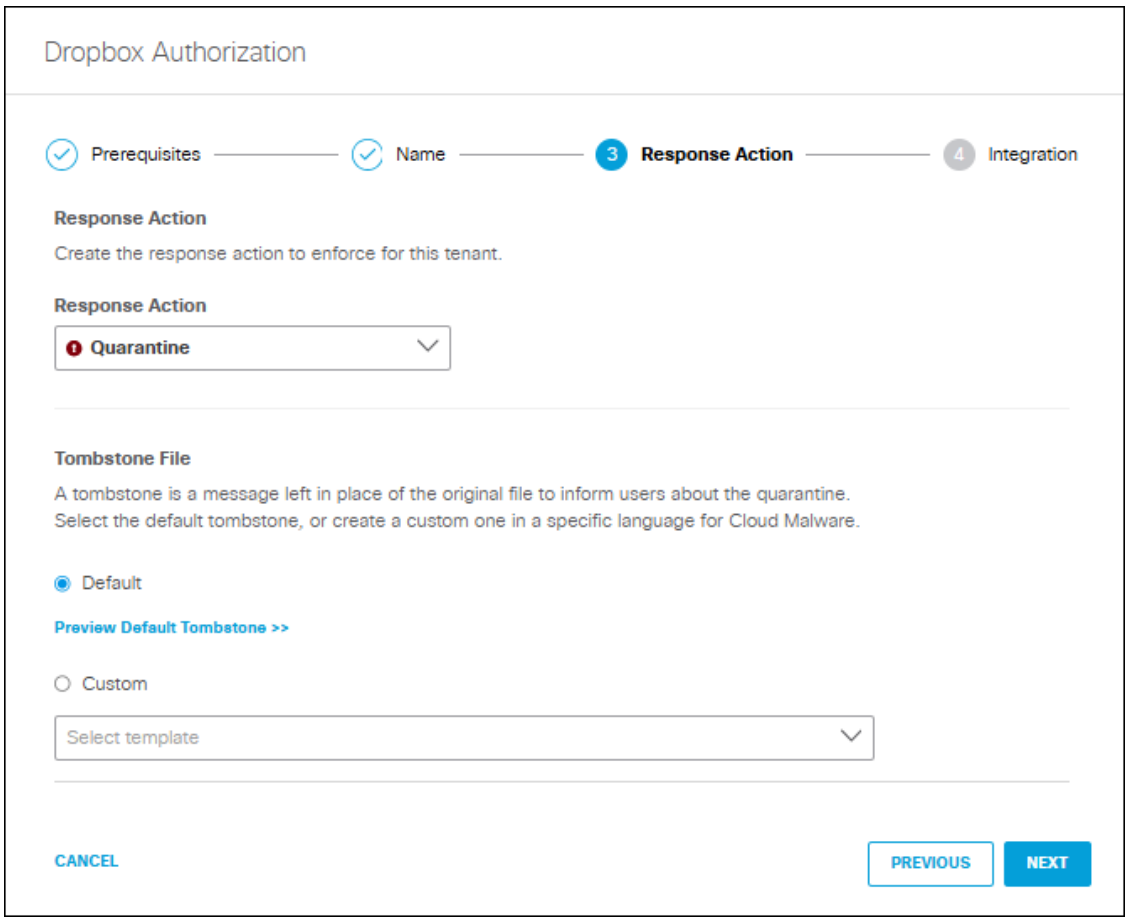
You can change the Response Action you have selected for a tenant.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **SaaS API Platforms** section, click **Dropbox**.
3. In the **Cloud Malware** section , from the **Edit** column, click **Edit**. You can edit any authorized tenant.



4. Select a **Response Action** for Secure Access to apply to Dropbox files found with malware.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Dropbox admin.
     - Replace the file in its original location with a "tombstone" text file named *filename*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



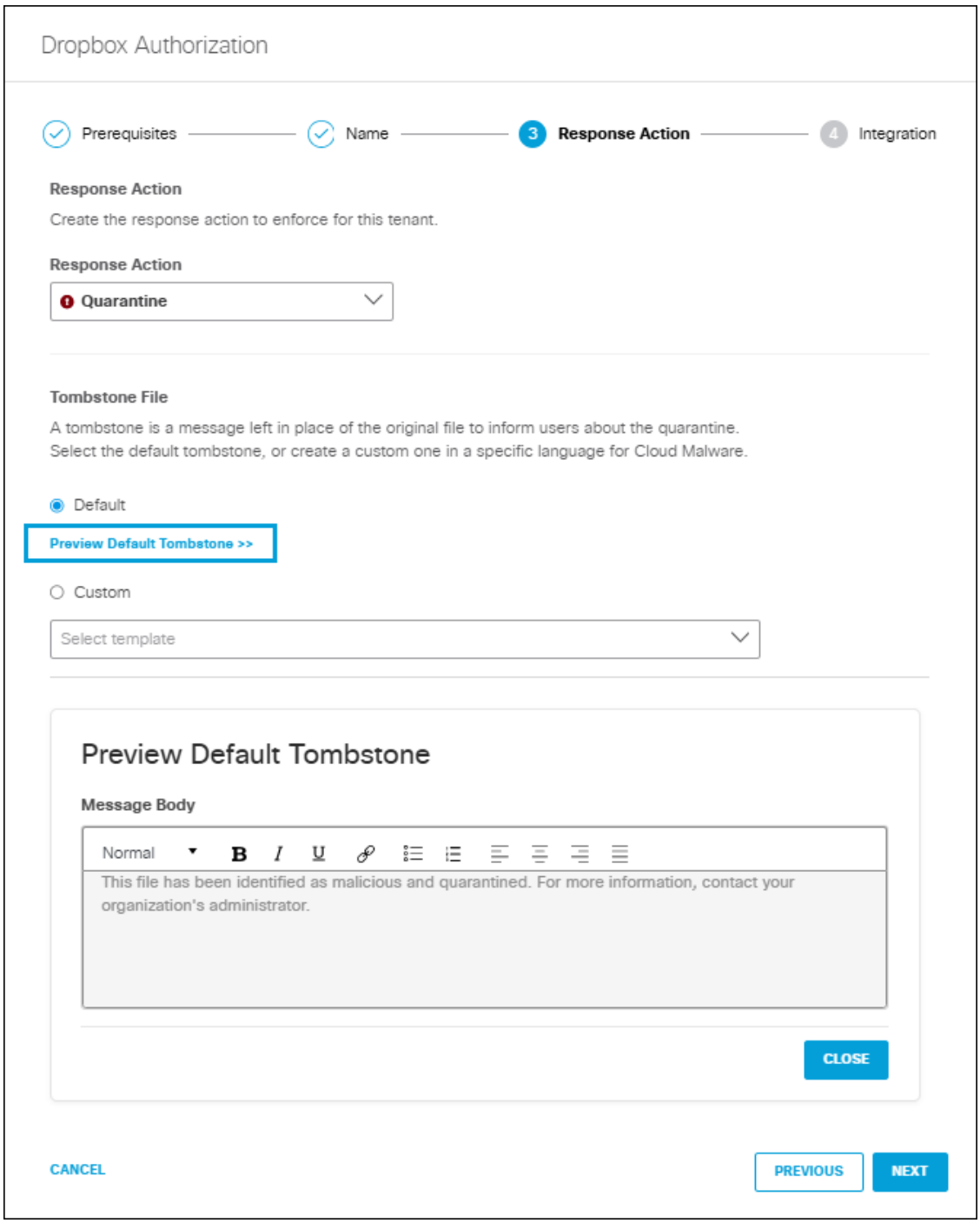
5. Define the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

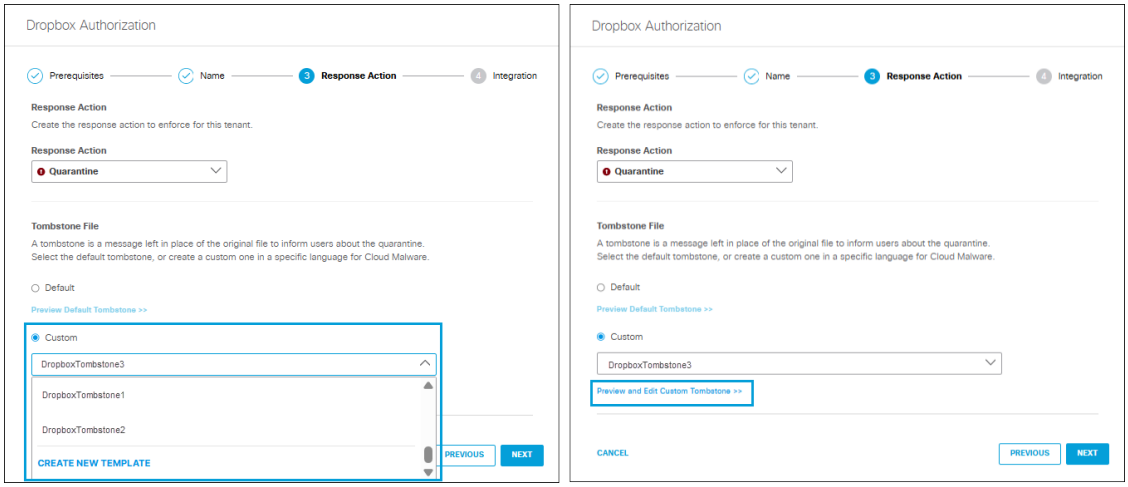


c. Click **CLOSE** to close the preview.

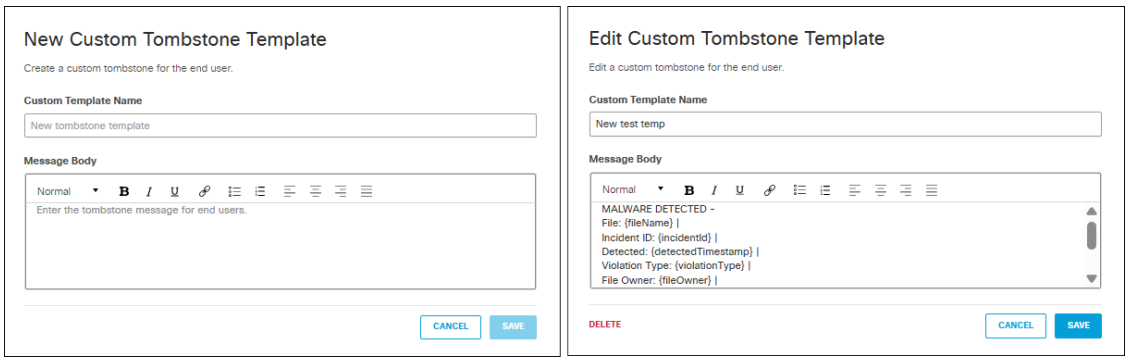
- **To Use a Custom Tombstone Template:**

  a. Click **Custom**.

  b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (SeeManage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

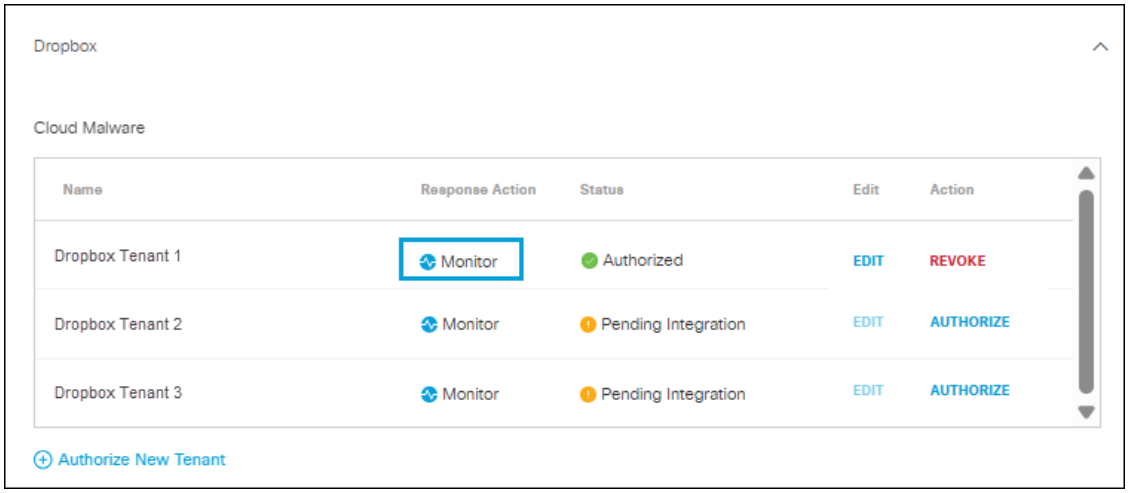
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

6. Click **Next**.



The new **Response Action** is displayed.

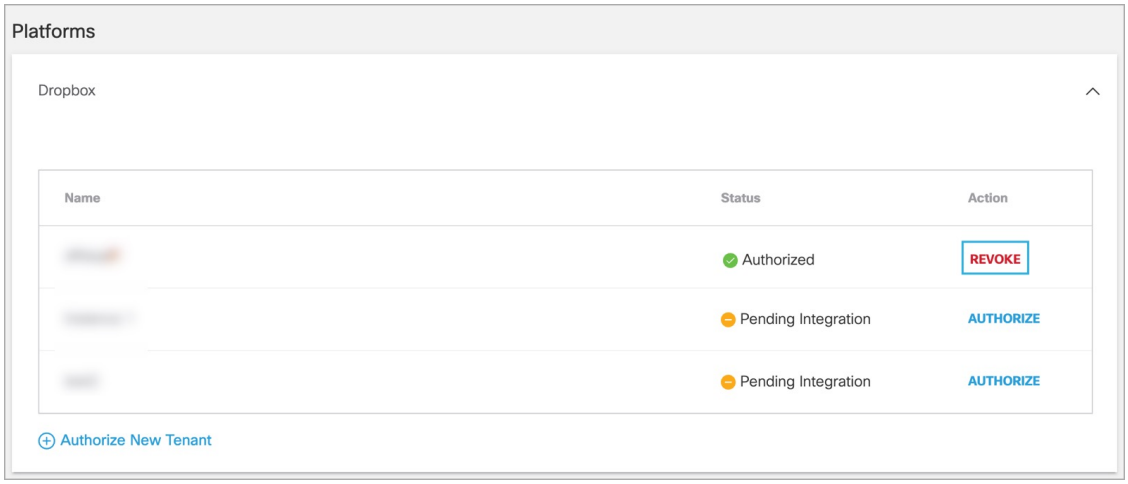


Revoke Authorization

Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.

Enable Cloud Malware Protection for GitHub Tenants

Configure cloud malware protection for GitHub to monitor repository files for security threats and ensure compliance.

Secure Access supports these Cloud Access Security Broker (CASB) features for GitHub:

- Cloud Malware protection.
- monitors repository activities for security compliance.

Prerequisites

- Full Admin user role. For more information, refer to Manage Accounts.
- The person performing the authentication *must* be a GitHub Super Admin.
- Chrome or Firefox is recommended with pop-up blockers/ad blockers disabled (only for the duration of authorization).
- Secure Access for GitHub must be installed in the tenant by a GitHub Admin User.

Supported content types

The following table outlines the content types supported for scanning and the specific scan types available.

Table 25: Security scan support for GitHub content

Content Type	Malware Scan
Repository files	Yes

Content Type	Malware Scan
Commit messages	No
Pull Request (PR) descriptions	No
PR changed files	Yes
PR reviews	No
PR review comments	No
Issues (body)	No
Issue comments	No
Commit comments	No
Release notes (body)	No
Release binary assets	No
Embedded image attachments	Yes*
Embedded file attachments	No

Limited scan support for attachments

- **Private and internal repositories**: The system cannot download file attachments in PR or in comments (such as PDFs, ZIPs, or documents) from private or internal repositories. Access to these files is gated by browser-based user sessions, which are not accessible via API.
- **Image attachment expiration**: Embedded images use time-limited links that expire approximately 5 minutes after generation. After the 5-minute duration, the image will not be scanned.

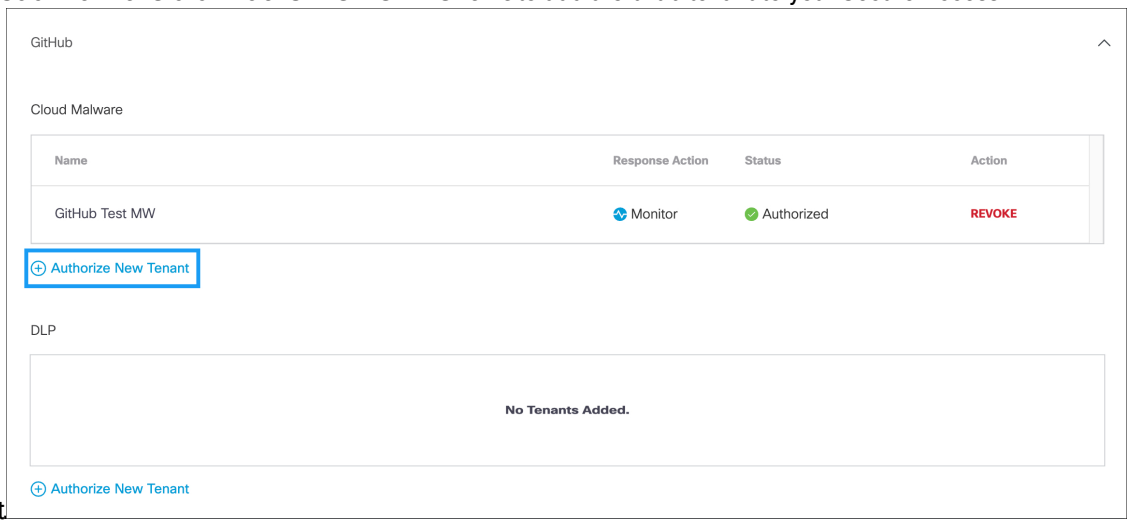
Authorize a Tenant

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click to expand **GitHub**.

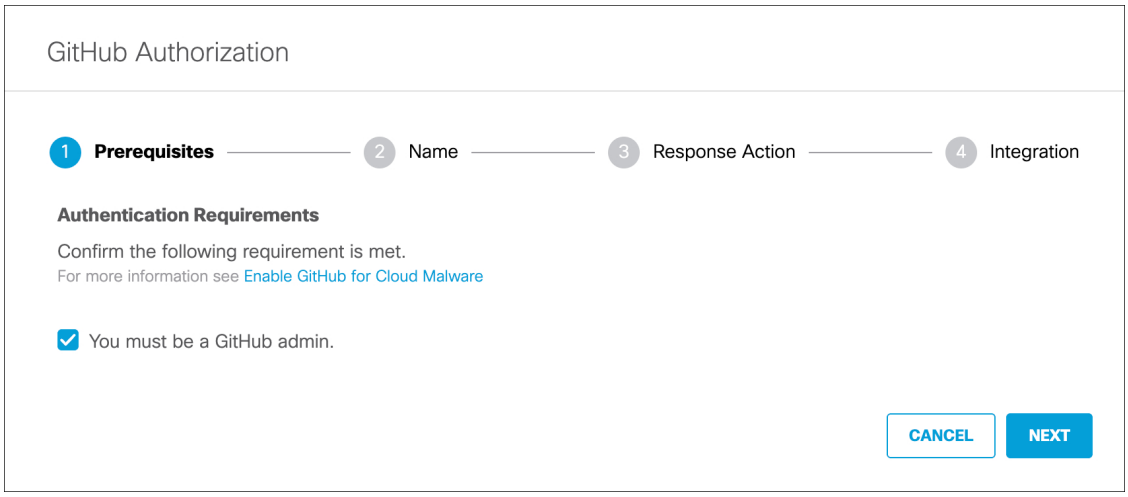


3. Under **Cloud Malware** click **Authorize New Tenant** to add a GitHub tenant to your Secure Access environment.

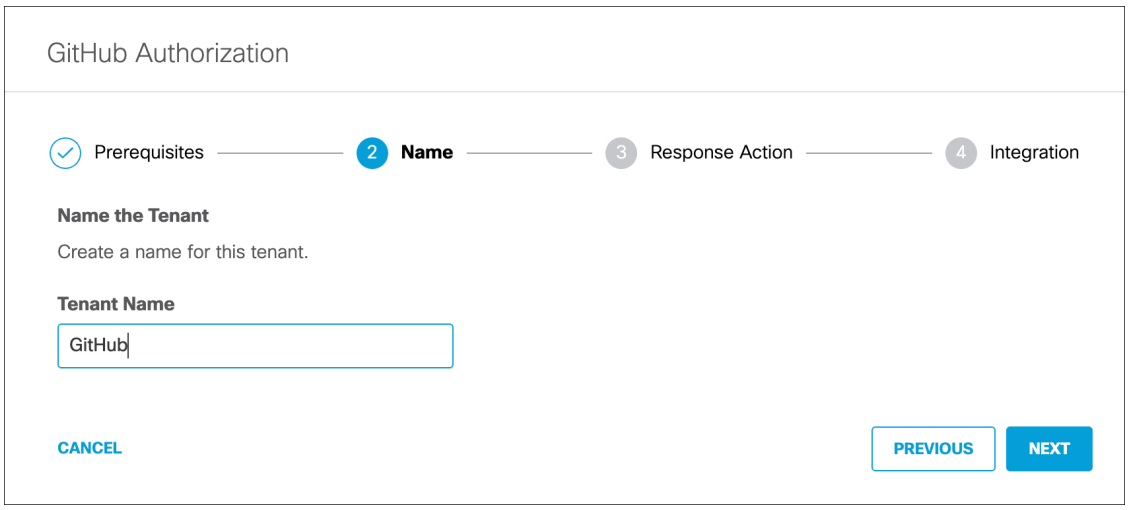


4. In the **GitHub Authorization** dialog box, check the check box to verify you meet the prerequisites, then click **Next**.

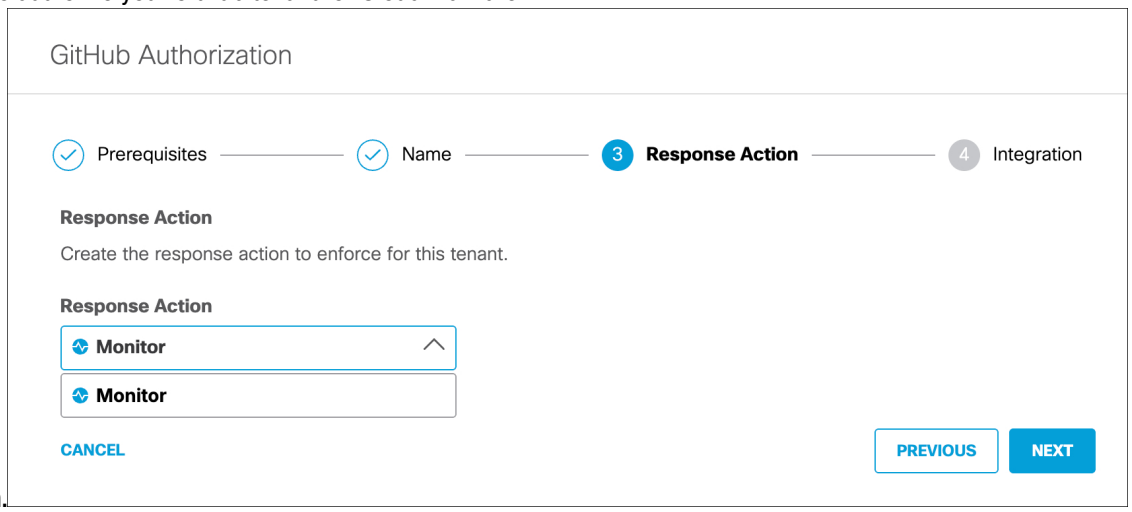
> **Note**
>
> The link to the SaaS API Connector brings you to the Umbrella DLP Connector site in the Google Workspace Marketplace. This is correct, despite the nomenclature difference.



5. Provide a name for your tenant, then click **Next**.



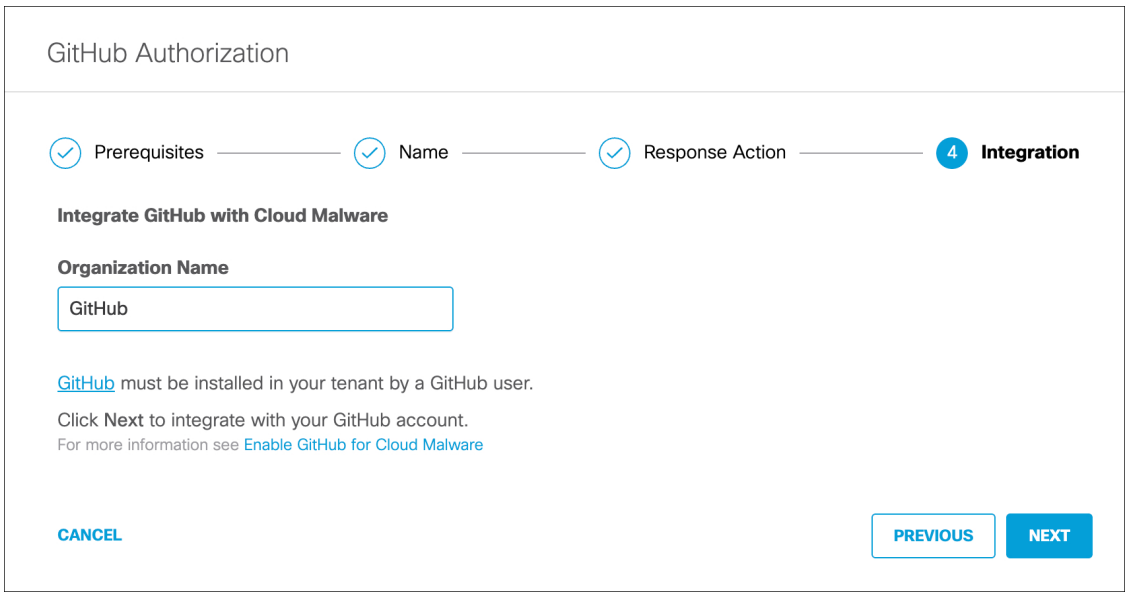
6. Choose to authorize your GitHub tenant for Cloud Malware protection.



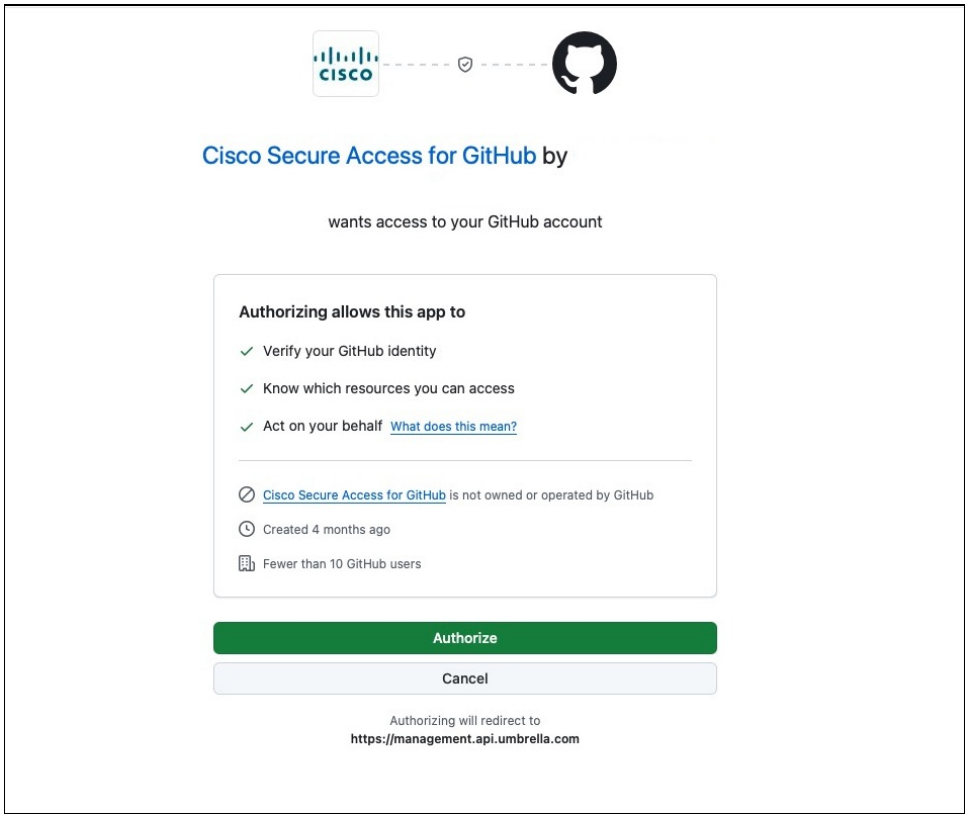
If you choose to authorize for Cloud Malware protection, you must also select a **Response Action** for Secure Access to apply to GitHub files found with malware.

- Choose **Monitor** to cause Secure Access to log files detected with malware.

7. Click **Next** to proceed to **Integration**.
8. Enter a valid **Organization Name**, click **Next**.



9. Review the permissions requested by the Cisco Secure Access for GitHub application in the GitHub authorization page.

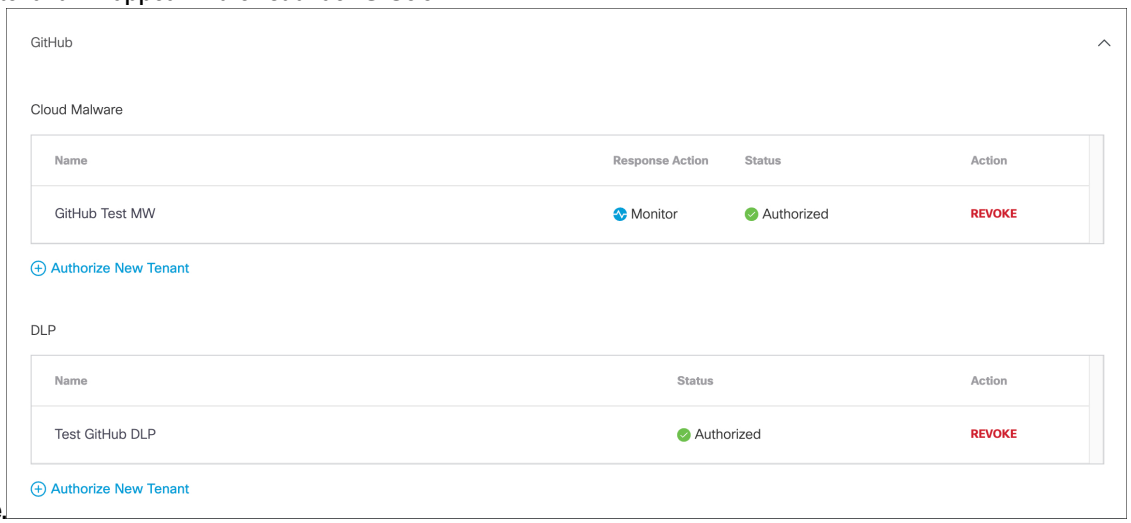


10. Click Authorize to grant the application access to your GitHub account.

    You are redirected to the Secure Access Dashboard and a message appears showing the integration was successful. It may be up to 8 hours for the integration to be confirmed and appear as **Authorized**.

11. Click **Done**.

12. The new tenant will appear in the list under **Cloud Malware**.



Revoke Authorization

Revoke an authorized tenant in GitHub to prevent further access.

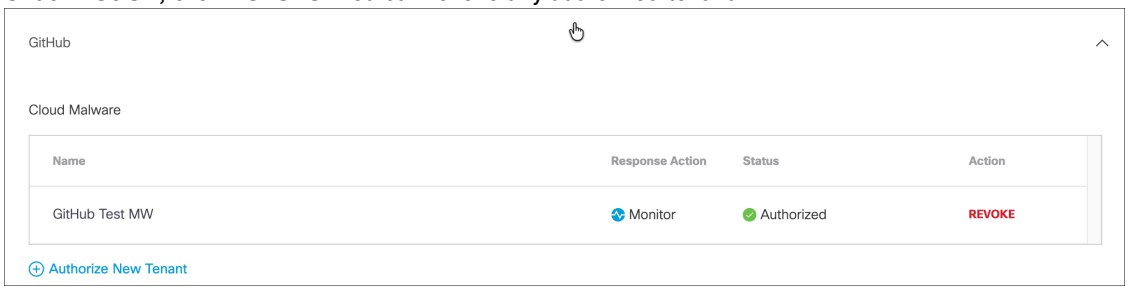
Remove access for a specific tenant, ensuring that they can no longer interact with your GitHub resources.

This task is used when you need to terminate authorization for a tenant–such as when the tenant's access should be removed due to changes in requirements or security considerations.

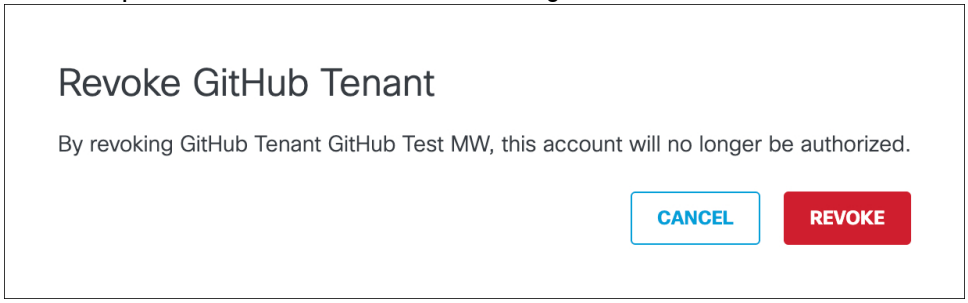
Follow these steps to revoke tenant authorization.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected tenant will no longer be authorized.



Enable Cloud Malware Protection for Jira Tenants

Provides instructions for completing the Enable Cloud Malware Protection for Jira Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports Cloud Malware protection in Jira Enterprise sites for Jira pages and comments, as well as file attachments to Jira pages and comments. A tenant can access only a single Jira site; to apply Cloud Malware protection to multiple Jira sites, you must establish a separate tenant for each.

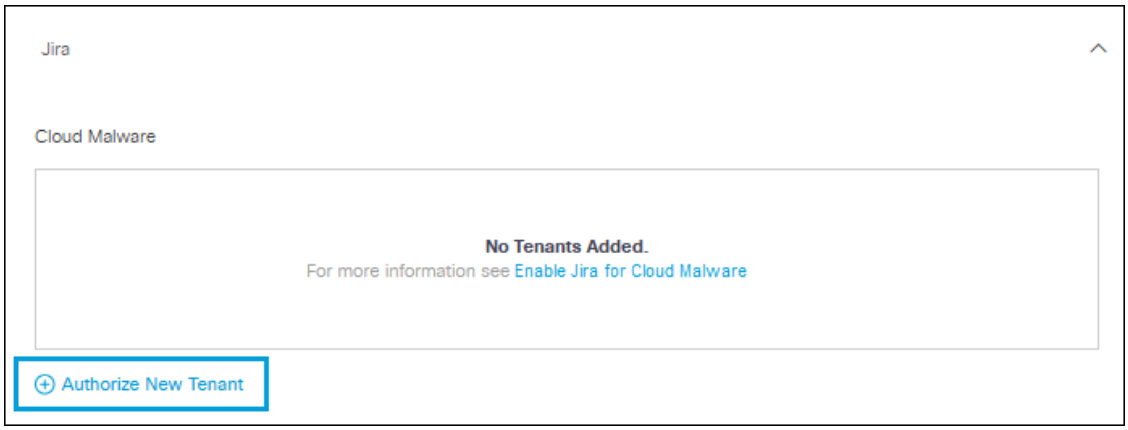
To enable this protection you must first authorize your Jira tenant with Secure Access as described here.

Before you begin

- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Jira account.

Procedure

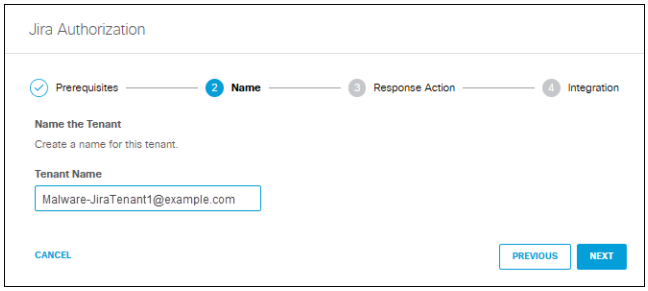
1. Navigate to **Admin > Authentication**.
2. Under **Platforms**, click to expand **Jira**.
3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Jira tenant to your Secure Access environment.



4. In the **Jira Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

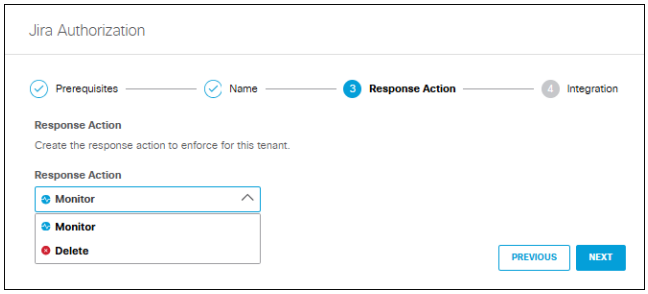


5. Enter the **Tenant Name**. Click **Next**.



6. Select a **Response Action** for Secure Access to apply to Jira attachment files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log Jira attachment files detected with malware.
   - Choose **Delete** to cause Secure Access to delete attachment files detected with malware.

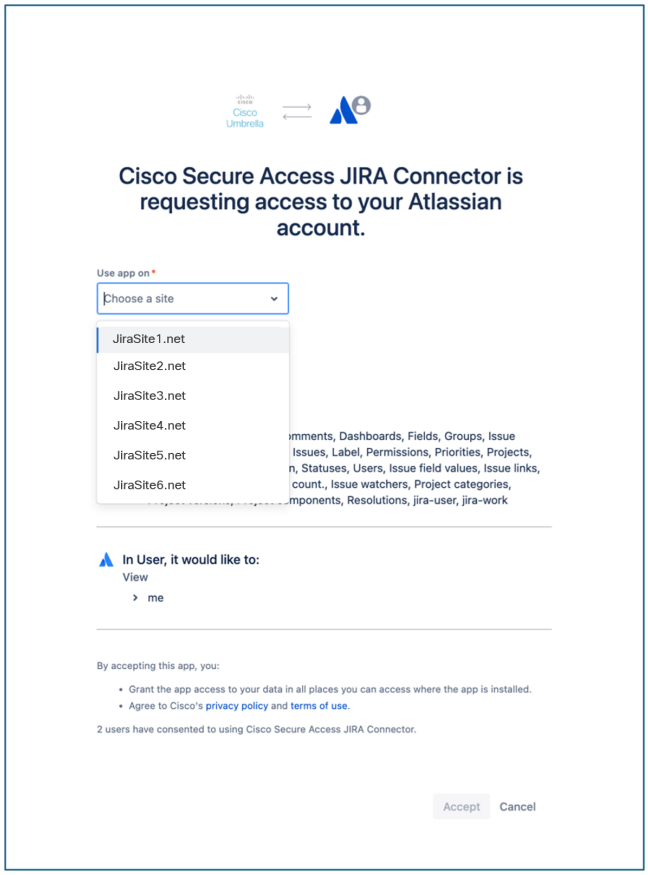
> **Note**
>
> Secure Access leaves no indication in the Jira page or comment of the attachment deletion.



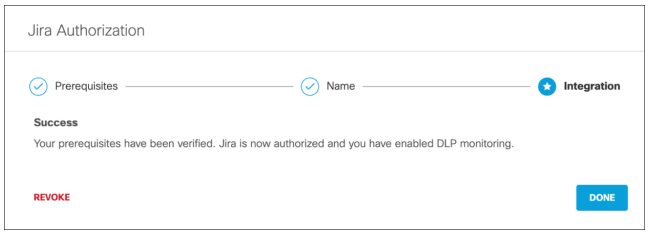
7. Click **Next** to be redirected to the Atlassian login page.



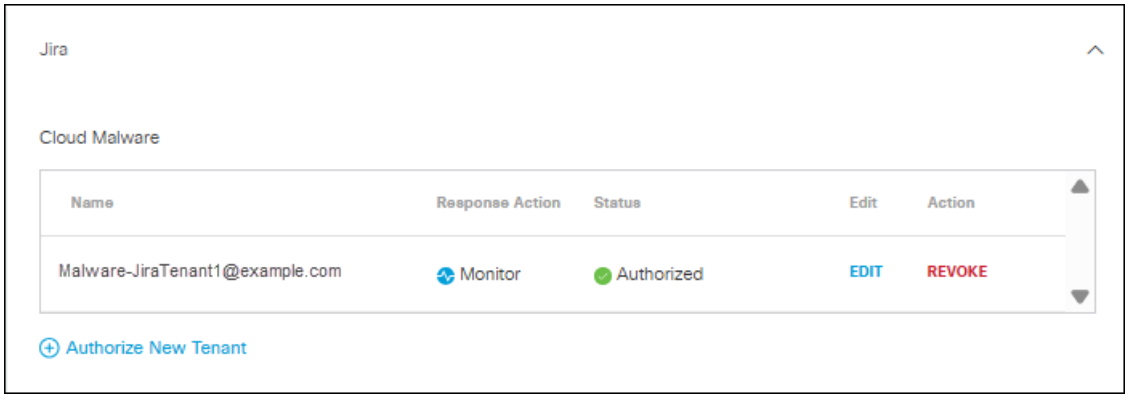
8. Log in with Jira admin credentials. The Jira Access Authorization page will appear.
9. From the **Use app on** drop-down, select a Jira site for the new tenant to access. (Each tenant can access only one Jira site.) Click **Accept**.



10. You are redirected to Secure Access and a message appears showing the integration was successful. It may take up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done** to complete.



11. The new Cloud Malware tenant will appear on the Authorization page in the list under **Jira**.



Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants

Describes Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants in Cisco Secure Access and explains Limitations. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports two Cloud Access Security Broker (CASB) features for Microsoft 365:

- Cloud Malware protection for OneDrive, SharePoint Online, and Outlook sites within your Microsoft 365 deployment.

Note on running both Microsoft 365 and Cloud Malware: Microsoft 365 and Cloud Malware both protect users against malware. However, their functionalities are not redundant. Microsoft 365 might discover malware that Cloud Malware does not find. Cloud Malware also finds malware that Microsoft 365 overlooks. There is value to running Microsoft 365 and Cloud Malware simultaneously.

- CASB detection of third-party cloud applications that have been granted OAuth-based permission to access a user's protected resources on Microsoft 365 Sharepoint Online and OneDrive. For more information, see Third-Party Apps Report.

You can enable CASB features for authorized tenants that use the following Microsoft 365 applications:

- Sharepoint Online
- OneDrive
- Outlook (For Cloud Malware protection only and for the primary inbox only. For outgoing mail you can enable Data Loss Prevention; see Enable SaaS API Data Loss Prevention for Microsoft 365 Tenants.)

> **Note**
>
> You cannot add an application to an existing tenant. If you have an existing Microsoft 365 tenant that uses one or two of these applications and you wish to add another application to that tenant, you must first revoke authorization for the existing tenant, then create a new tenant using all the desired applications.

Limitations

- A tenant the fails to authenticate cannot be deleted.
- Secure Access Cloud Malware attempts to quarantine a file will fail if that file has been locked by Microsoft 365. This may occur if Microsoft 365 Advanced Threat Protection (ATP) has detected malware in the file. In such a case, the lock placed by ATP take precedence over Umbrella's ability to detect or remediate DLP violations in malware.

Prerequisites for Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants

Describes Prerequisites for Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Full Admin user role. For more information, see Manage Accounts.
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- The user performing the installation *must* use a service account with a Microsoft 365 Global Admin and active license
- Audit log must be enabled for Microsoft 365. For more information, refer to Microsoft Technical documentation and search for **Turn auditing on or off.**

- Sharepoint Online and OneDrive must be enabled for the organization.
- The following IP addresses must be allowed if there are Firewall rules that prevent third-party applications:
  - 146.112.161.0/24
  - 146.112.163.0/24
  - 146.112.165.0/24
  - 146.112.167.0/24
- Users must have the following API permissions for Microsoft:

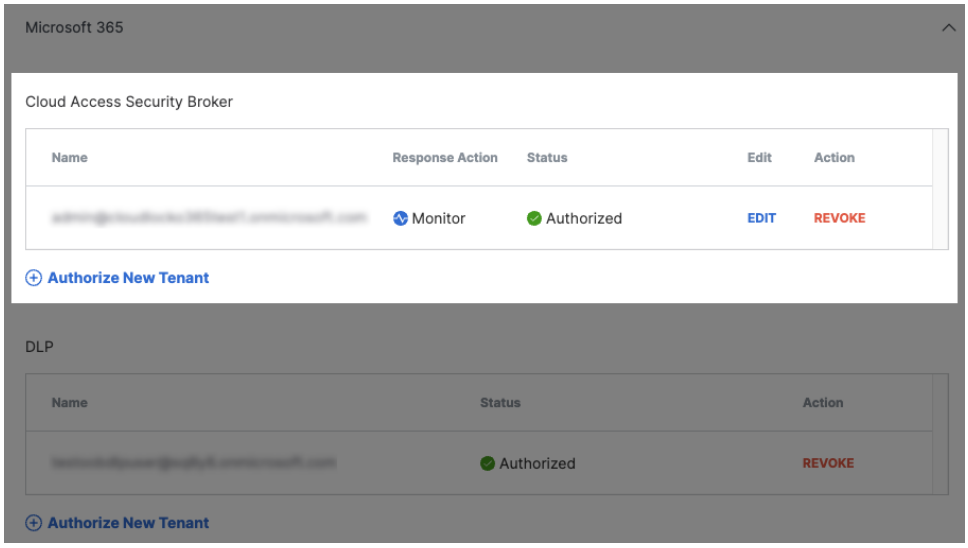
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
1. Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
2. Directory.Read.All	Application	Read directory data	Yes
3. Files.Read.All	Delegated	Read all files that user can access	No
4. Files.Read.All	Application	Read files in all site collections	Yes
5. Sites.Read.All	Delegated	Read items in all site collections	No
6. User.Read	Delegated	Sign in and read user profile	No
7. User.Read.All	Application	Read all users' full profiles	Yes
Microsoft 365 Management APIs			
1. ActivityFeed.Read	Application	Read activity data for the Organization	Yes
SharePoint			
1. Site.FullControl.All	Application	Full control of all site collections	Yes
2. User.Read.All	Application	Read user profiles	Yes

Authorize a Tenant

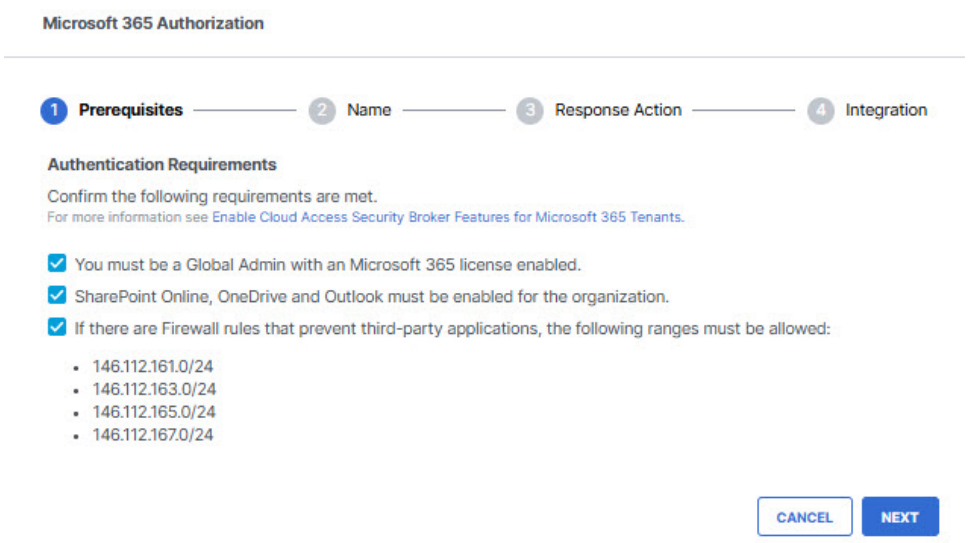
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

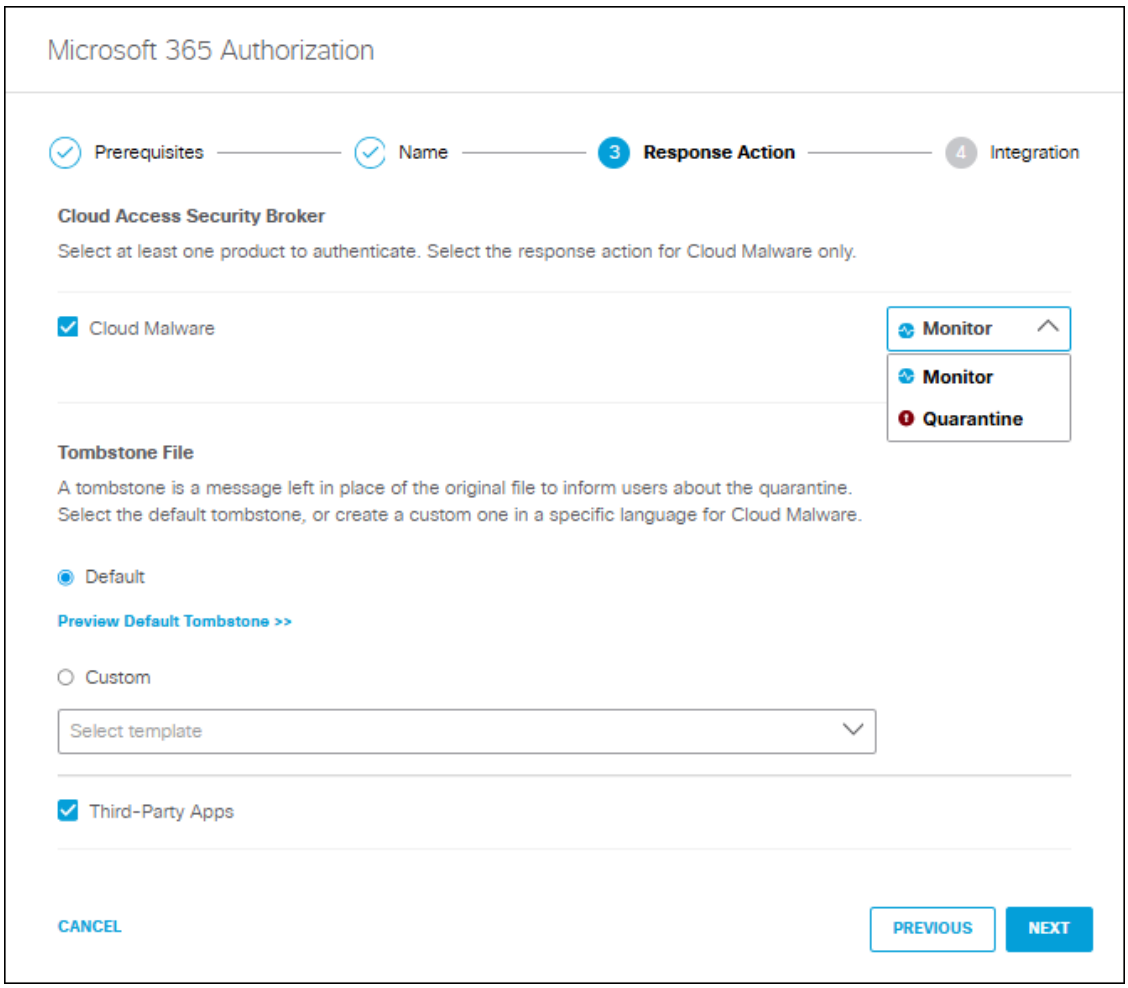
1. Navigate to **Admin** > **Authentication**.
2. Click to expand **Microsoft 365** in the list of **Platforms**.
3. Click **Authorize New Tenant** in the **Cloud Access Security** Broker subsection to add a Microsoft 365 tenant to your Secure Access environment.



4. Check the boxes to confirm that you meet all three **Authentication Requirements** in the **Microsoft 365 Authorization Prerequisites** dialog, then click **Next**.



5. Create a name for your tenant, then click **Next**.
6. Select one or both Cloud Access Security Broker (CASB) features to authenticate: **Cloud Malware** and **Third-Party Apps**.



If you choose to authorize for Cloud Malware protection, you must also select a **Response Action** for Umbrella to apply to Microsoft 365 files found with malware.

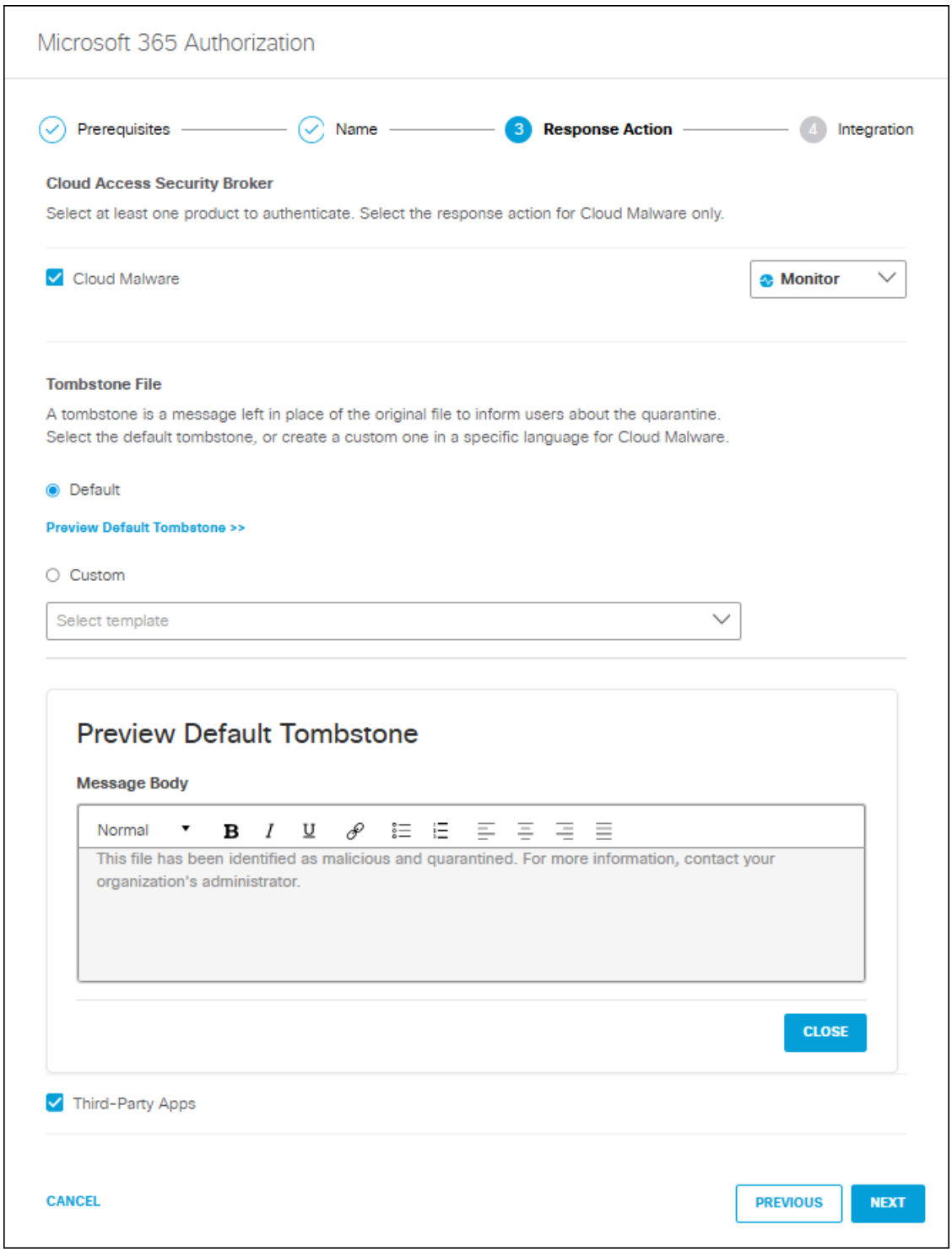
- Choose **Monitor** to cause Umbrella to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
- Choose **Quarantine** to:
  - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
  - Replace the file in its original location with a text file named *`filename`*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

> **Note**
>
> If you choose **Quarantine** this will apply only to rules applied to Sharepoint and OneDrive; Secure Access Cloud Malware supports monitoring Outlook messages in the primary inbox, but cannot quarantine them.
>
> For more information on Cloud Malware monitoring and quarantine features, see Manage Cloud Malware Protection. For more information on Third-Party Apps detection features, see Third-Party Apps Report.
>
> After making your selections, click **Next**.

7. Define the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**
     a. Click **Default**.
     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

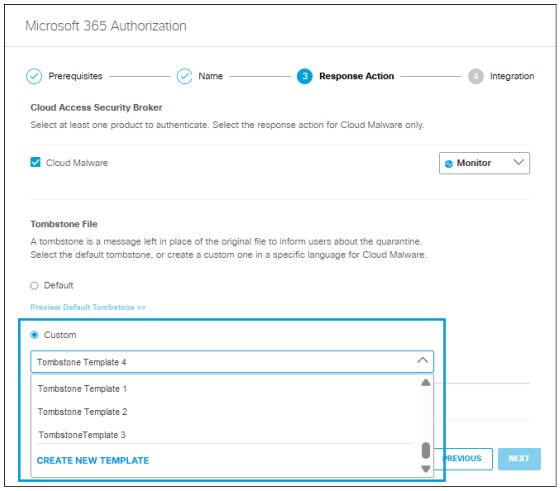


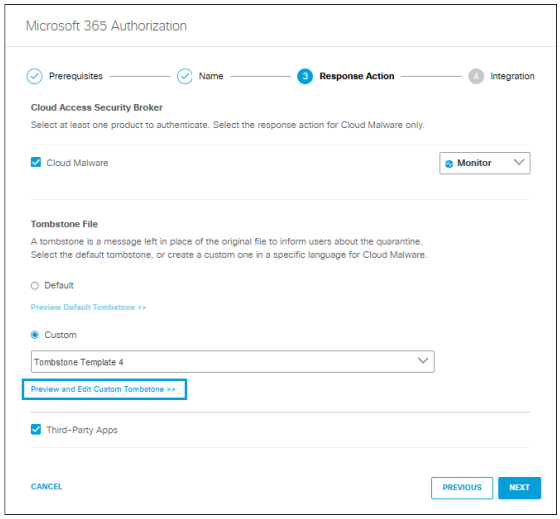
c. Click **CLOSE** to close the preview.

- **To Use a Custom Tombstone Template:**

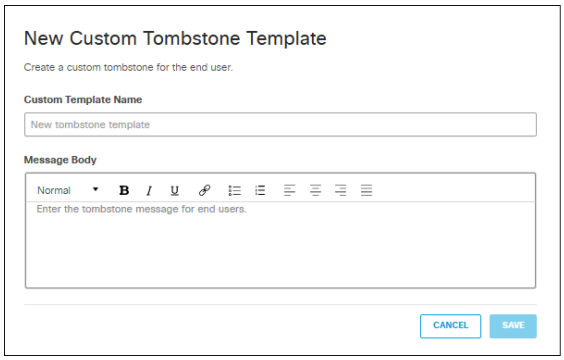
a. Click **Custom**.

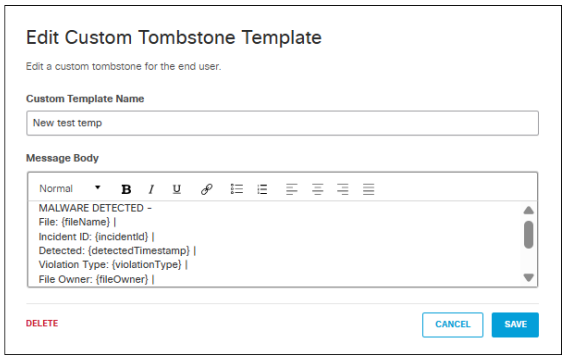
b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.





c. When you choose to create or edit a custom template for for tombstone text you will see one of these two dialogs, which are almost identical:





The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

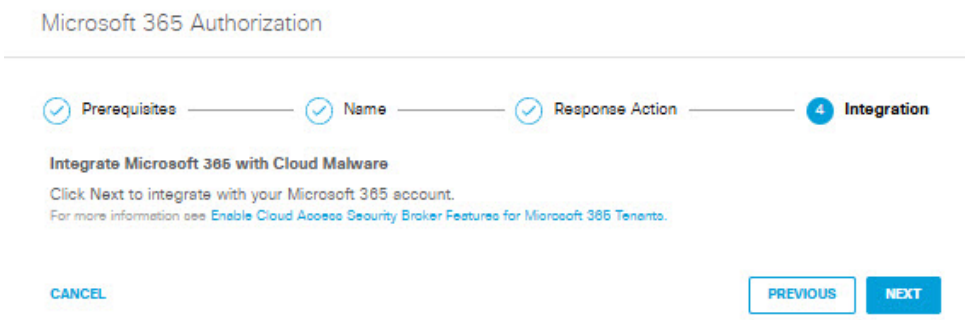
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

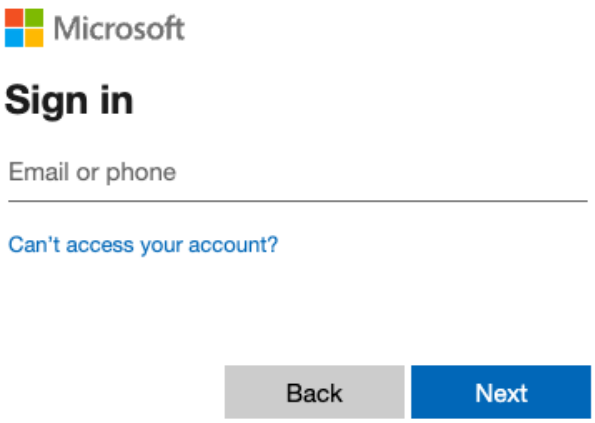
3. Click **SAVE** to complete the changes.

8. Click **Next** to proceed to **Integration**.
9. At the **Integration** step, click **Next**.



You are redirected to the Microsoft 365 login page.

10. Log into Microsoft 365 with admin credentials to authorize your Microsoft 365 account as a Secure Access CASB.



You are redirected to Secure Access, which displays a message when the authorization is complete. It can take up to 24 hours for the CASB integration status in Secure Access to show that authorization is complete.

11. Click **Done** to complete.

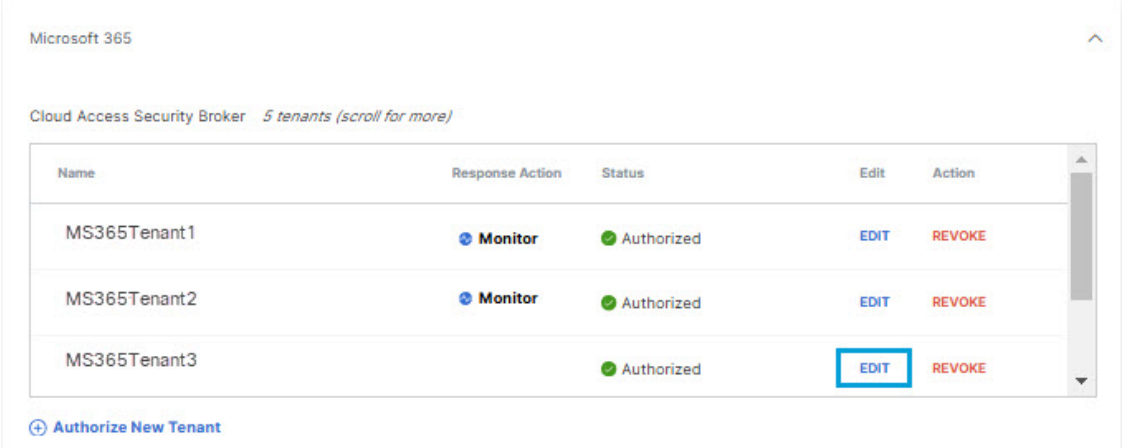
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the protection type or Response Action you have selected for a tenant.

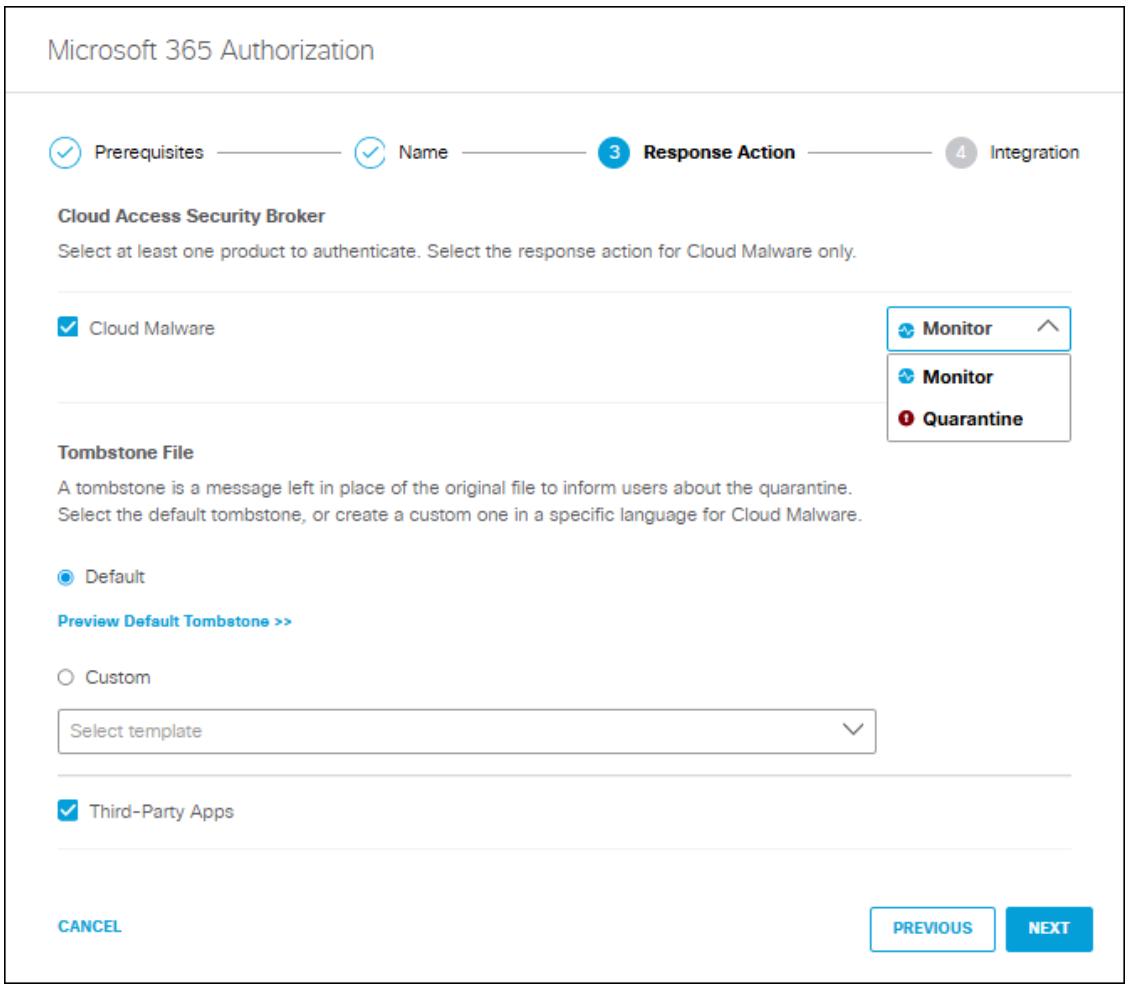
You can change the protection type or Response Action you have selected for a tenant.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. Click to expand **Microsoft 365** in the list of **Platforms**.
3. In the **Cloud Access Security Broker** subsection , from the **Edit** column, click **Edit**. You can edit any tenant.



4. Choose to authorize your Microsoft 365 tenant for Cloud Malware protection, or detection of third-party cloud applications, or both.



If you choose to authorize for Cloud Malware protection, you must also select a **Response Action** for Umbrella to apply to Microsoft 365 files found with malware.

- Choose **Monitor** to cause Umbrella to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
- Choose **Quarantine** to:
  - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
  - Replace the file in its original location with a text file named *filename*.ppt_Cisco_Quarantined.txt explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

> **Note**
>
> If you choose **Quarantine** this will apply only to rules applied to Sharepoint and OneDrive; Secure Access supports monitoring outgoing Outlook messages, but cannot quarantine them.
>
> For more information on Cloud Malware monitoring and quarantine features, see Manage Cloud Malware Protection. For more information on Third-Party Apps detection features, see Third-Party Apps Report.

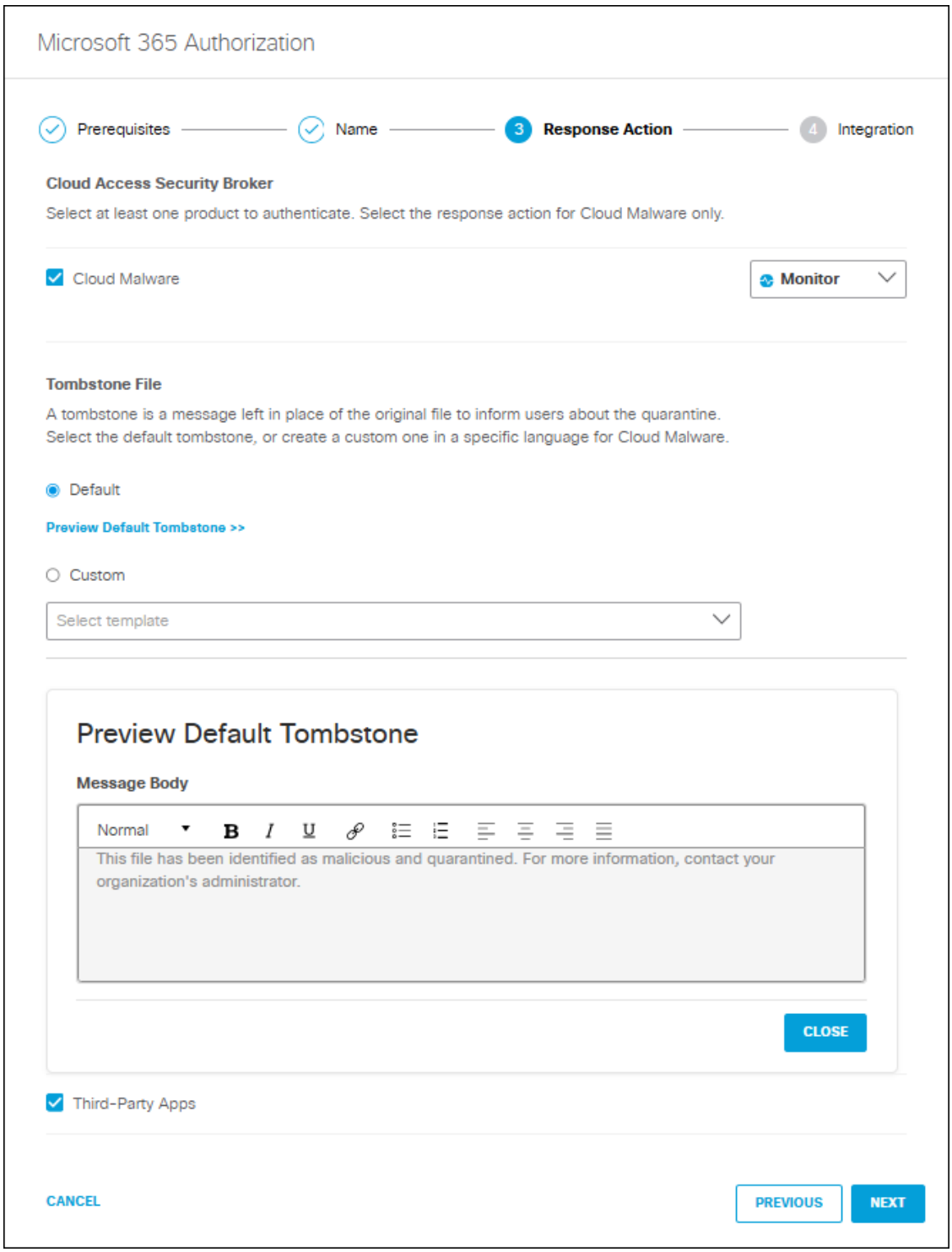
5. Change the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

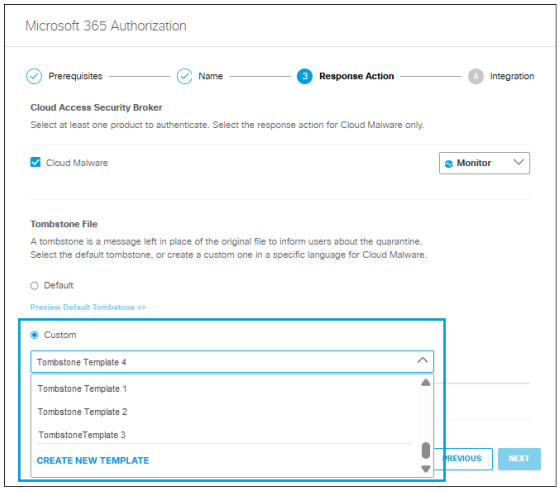


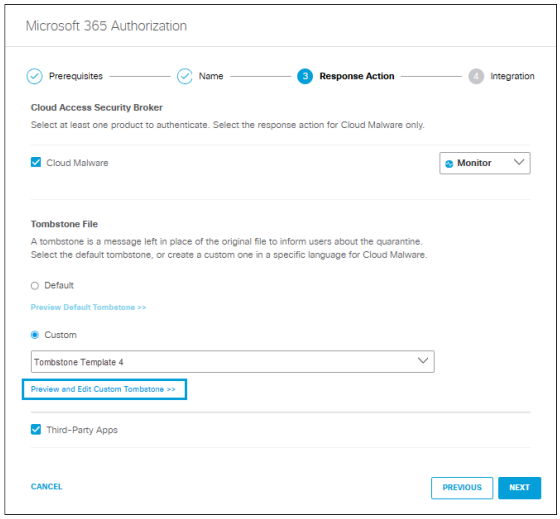
c. Click **CLOSE** to close the preview.

- **To Use a Custom Tombstone Template:**

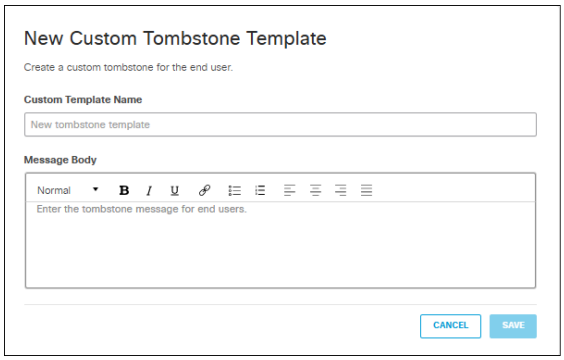
a. Click **Custom**.

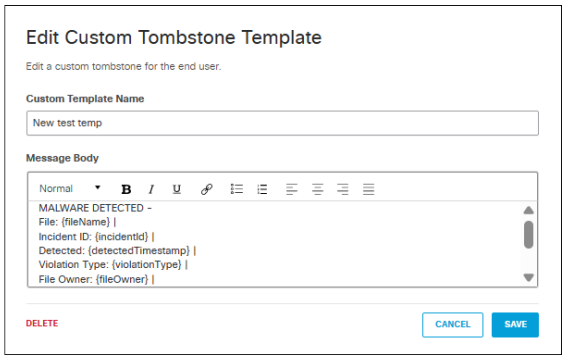
b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.





c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:





The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

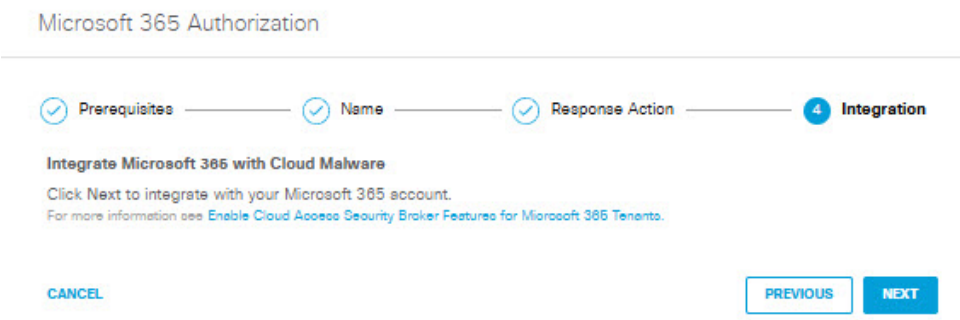
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

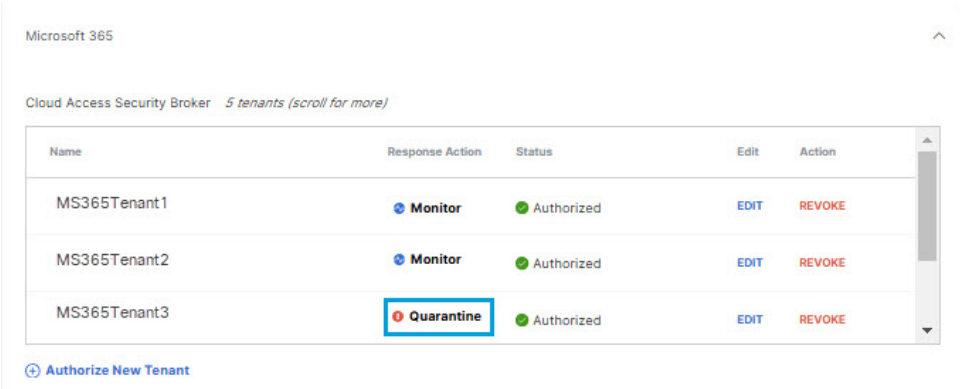
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

6. Click **Next** to proceed to **Integration**.
7. At the **Integration** step, click **Next**.



8. The new Response Action is displayed.



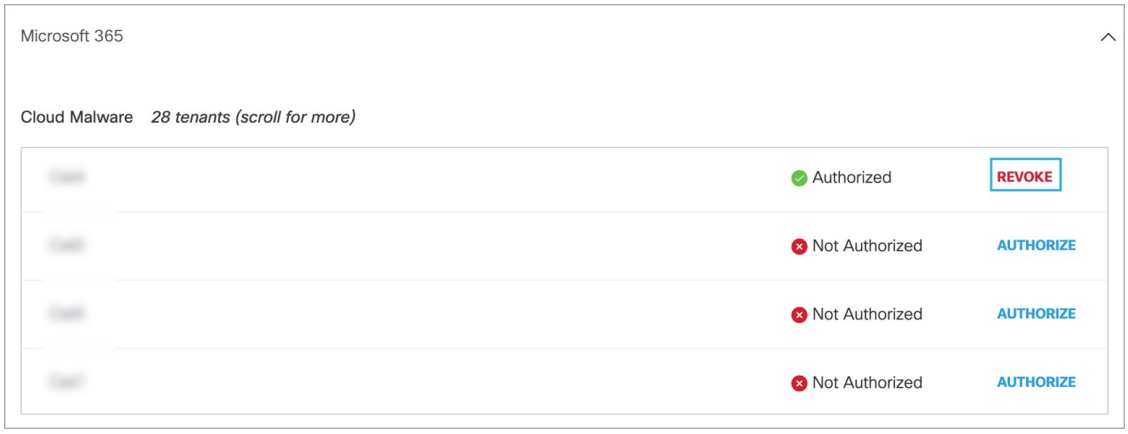
> **Note**
>
> For tenants authorized only for CASB detection of third-party applications, no Response Action is shown.

Revoke Authorization

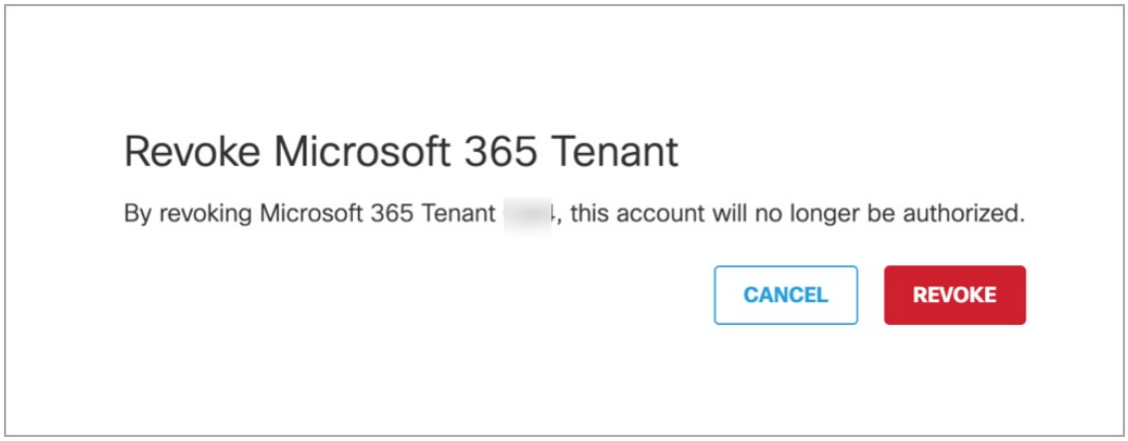
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



Enable Cloud Malware Protection for Salesforce Tenants

Provides instructions for completing the Enable Cloud Malware Protection for Salesforce Tenants workflow in Cisco Secure Access. You must have full admin access to the Secure Access dashboard.

Secure Access supports Cloud Malware protection in both production and sandbox development Salesforce environments for:

- files uploaded to your Salesforce Enterprise Grid deployment in the Sales Cloud and Service Cloud.
- files exchanged in Salesforce chatter posts. (Cloud Malware protection is not available for Salesforce sObjects or chatter posts--only for files attached to chatter posts.)

To enable this protection you must first authorize your Salesforce tenant with Secure Access as described here.

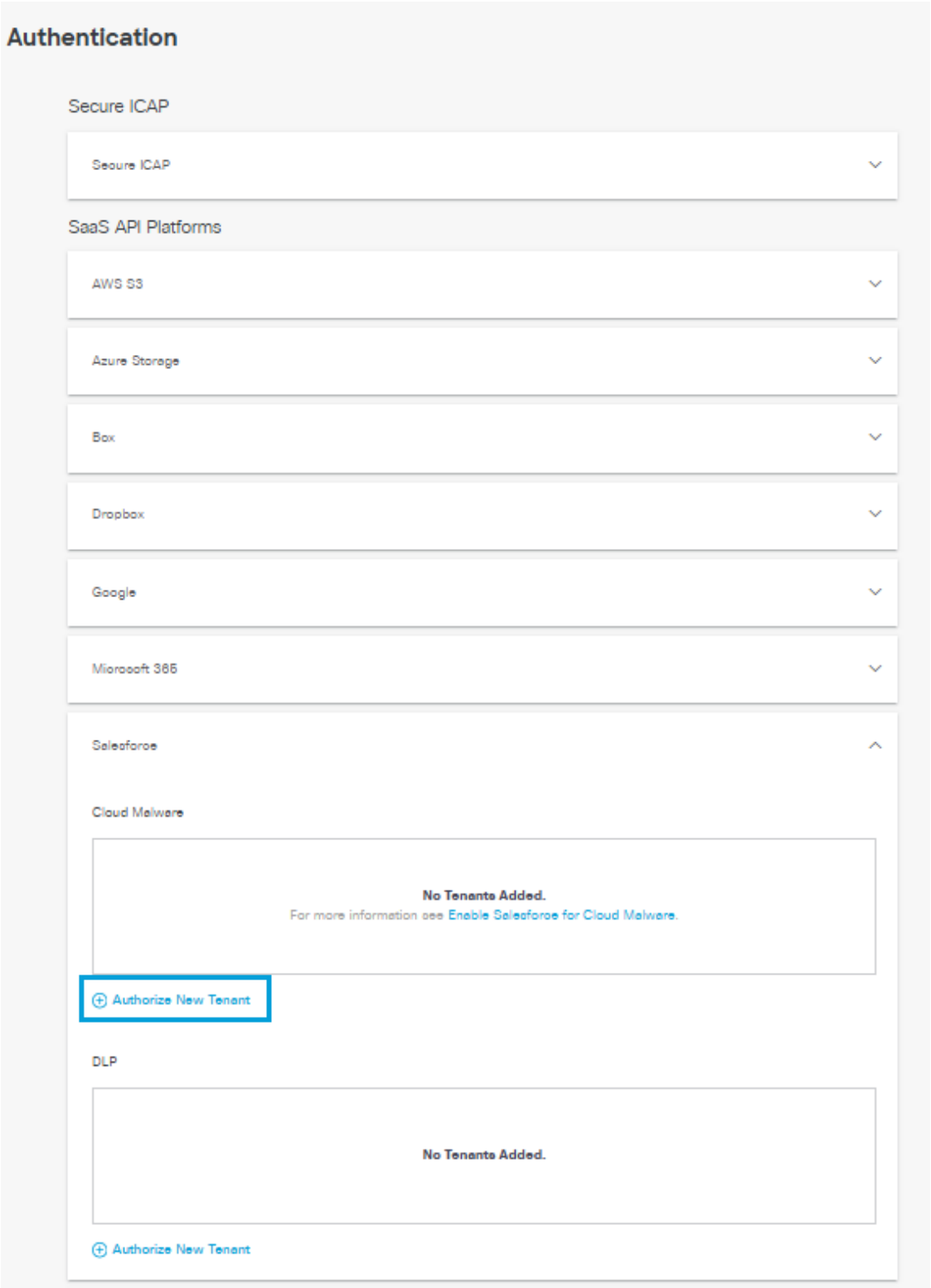
Before you begin

- You must have full admin access to the Secure Access dashboard. See Manage Accounts.
- You must have full admin access in a Salesforce Enterprise Grid account.
- You must install or update `Node.js`. The Salesforce CLI requires `Node.js` to run. We recommend using `Node.js` 18.x or higher; `Node.js` 20.x is preferred.
- You must install the Salesforce CLI. This is the primary tool for interacting with Salesforce orgs and managing Salesforce DX projects.
- You must log in to the Salesforce org you intend to authorize as a tenant.
- You must Download the Salesforce quarantine package and install it for your Salesforce tenant. This enables Secure Access to support the quarantine response action for Salesforce files. (If you have already deployed the package to support SaaS API DLP for this tenant, you need not do it again.)
- You must set the appropriate systems permissions in your Salesforce deployment. (If you have already done this to support SaaS API DLP for this tenant, you need not do it again.)

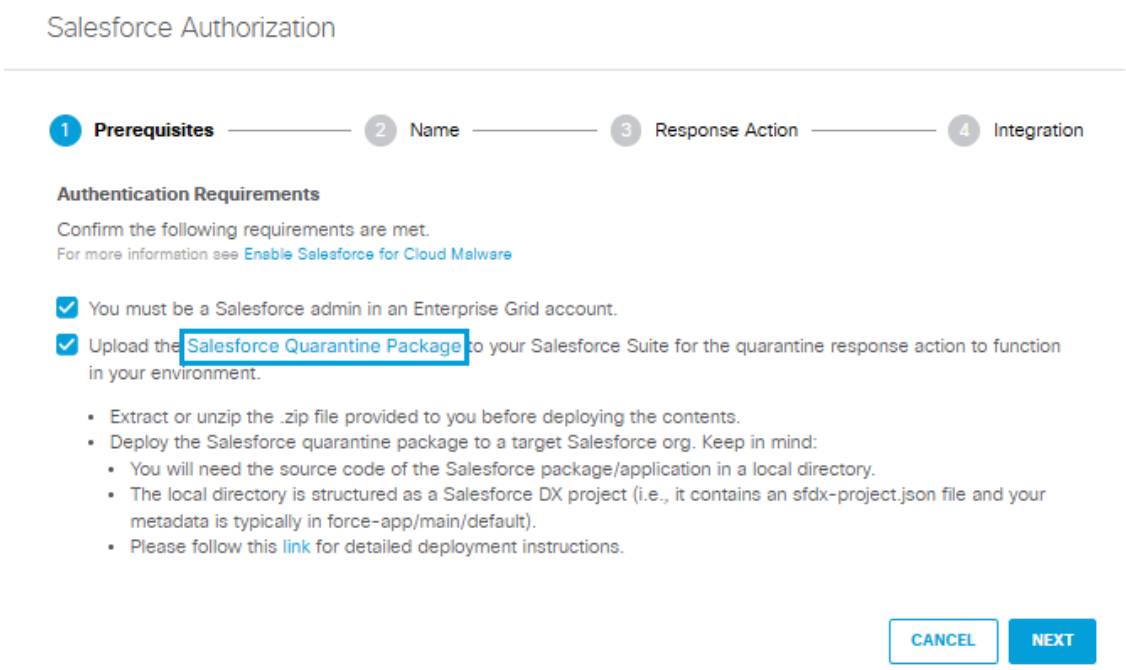
The Salesforce user account to which the quarantine package is deployed and permissions are applied must be the same one that will be used to authorize the Salesforce tenant for Cloud Malware protection

Procedure

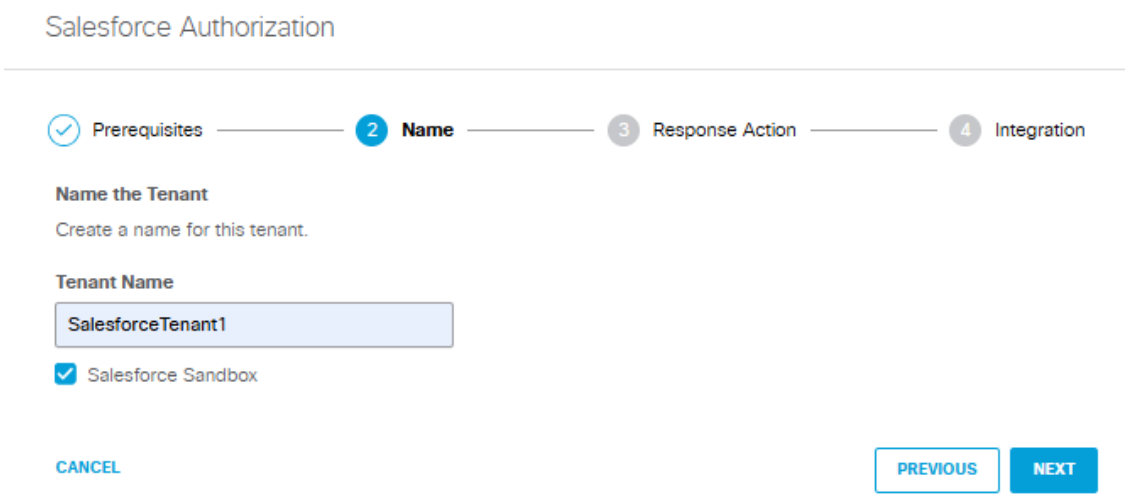
1. Navigate to **Admin > Authentication**.
2. Under **SaaS API Platforms**, click to expand **Salesforce**.



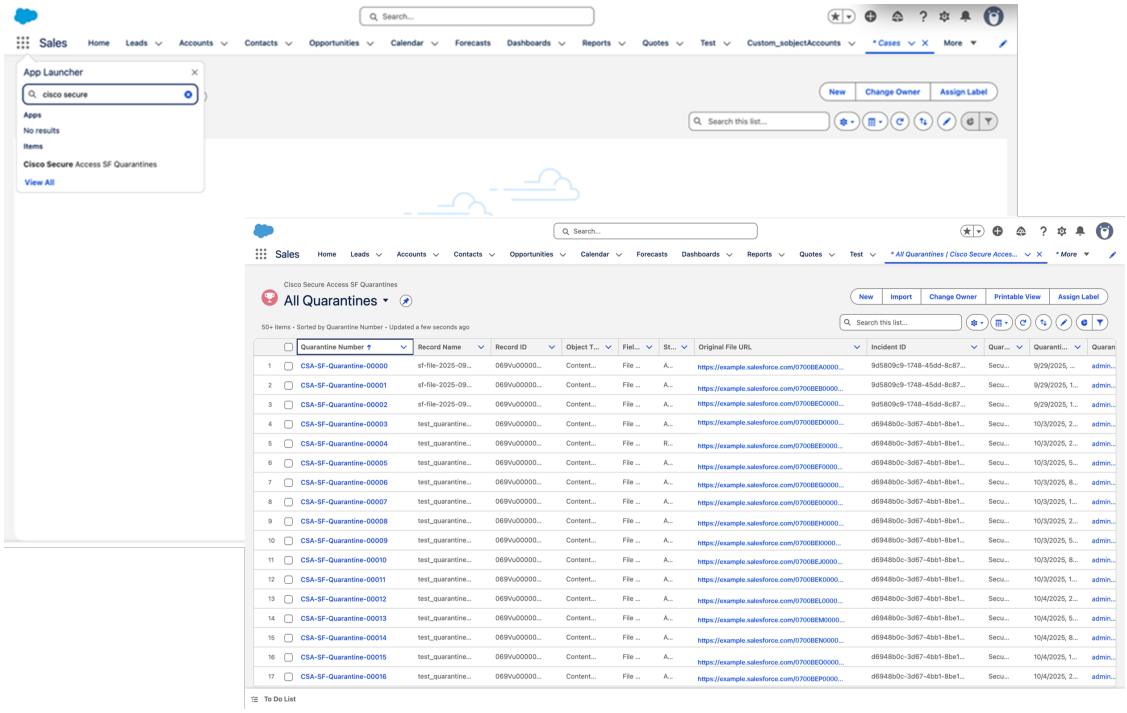
3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Salesforce tenant to your Secure Access environment.
4. In the **Salesforce Authorization** dialog, click the **Salesforce Quarantine Package** link and deploy the Salesforce quarantine package to your Salesforce tenant. This enables Secure Access to support the quarantine response action for Salesforce. (If you have already deployed the package to support SaaS API DLP for this tenant, you need not do it again.)



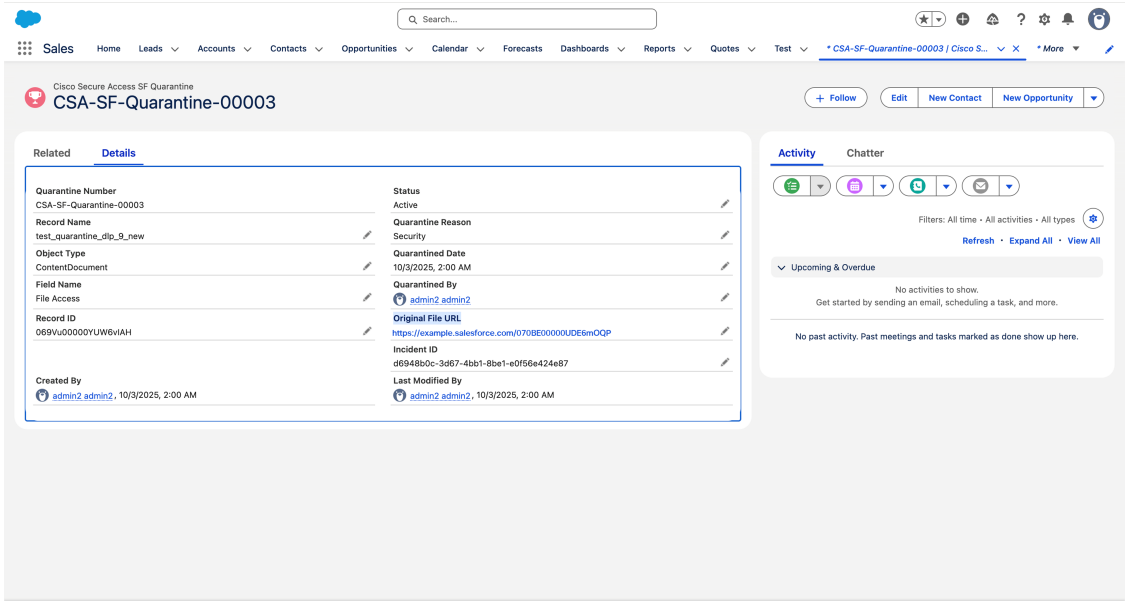
5. In the **Salesforce Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.
6. Enter the **Tenant Name**. If the tenant is a Salesforce sandbox, check **Salesforce Sandbox**. Click **Next**.



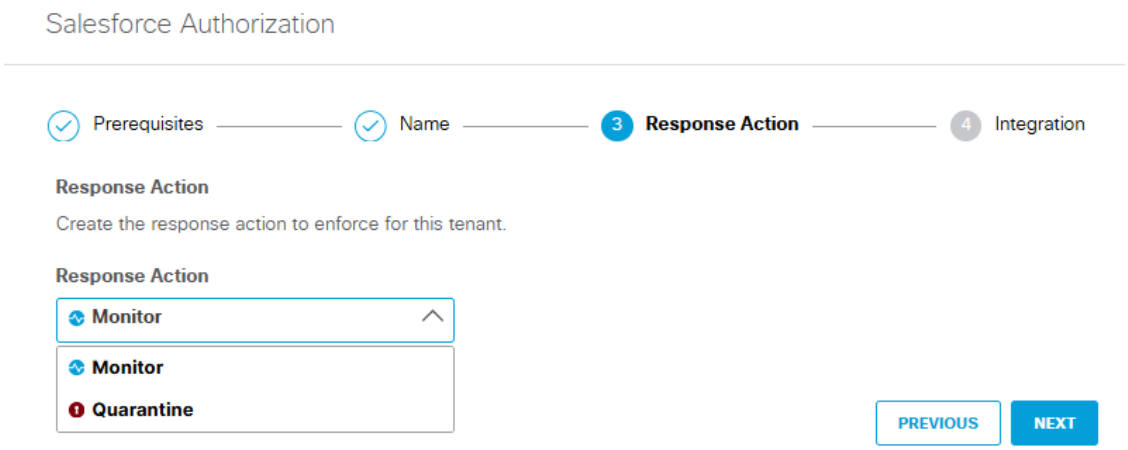
7. Select a **Response Action** for Secure Access to apply to Salesforce files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log Salesforce files detected with malware (including those attached to chatter posts). You will be able to manually quarantine files from the Cloud Malware report.
   - Secure Access applies the **Quarantine** response action to files only (including those attached to chatter posts). The quarantine option will work for Salesforce only if you have downloaded the Salesforce quarantine package and installed it for your Salesforce tenant. Choose **Quarantine** to:
     - Remove all collaborators, and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.



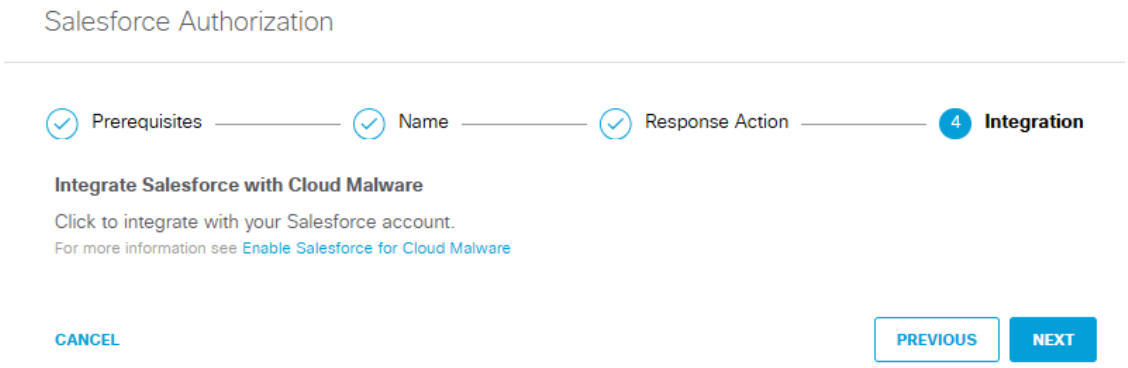
Click on the listing for an individual file to see the information about it:



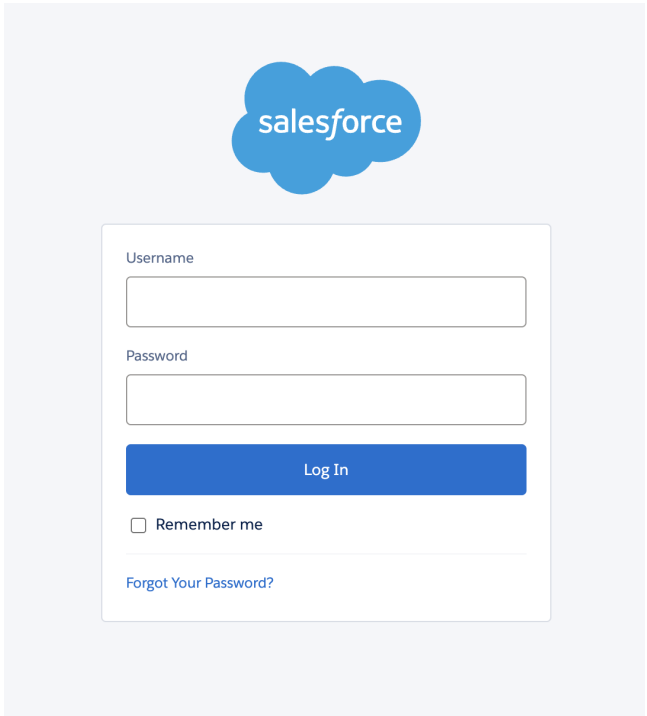
- Replace the file in its original location with a text file named ***filename*_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



8. Click **Next** to be redirected to the Salesforce login page.

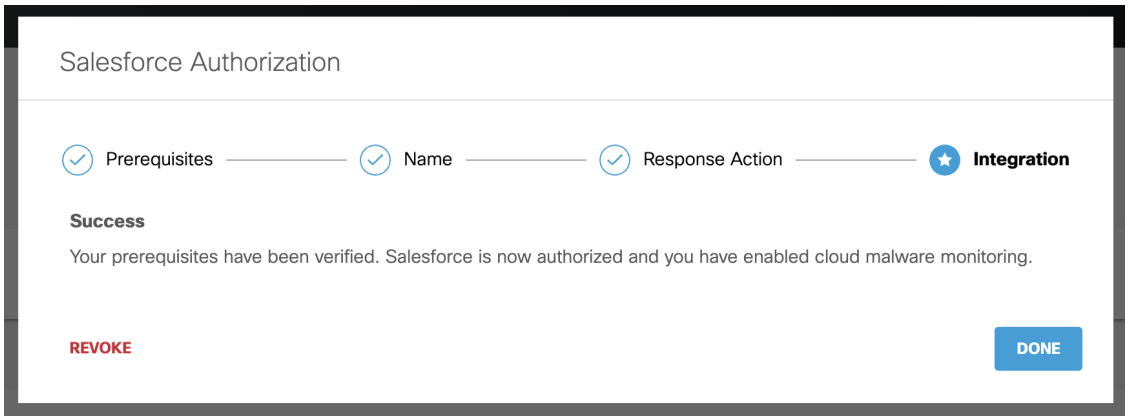


9. Log in to Salesforce with admin credentials to grant access.



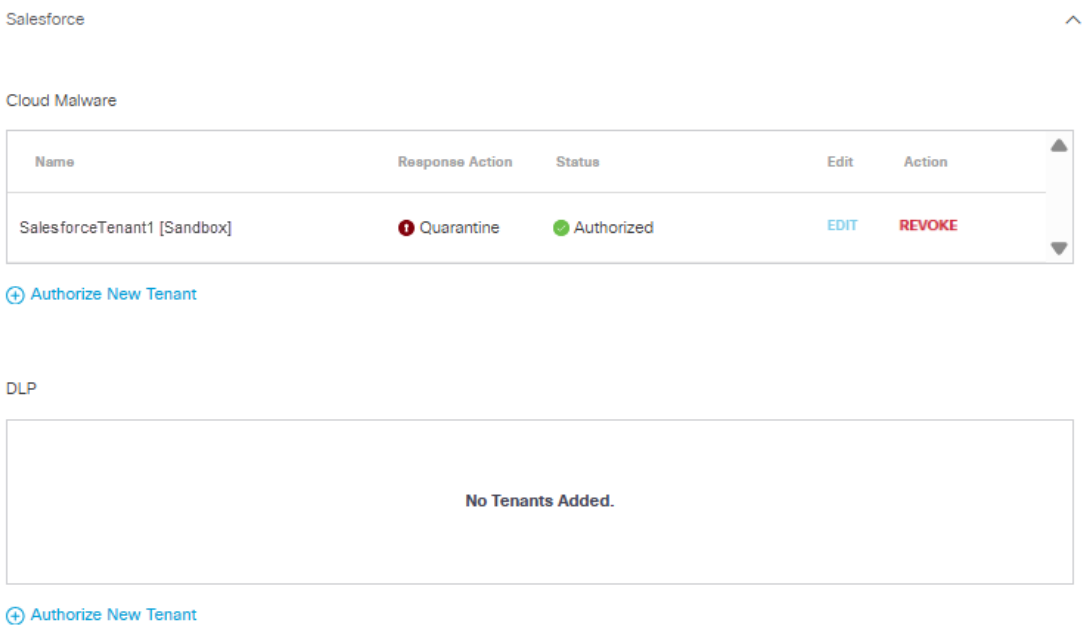
You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized.

10. Click **Done** to complete.



11. The new tenant will appear on the Authorization page in the list under **Salesforce**.

If you checked **Salesforce Sandbox** in Step 6, the tenant name will have `[Sandbox]` appended to it.



Edit a Salesforce Cloud Malware Tenant

Provides instructions for completing the Edit a Salesforce Cloud Malware Tenant workflow in Cisco Secure Access. You must have the Secure Access Full Admin user roll.

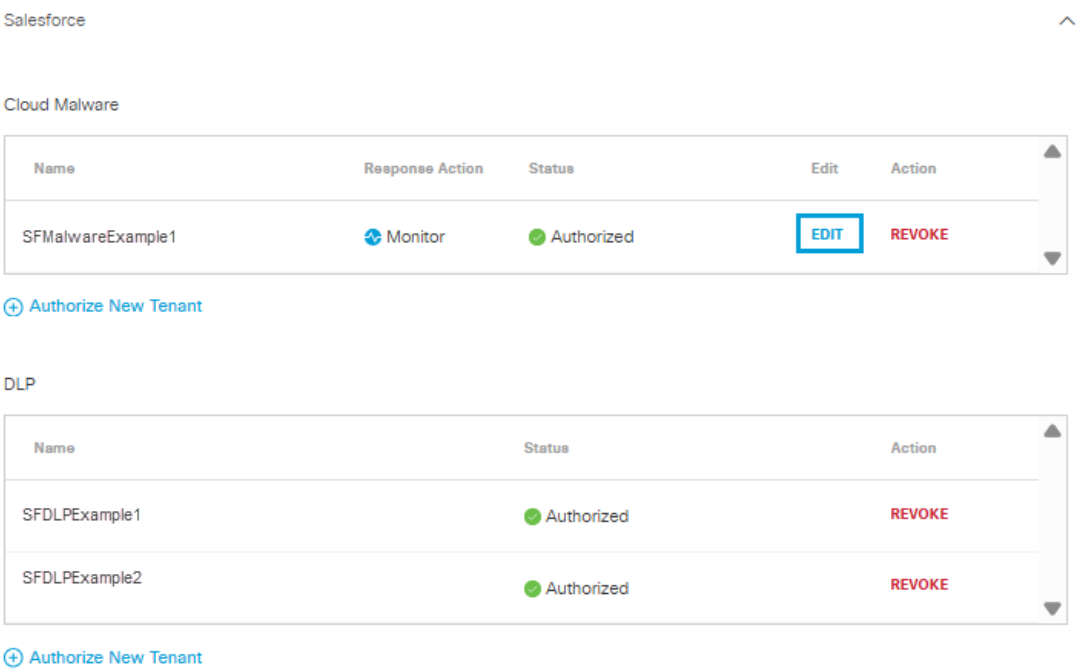
You can change the Response Action you have selected for a Salesforce tenant. Secure Access supports Cloud Malware protection for files uploaded to your Salesforce Enterprise Grid deployment or exchanged in Salesforce chatter posts--in both production and sandbox development environments. (Cloud Malware protection is not available for Salesforce sObjects or chatter posts--only for files attached to chatter posts.)

Before you begin

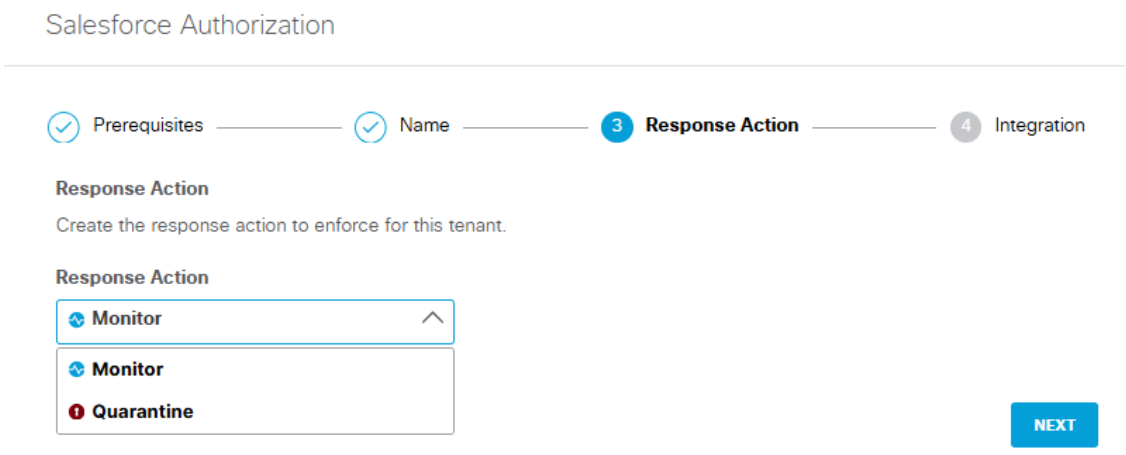
- You must have the Secure Access Full Admin user roll. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin > Authentication**.
2. In the **SaaS API Platforms** section, click **Salesforce**.
3. In the **Cloud Malware** section , from the **Edit** column, click **Edit**. You can edit any tenant.

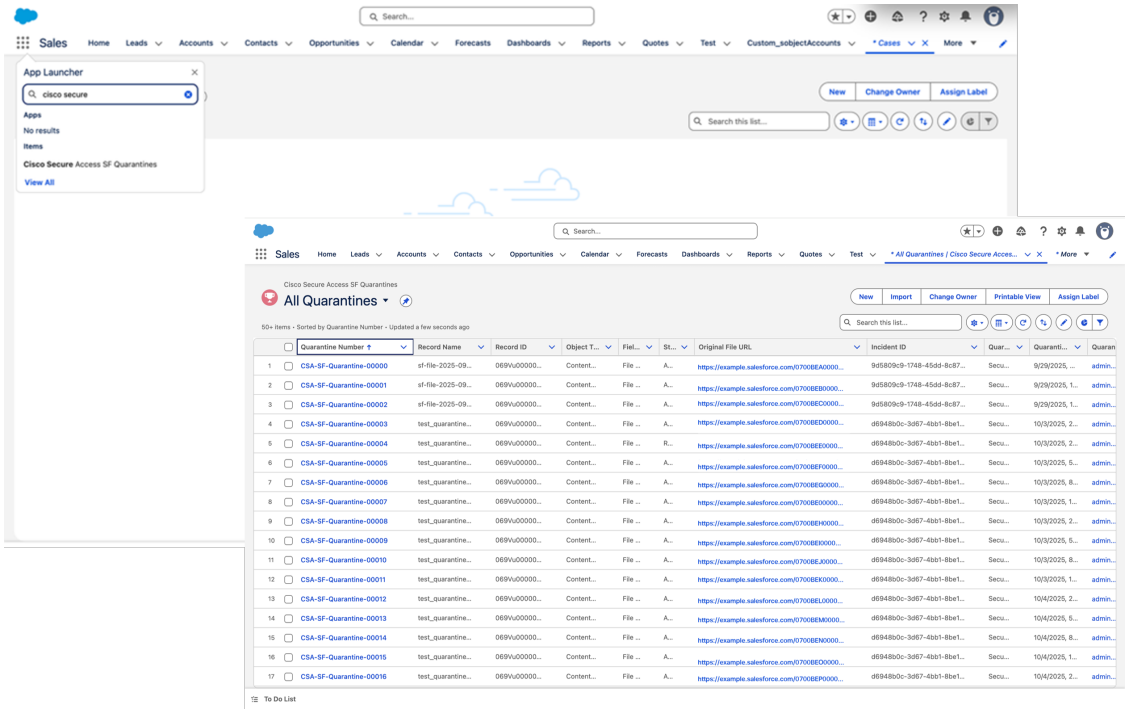


4. Select a **Response Action** for Secure Access to apply to Salesforce files found with malware and then click **Next**.

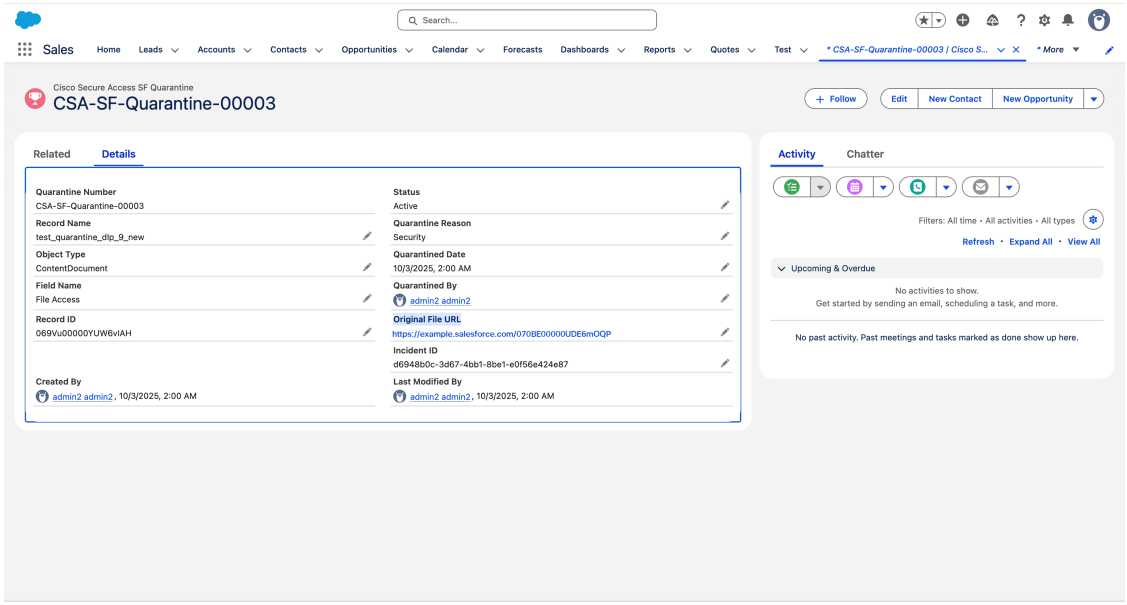


- Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.

- Secure Access applies the **Quarantine** response action to files only. The quarantine option will work for Salesforce only if you have downloaded the Salesforce quarantine package and installed it for your Salesforce tenant. When the system quarantines a Salesforce file:
  - The system remove all collaborators, and changes the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.

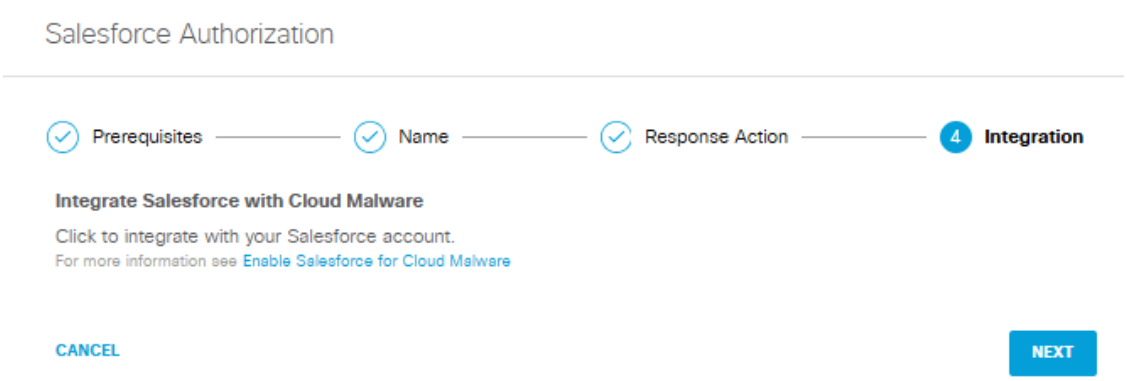


Click on the listing for an individual file to see the information about it:

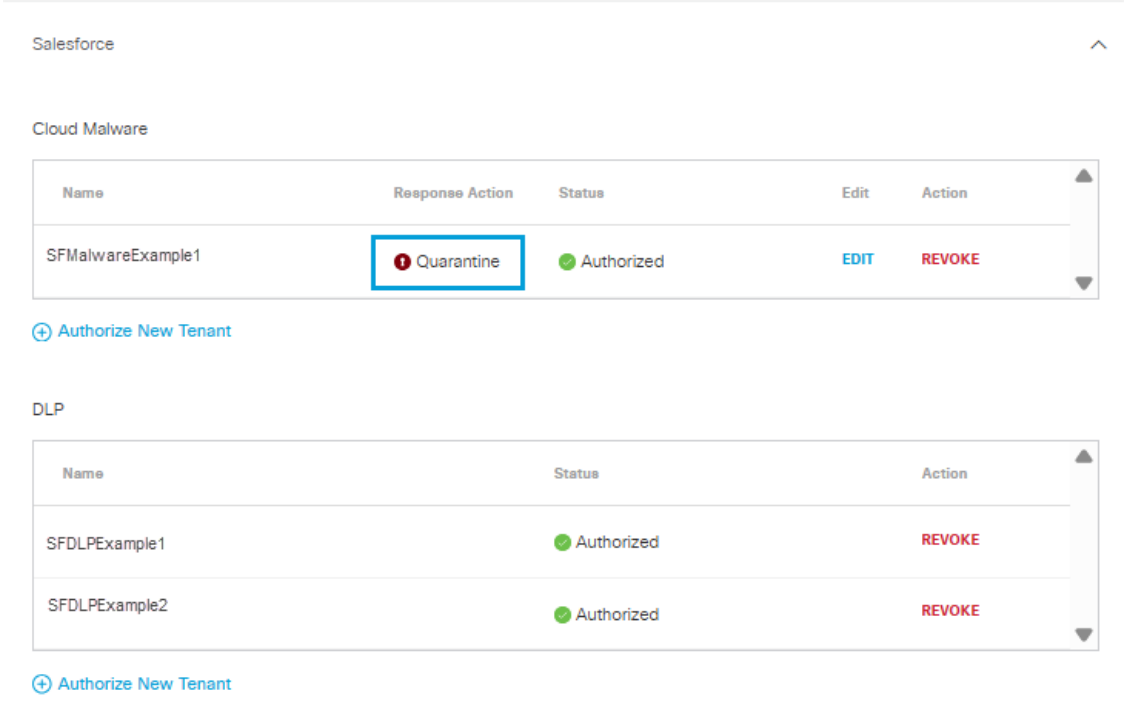


- The system replaces the file in its original location with a text file named ***filename*_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

5. Click **Next**.



The new **Response Action** is displayed.



Enable Cloud Malware Protection for ServiceNow Tenants

Describes Enable Cloud Malware Protection for ServiceNow Tenants in Cisco Secure Access. Secure Access supports Cloud Malware protection for your ServiceNow deployment.

Secure Access supports Cloud Malware protection for your ServiceNow deployment. Once you have authorized a ServiceNow tenant for Cloud Malware protection, you can create an app in ServiceNow to view the Cisco Quarantine table maintained in ServiceNow.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization).

- The application scope in your ServiceNow deployment must be set to Global.
- You must obtain the Instance Name for your ServiceNow account.
- The user performing the installation must use a ServiceNow account with the **ais_high_security_admin** role and the **oauth_user** role.
- You must add an OAuth Client to your ServiceNow deployment

Limitation

- A tenant that fails to authenticate cannot be deleted.

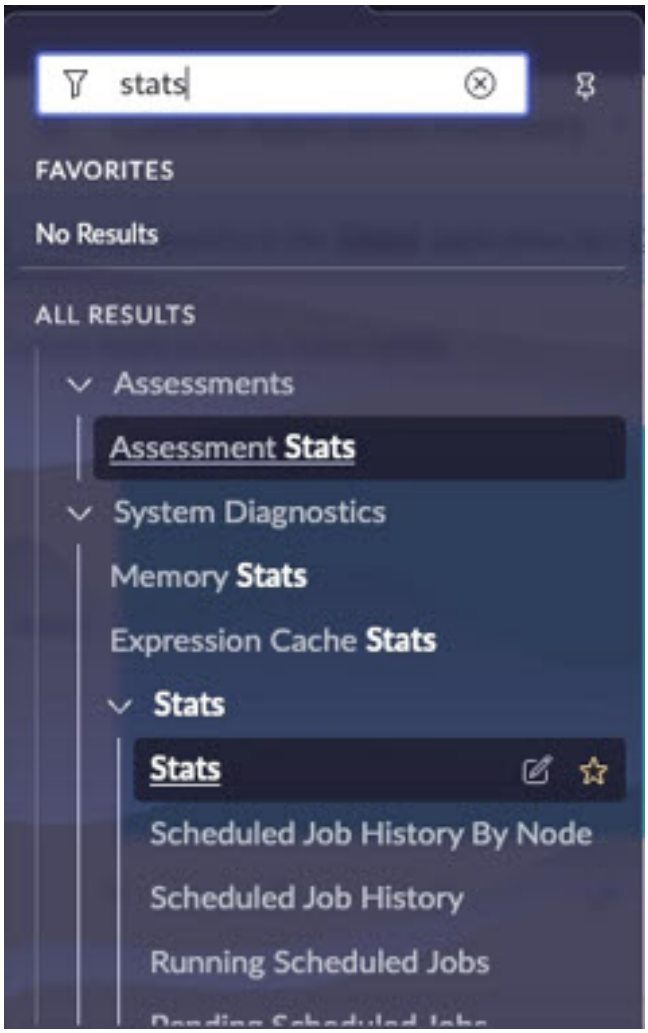
Find the Instance Name for your ServiceNow admin Account

Provides instructions for completing the Find the Instance Name for your ServiceNow admin Account workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal.

Procedure

1. Navigate to the **All** tab.
2. Filter for **Stats**. Under **System Diagnostics** > **Stats** click on **Stats**.



3. In the **Servlet Statistics** page that appears, note the value of the **Instance name**.

Assign the oauth_user role to the ServiceNow admin Account

Provides instructions for completing the Assign the oauth_user role to the ServiceNow admin Account workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal. Make sure you have the **ais_high_security_admin** role and the application scope is set to **Global**.

Procedure

1. Navigate to **All** > **User Administration** > **Users**.
2. Search for the User ID of the admin account and click on it.
3. Click on the **Roles** tab.
4. Click **Edit**.
5. Under **Collection** search for the role **oauth_user**, select it, and click **>** to move it to the **Roles List**.
6. Click **Save**.

Add an OAuth Client to Your ServiceNow Deployment

Provides instructions for completing the Add an OAuth Client to Your ServiceNow Deployment workflow in Cisco Secure Access. Perform these steps in your ServiceNow IT Service Management portal.

Perform these steps in your ServiceNow IT Service Management portal. Make sure you have the **ais_high_security_admin** role and the **oauth_user** role ,and the application scope is set to **Global**.

Procedure

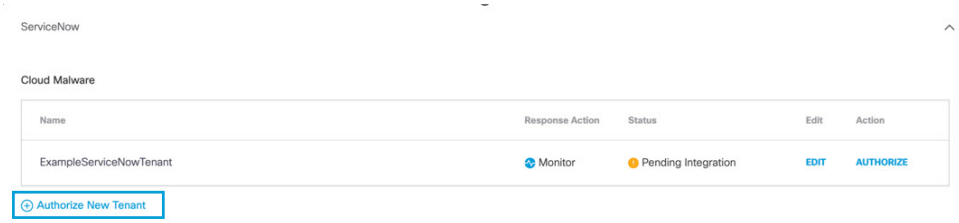
1. Navigate to **All** > **System OAuth** > **Application Registries**
2. Click on **New** and select **Create an OAuth API endpoint for external clients.**
3. Fill out the form that appears with the following required values (other fields are optional):
   - **Name:** Enter a name that will be used by the Secure Access ServiceNow Connector as a Client Id.
   - **Client Secret:** Enter a secret value compliant with your org policy. Take note of this value, as you will need it again when authorizing your ServiceNow tenant with Secure Access.
   - **Redirect URL:** https://management.api.umbrella.com/admin/v2/cloudApplicationInstances/oauth2/callback
   - **Refresh Token Live Span:** We recommend entering 31,536,000 seconds, which is one year. Once the refresh token expires, the ServiceNow tenant will need to be authorized with Secure Access again.
   - **Application:** Global.
4. Click **Submit**.

Authorize a Tenant

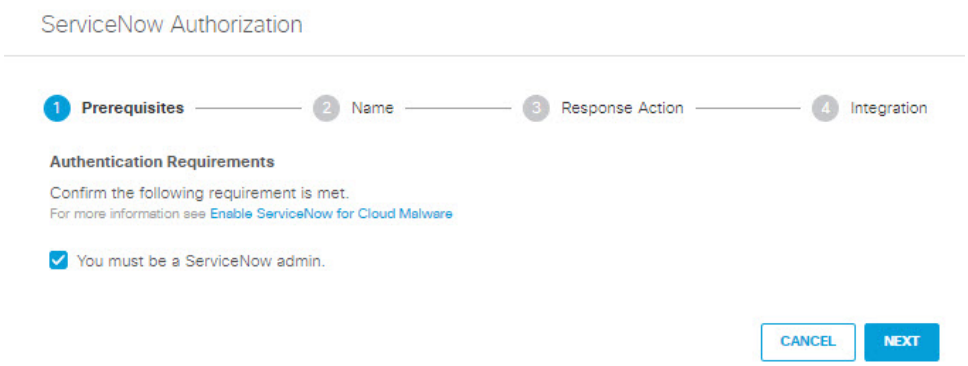
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

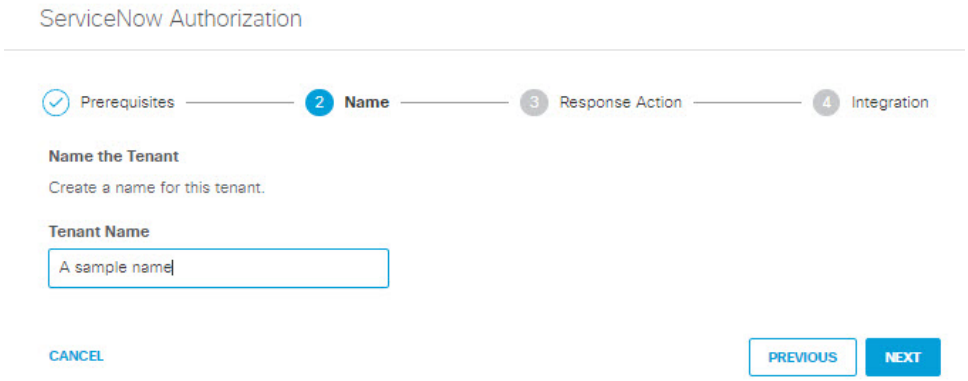
1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **ServiceNow**.
3. In the **Cloud Malware** subsection, click **Authorize New Tenant** to add a ServiceNow tenant to your Secure Access environment.



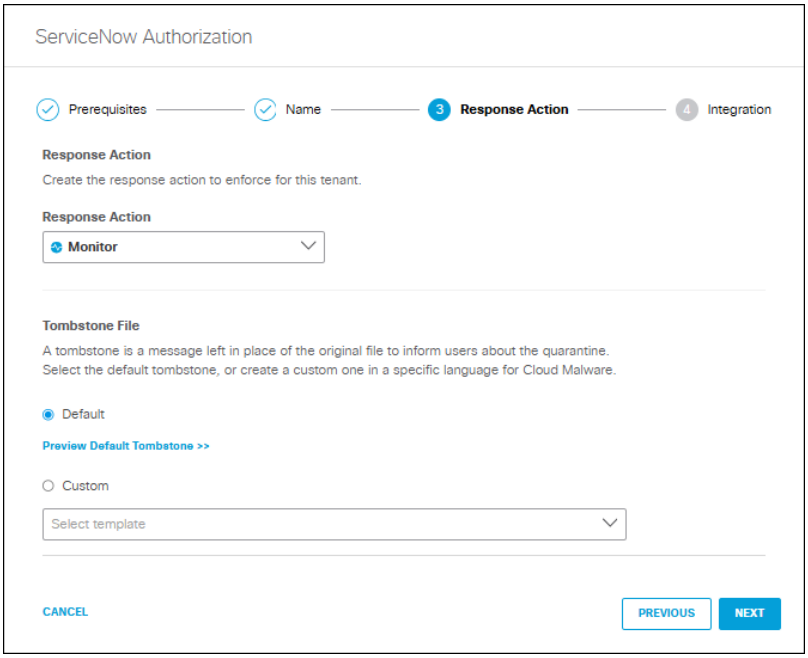
4. In the **ServiceNow Authorization** dialog, check the checkbox to verify you meet the prerequisite and then click **Next**.



5. Add a **Tenant Name** and then click **Next**.



6. Select a **Response Action** for Secure Access to apply to ServiceNow found with malware, then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a table named **Cisco_Quarantine_Malware** which can be access only by the admin user who authorized the ServiceNow tenant.
     - Attach a footprint to the notes\activities area of the table the file was originally attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.



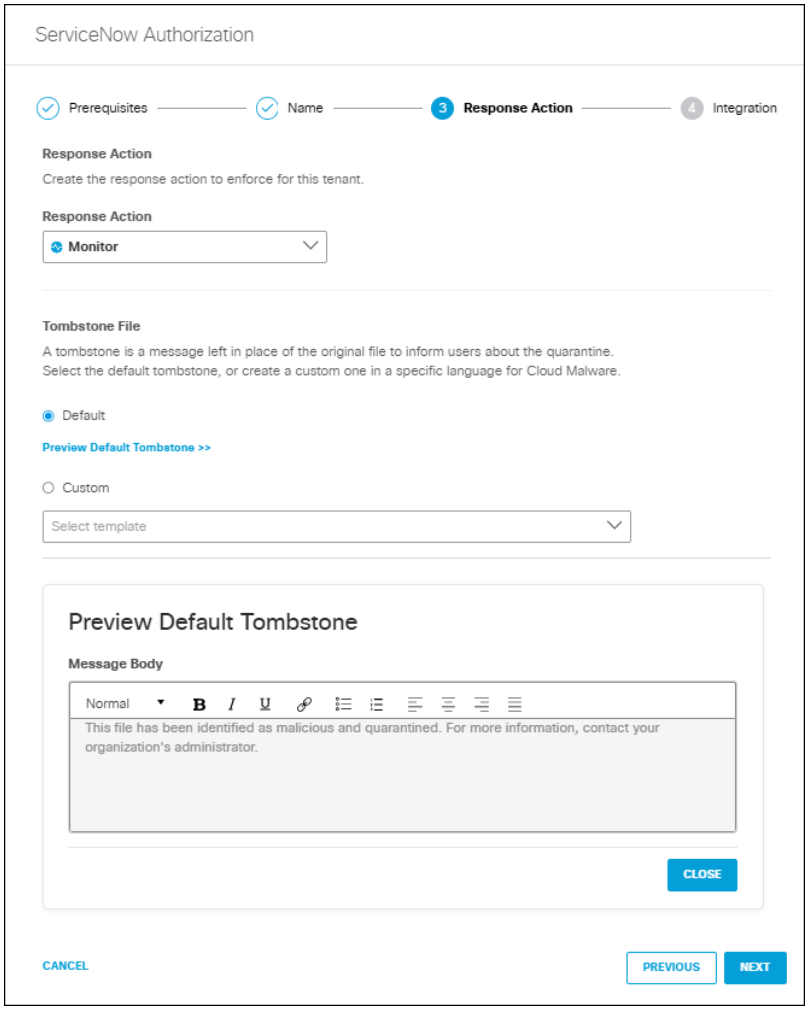
7. Define the message to appear in the footprint attached to the notesactivities area of the table the quarantined file was originally attached to.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a footprint as described in the previous step. You determine the contents of this footprint using a *tombstone template*:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

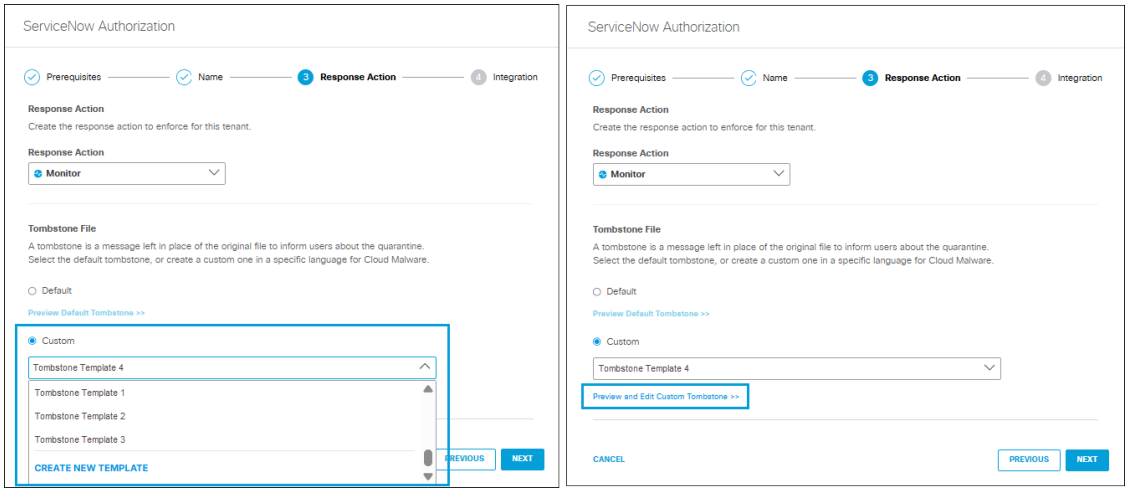


c. Click **CLOSE** to close the preview.

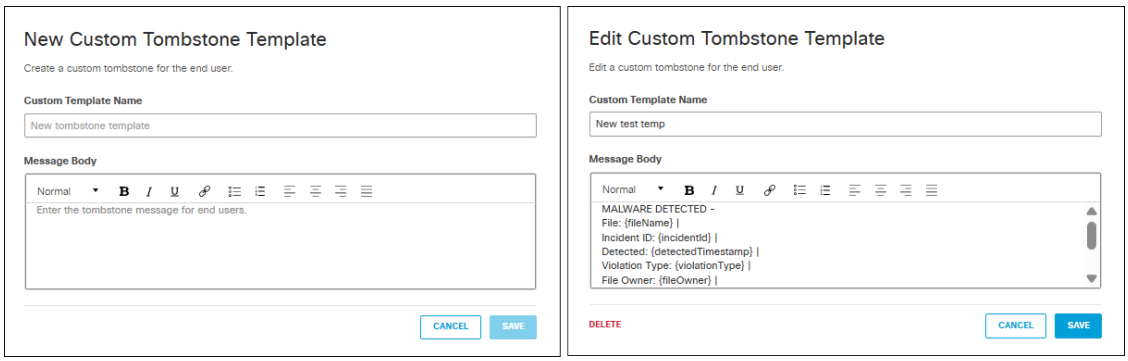
- **To Use a Custom Tombstone Template:**

a. Click **Custom**.

b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

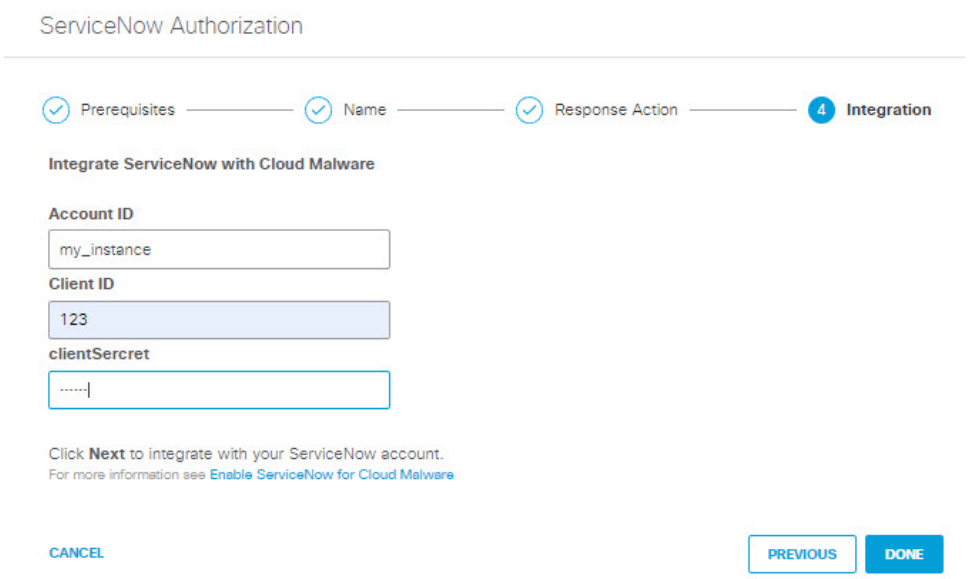
   The text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
   - **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileLocation}** - The file URL.

> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

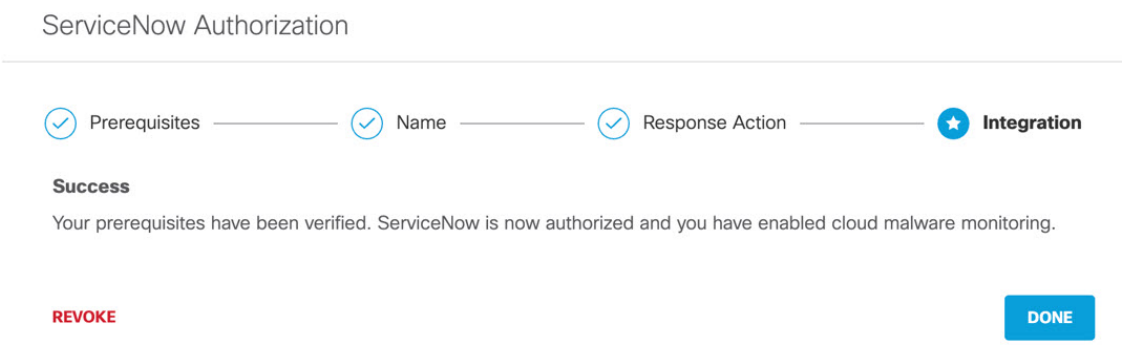
3. Click **SAVE** to complete the changes.

8. Enter the following and then click **Done**:
   - **Account ID**: Enter the Instance Name for your ServiceNow account.
   - **Client ID**: Enter the **Name** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.
   - **Client Secret**: Enter the **Client Secret** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.



> **Note**
>
> Save this information in a reliable location, as you will need it any time you change the Response Action for the tenant in the future.

9. You are redirected to the ServiceNow OAuth login page and a message will appear notifying you that secure-access-oauth would like to connect to your ServiceNow account. Click **Allow**.
10. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done**.



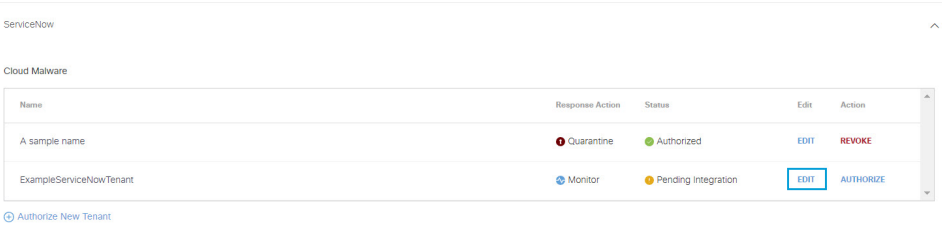
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the Response Action you have selected for a tenant.

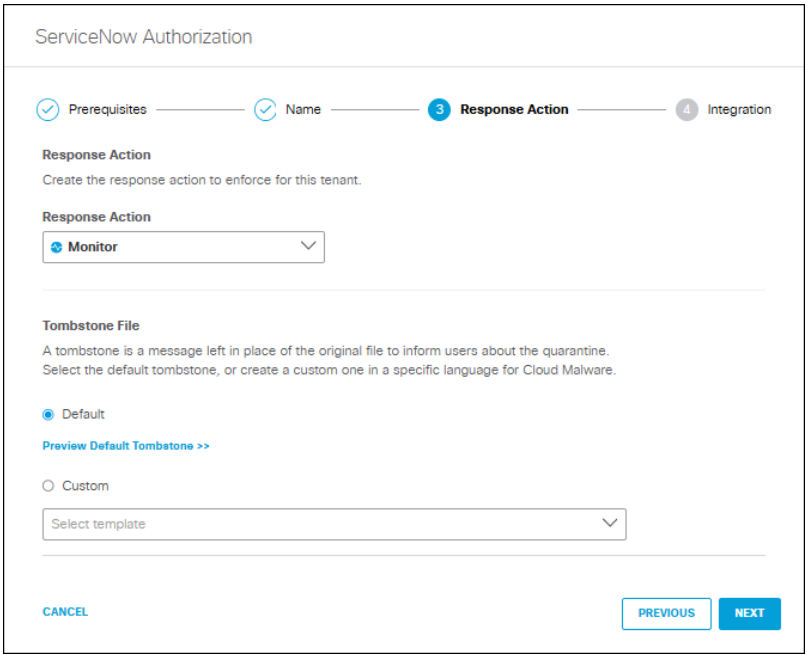
You can change the Response Action you have selected for a tenant.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **ServiceNow**.
3. In the **Cloud Malware** subsection , from the **Edit** column, click **Edit**. You can edit any tenant.



4. Select a **Response Action** for Secure Access to apply to Microsoft 365 files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
   - Choose **Quarantine** to:
     - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Microsoft 365 admin.
     - Replace the file in its original location with a text file named *filename*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.



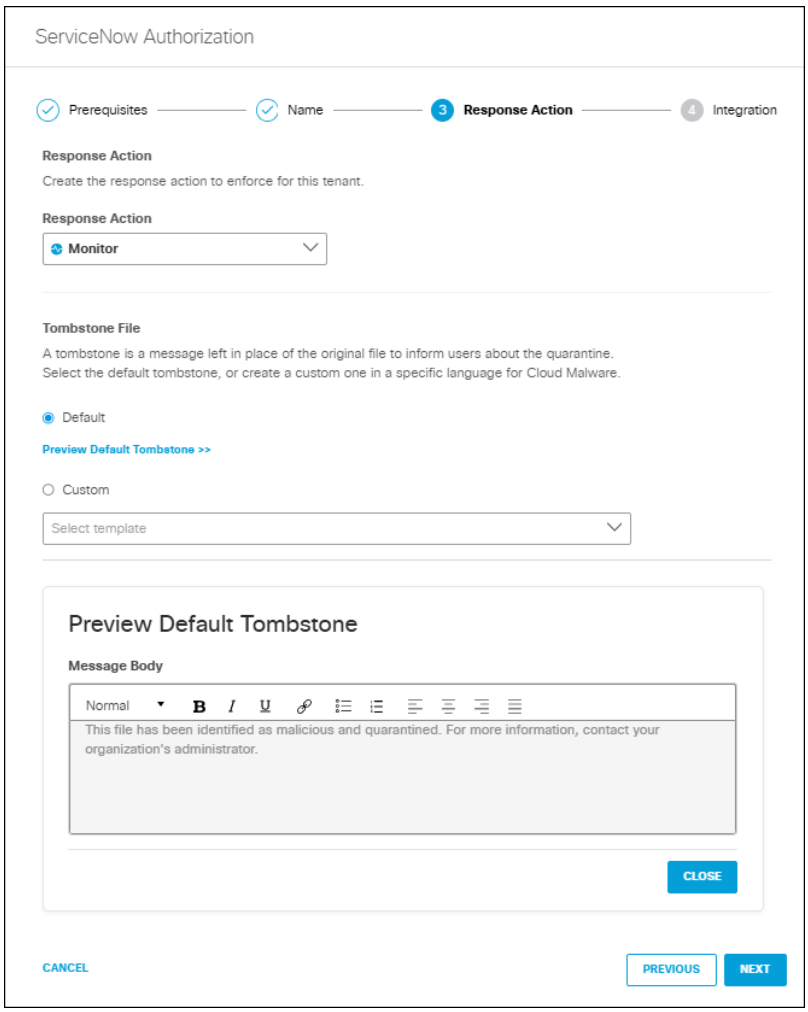
5. Define the message to appear in the footprint attached to the notesactivities area of the table the quarantined file was originally attached to.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a footprint as described in the previous step. You determine the contents of this footprint using a *tombstone template*:

   - **To Use the Default Tombstone Template:**

     a. Click **Default**.

     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

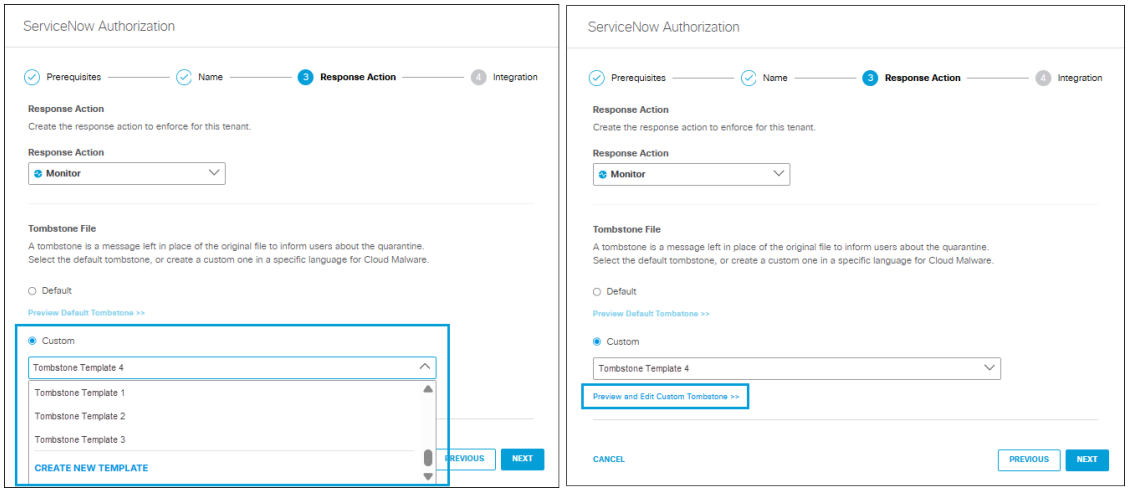


c. Click **CLOSE** to close the preview.

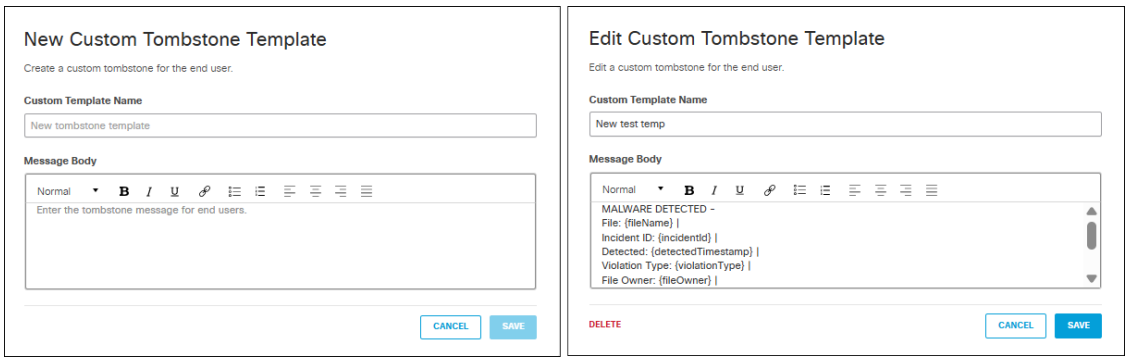
- **To Use a Custom Tombstone Template:**

a. Click **Custom**.

b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

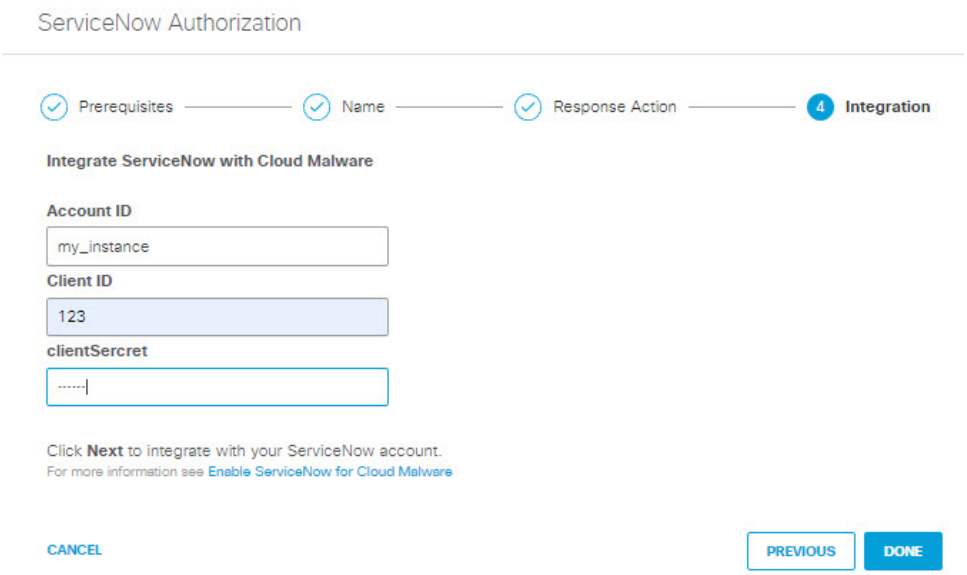
   The text can include the following variables, which you must enclose in braces (**{}**):

   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
   - **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{fileLocation}** - The file URL.

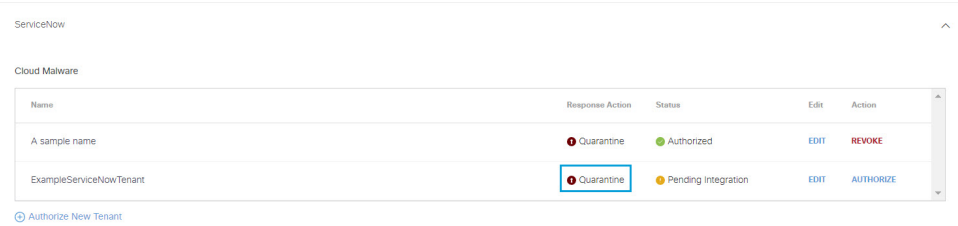
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

6. Enter the following and then click **Done**:
   - **Account ID**: Enter the Instance Name for your ServiceNow account.
   - **Client ID**: Enter the **Name** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.
   - **Client Secret**: Enter the **Client Secret** you supplied in Step 3 of Add an OAuth Client to Your ServiceNow Deployment.



7. The new **Response Action** is displayed.

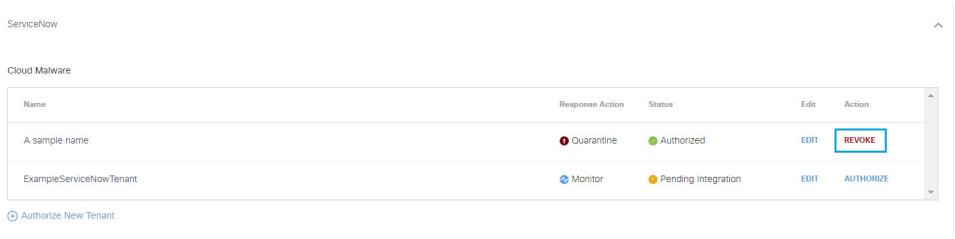


Revoke Authorization

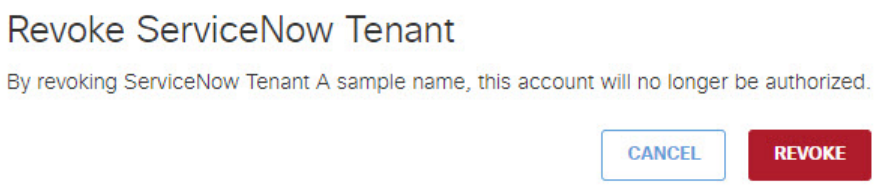
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. For **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Click **Revoke**. The selected account is no longer authorized.



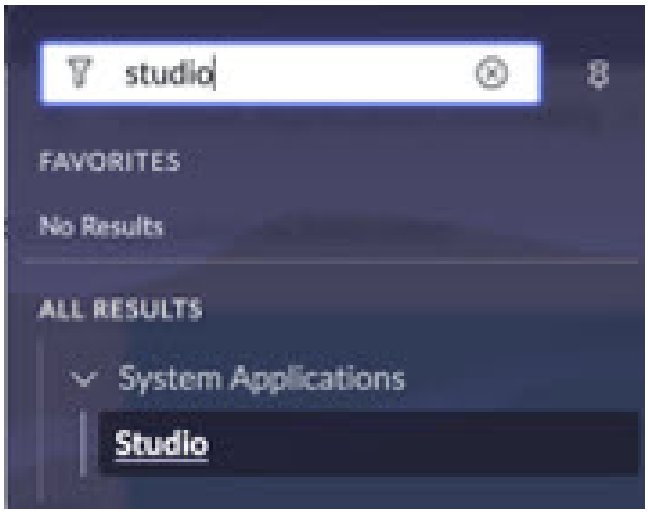
View the Cisco Quarantine Table in Service Now

Provides instructions for completing the View the Cisco Quarantine Table in Service Now workflow in Cisco Secure Access. ServiceNow maintains information about quarantined files in a table called Cisco Quarantine.

ServiceNow maintains information about quarantined files in a table called **Cisco Quarantine**. Perform these steps in your ServiceNow IT Service Management portal to create an application you can use to view that table:

Procedure

1. Filter for **Studio**. Under **System Applications** click on **Studio**.



2. In the Studio interface, click **Create Application**.
3. In the screens that follow, choose the following characteristics for your new application:
   a. Provide an application **Name** and **Description**.

Under **Advanced settings** choose **Global**.

Click **Create**.

b. Under **Roles**, select **ais_high_security_admin**.

Click **Continue**.

c. For **Format** select **Classic**.

Click **Continue**.

d. For **Data tables** select **Cisco Quarantine [u_cisco_quarantine]**.

Click **Done with tables**.

4. On the page titled **It's time to design your apps**, click **Start** to the right of the listing for your new application.
5. On the page titled **Let's customize the design of your Classic App**, click **Create**.

Enable Cloud Malware Protection for Slack Tenants

Describes Enable Cloud Malware Protection for Slack Tenants in Cisco Secure Access. Secure Access supports Cloud Malware protection for all messages and files within your Slack deployment.

Secure Access supports Cloud Malware protection for all messages and files within your Slack deployment.

Prerequisites

- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- You must have an active Slack tenant and Slack admin privileges (co-admin does not have sufficient privileges).

Limitations

- A tenant that fails to authenticate cannot be deleted.

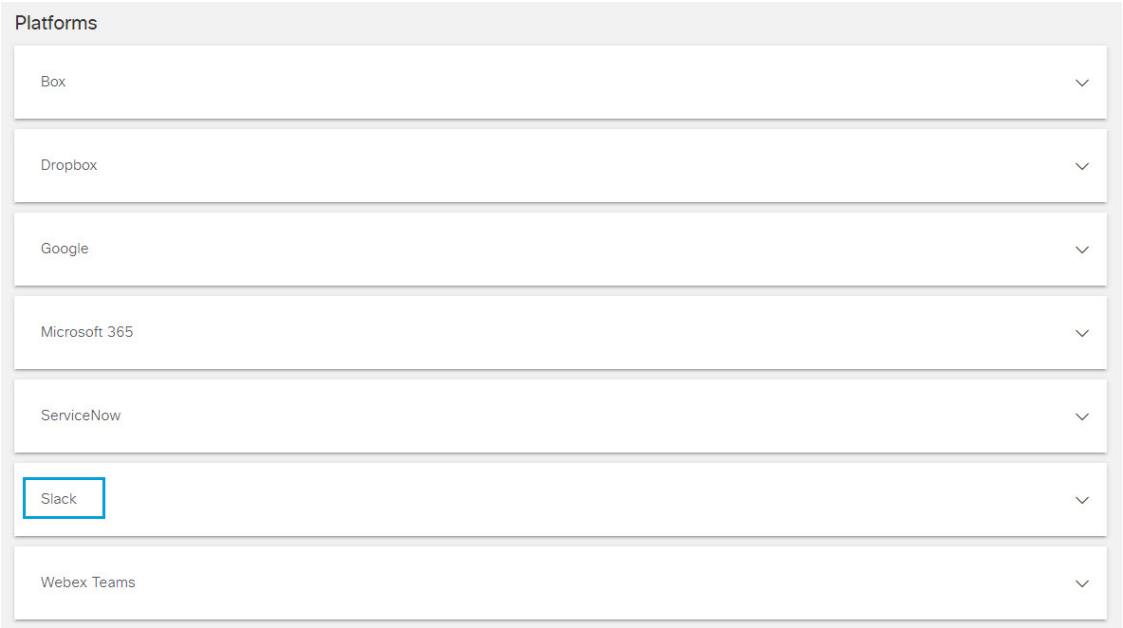
Authorize a Tenant

Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

---

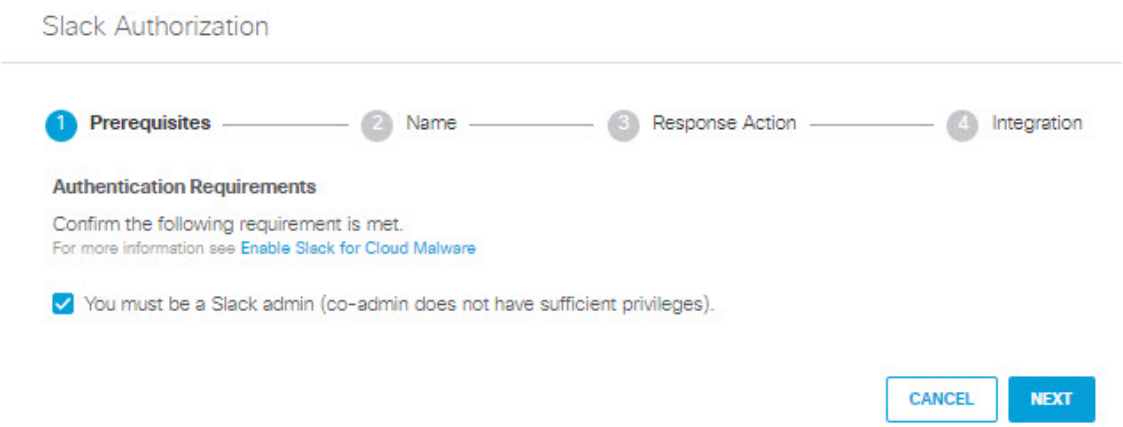
1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Slack**.



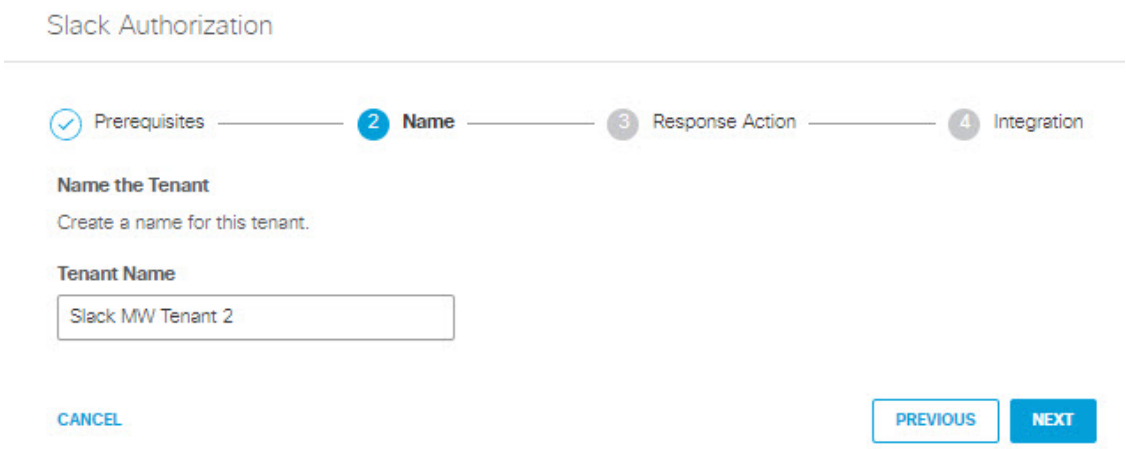
3. In the **Cloud Malware** section, click **Authorize New Tenant** to add a Slack tenant to your Secure Access environment.



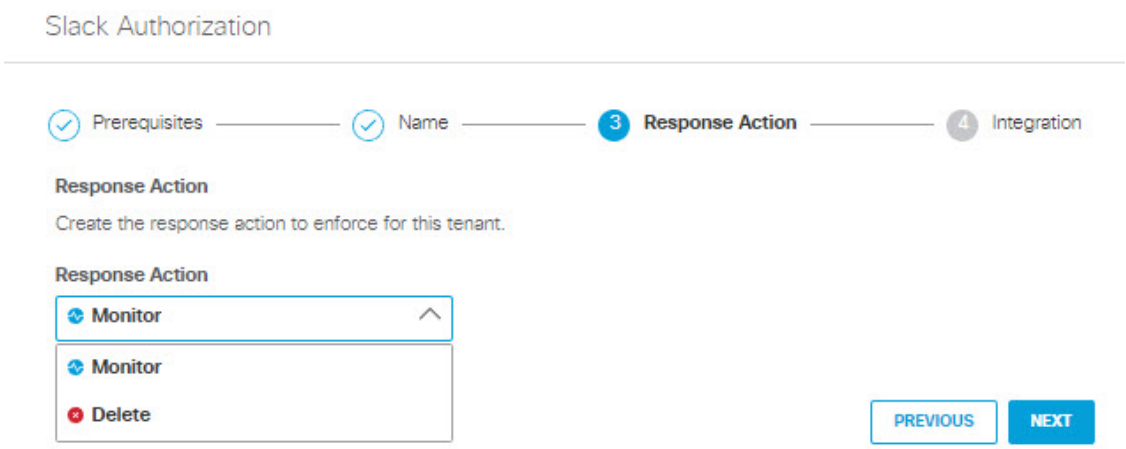
4. In the **Slack Authorization** dialog box, check the checkbox to verify you meet the prerequisite and then click **Next**.



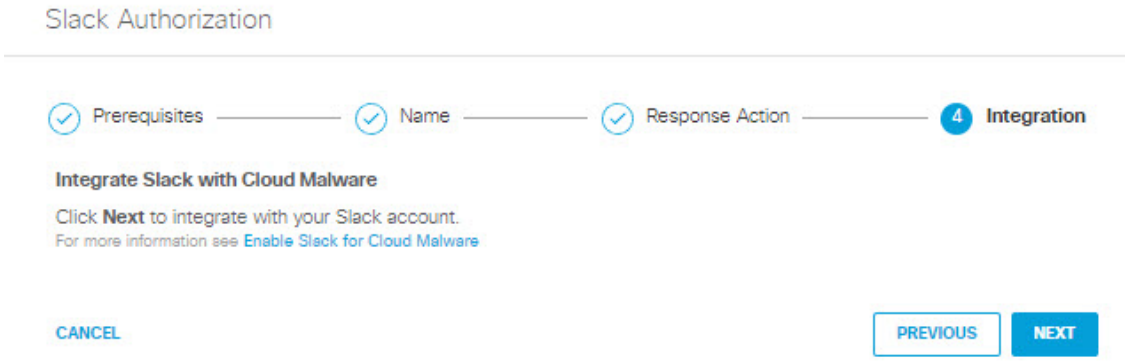
5. Add a **Tenant Name** and then click **Next**.



6. Select a **Response Action** for Secure Access to automatically apply to Slack messages and files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log messages and files detected with malware. You will be able to manually delete these from the Cloud Malware report.
   - Choose **Delete** to automatically delete the message or file.



7. Click **Next** to integrate with Slack.



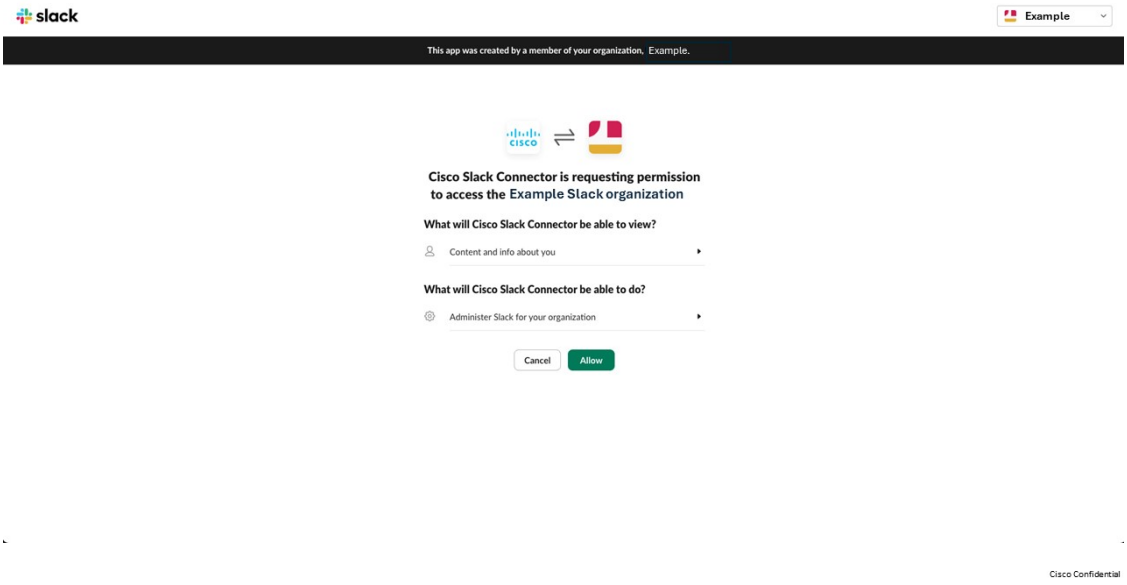
8. If you are not already logged in, the Slack login page will appear; log in to Slack with admin credentials to grant access.



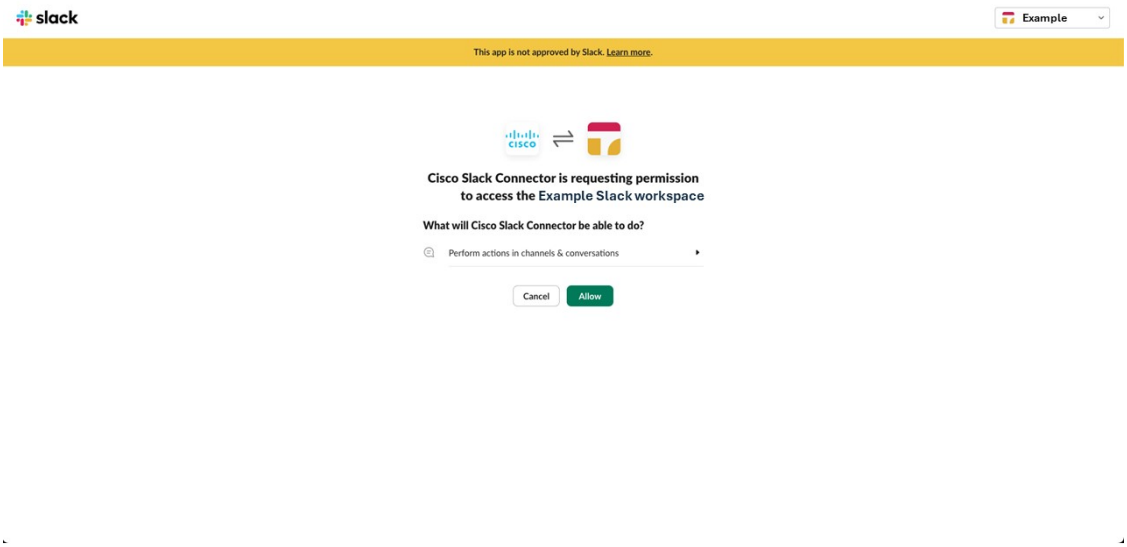
If you are already logged in to Slack with admin credentials, the Slack login page does not appear; proceed to Step 9.

9. Screens with prompts from Slack will appear .

a. Click **Allow** to authorize the Cisco Slack Connector to view content and information about your Slack account, and to administer Slack for your account.

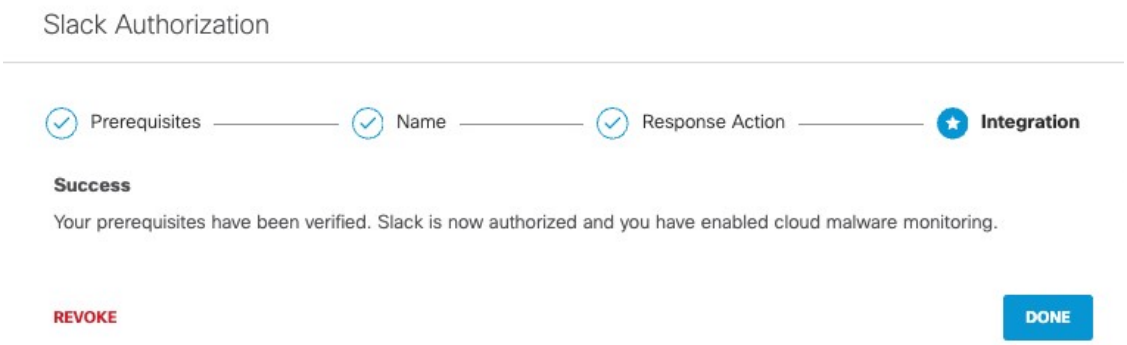


b. Click **Allow** to authorize the Cisco Slack Connector to perform actions in channels and conversations associated with your Slack account.



Cisco Confidential

10. You are redirected to Secure Access and a message appears showing the integration was successful. (It may be up to 24 hours for the integration to be confirmed and appear as **Authorized** in the Platforms section of the Authentication page.)
11. Click **Done**.



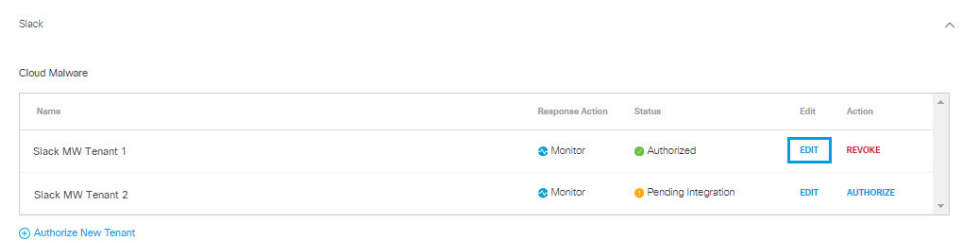
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the Response Action you have selected for a tenant.

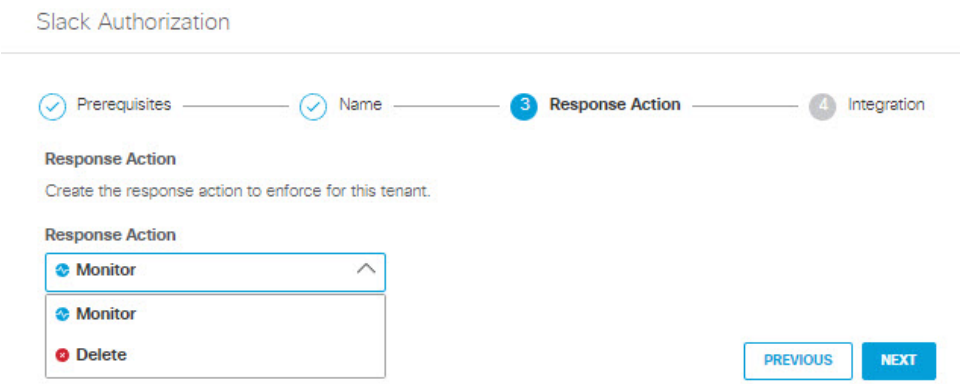
You can change the Response Action you have selected for a tenant.

Procedure

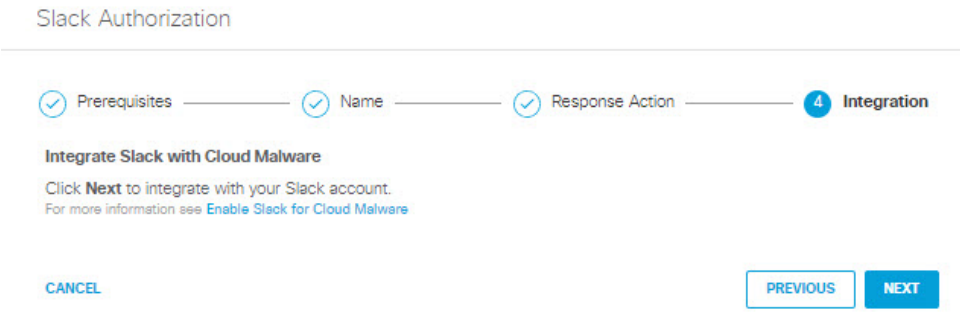
1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Slack**.
3. In the **Cloud Malware** section , from the **Edit** column, click **Edit**. You can edit any tenant.



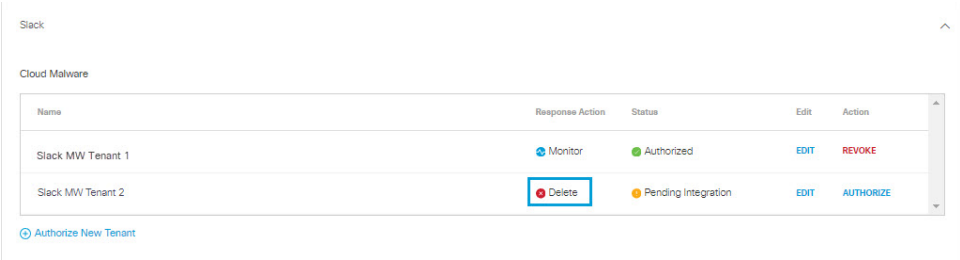
4. Select a **Response Action** for Secure Access to automatically apply to Slack messages and files found with malware and then click **Next**.
   - Choose **Monitor** to cause Secure Access to log messages and files detected with malware. You will be able to manually delete these from the Cloud Malware report.
   - Choose **Delete** to delete the message or file.



5. Click **Next**.



The new **Response Action** is displayed.

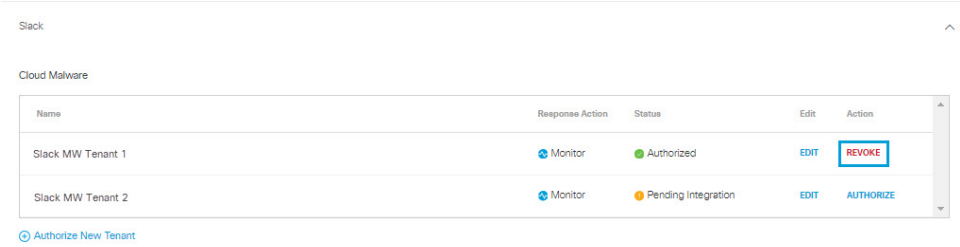


Revoke Authorization

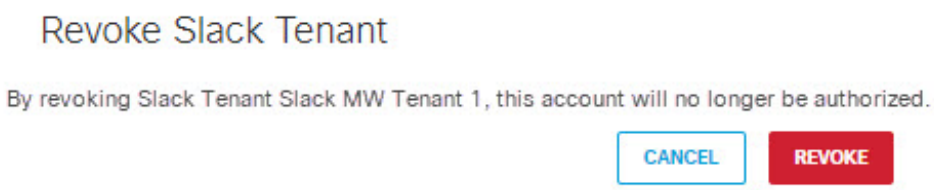
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Admin** > **Authentication**.
2. In the **Platforms** section, click **Slack**.
3. From the **Action** column, click **Revoke**. You can revoke any authorized tenant.



4. Click **Revoke**. The selected account is no longer authorized.



Enable Cloud Malware Protection for Webex Teams

Describes Enable Cloud Malware Protection for Webex Teams in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

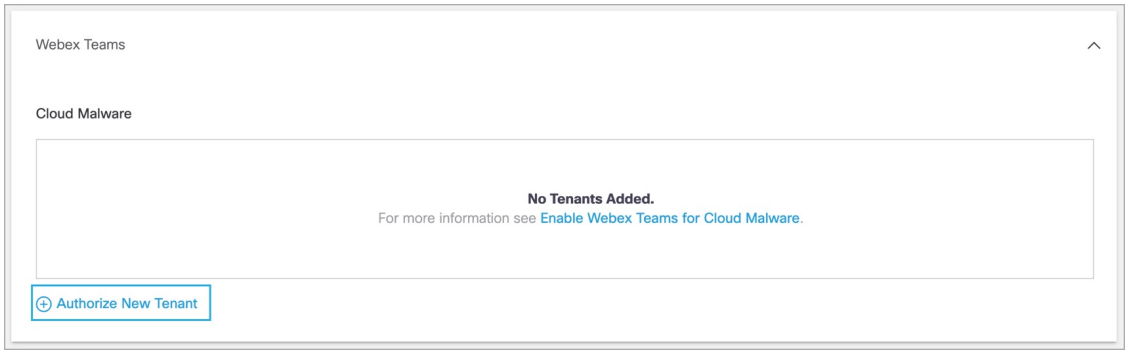
- Full Admin user role. For more information, see Manage Accounts.
- Chrome or Firefox (recommended) with pop-up blockers and ad blockers disabled (only for the duration of authorization)
- Full Administrator Privileges in Webex Teams and the Compliance Officer role
- The `EventsAPI` in your Webex Teams instance must be enabled. Contact your Webex Teams support team to ensure that the `EventsAPI` is turned on.

Authorize a Tenant

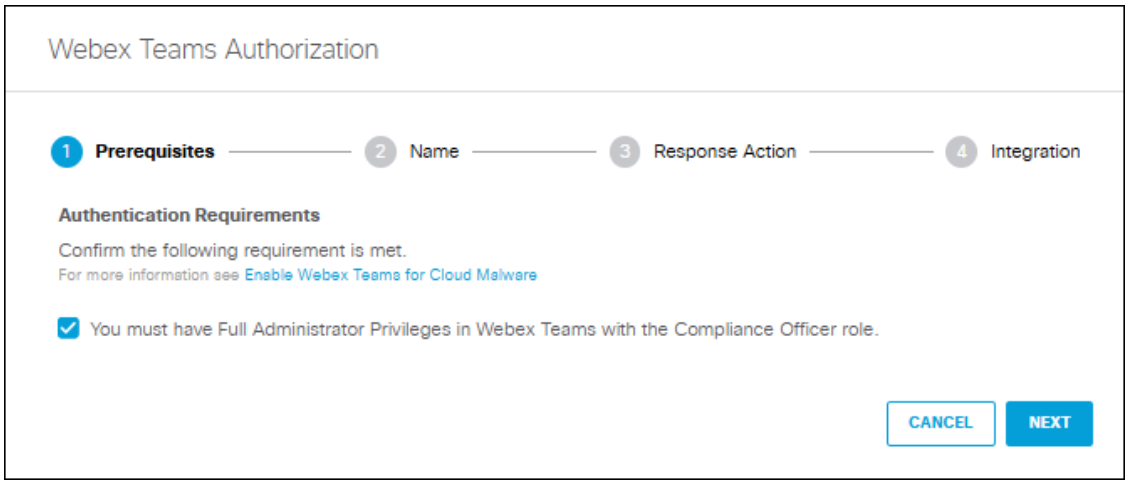
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

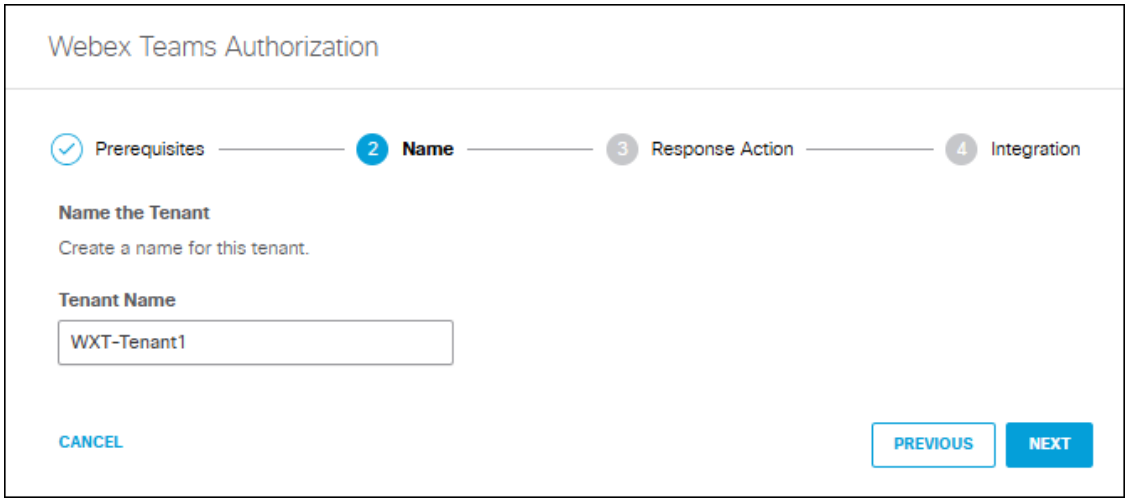
1. Navigate to **Admin** > **Authentication**.
2. Under **SaaS API Platforms**, click **Webex Teams**.
3. In the Cloud Malware subsection, click **Authorize New Tenant** to add a Webex Teams tenant to your Secure Access environment.



4. In the **Webex Teams Authorization** dialog, check the checkbox to verify you meet the prerequisite, then click **Next**.

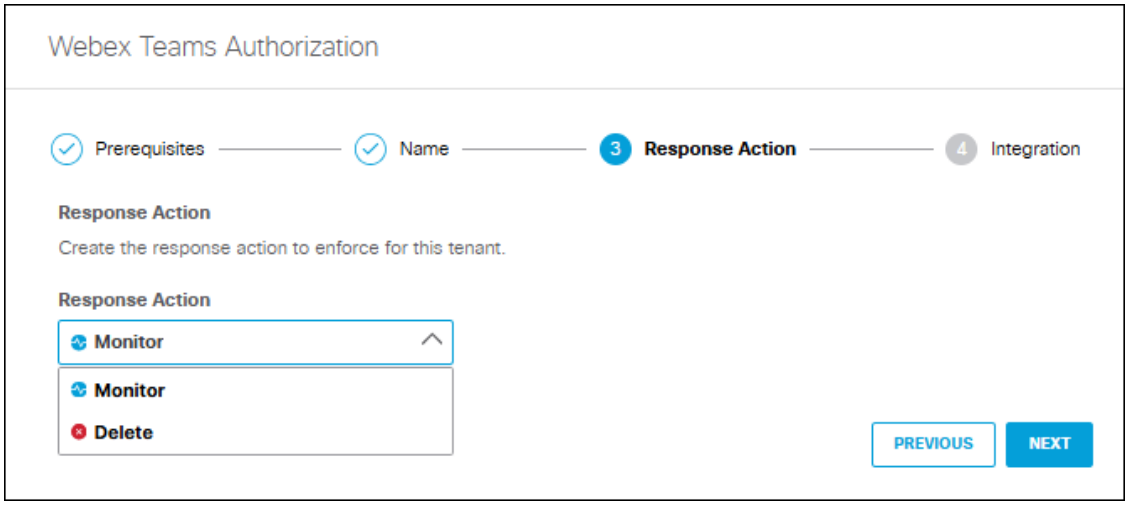


5. Enter the name of your tenant, then click **Next**.

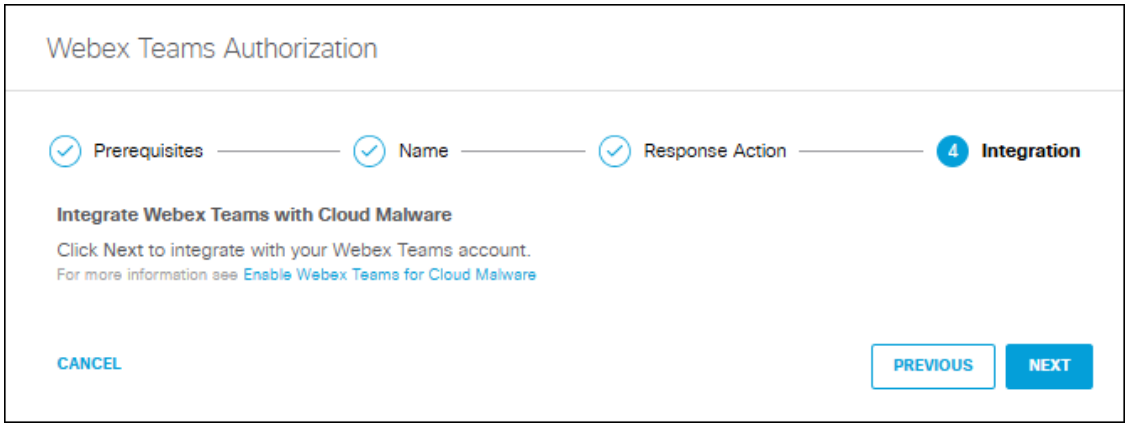


6. Select a **Response Action** for Secure Access to apply to Webex Teams files found with malware, then click **Next**.

- Choose **Monitor** to cause Secure Access to log messages and files detected with malware.You will be able to manually delete these from the Cloud Malware report.
- Choose **Delete** to cause Secure Access to automatically delete files detected with malware.



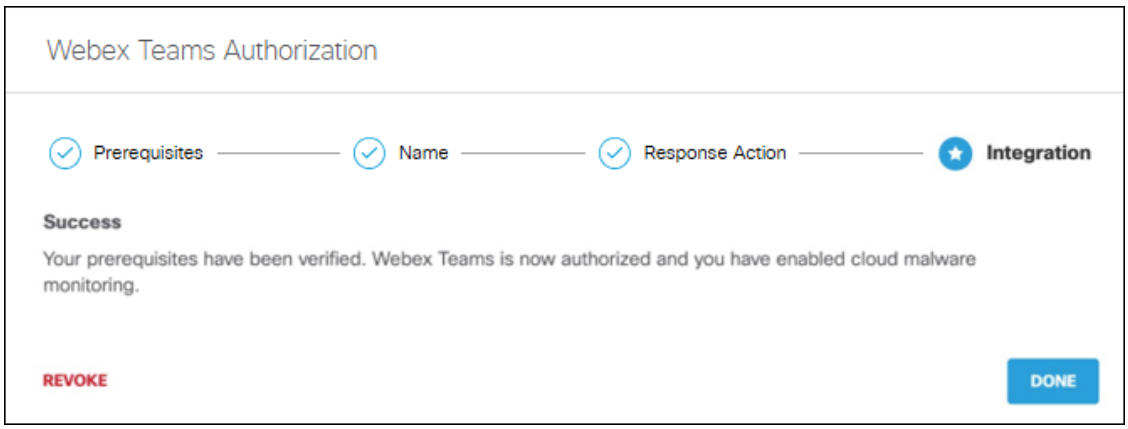
7. Click **Next** to complete the integration.



8. Enter your credentials and click **Sign in**.



9. You are redirected to Secure Access and a message appears showing the integration was successful. It may be up to 24 hours for the integration to be confirmed and appear as Authorized. Click **Done**.

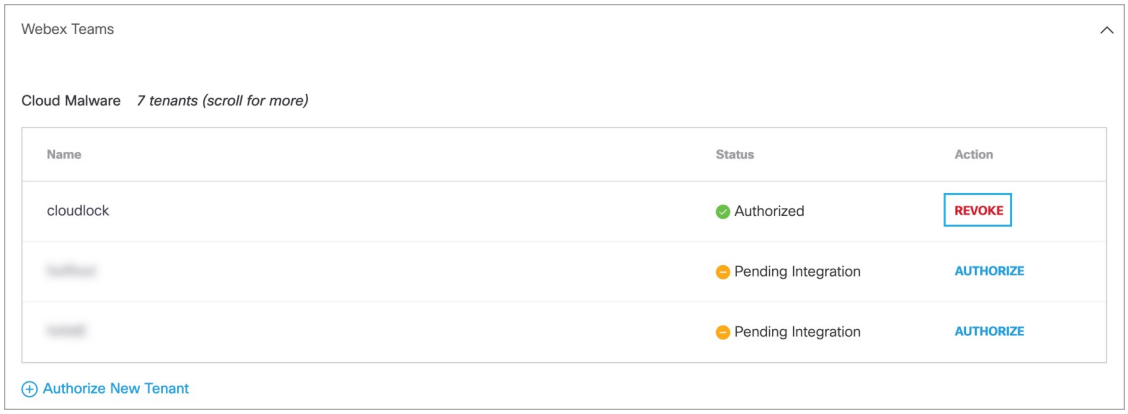


Revoke Authorization

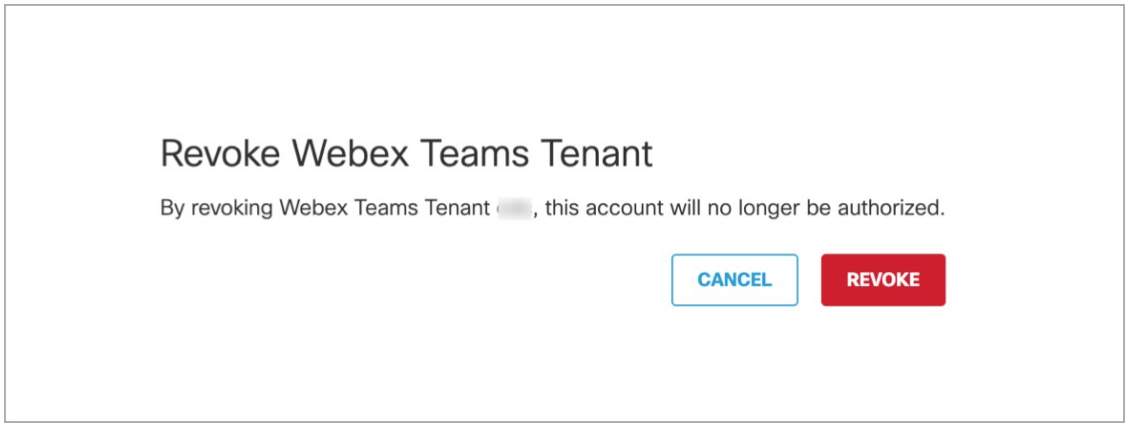
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected account is not authorized.



Cloud Access Security Broker Protection for Google Drive and Microsoft 365

Describes Cloud Access Security Broker Protection for Google Drive and Microsoft 365 in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

In addition to Cloud Malware protection for your Google Drive deployment and Outlook, OneDrive and SharePoint Online sites within your Microsoft 365 deployment, Secure Access supports detection of third-party cloud applications that have been granted OAuth-based permission to access a user's protected resources on sanctioned Google Drive and Microsoft 365 tenants. For more information, see Enable Cloud Access Security Broker Features for Google Drive and Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants.

Note

Third-party application detection is not supported for Microsoft Outlook.

Enable Cloud Access Security Broker Features for Google Drive

Describes Enable Cloud Access Security Broker Features for Google Drive in Cisco Secure Access and explains Prerequisites and Limitation. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access supports two Cloud Access Security Broker (CASB) features for Google Drive:

- Cloud Malware protection.
- Detection of third-party cloud applications that have been granted OAuth-based permission to access a user's protected resources on Google Drive. For more information, see Third-Party Apps Report.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- The person performing the authentication *must* be a Google Super Admin and have an active Google user license.
- Chrome or Firefox is recommended with pop-up blockers/ad blockers disabled (only for the duration of authorization).
- Secure Access DLP Connector (also known as the SaaS API Connector) must be installed in the tenant by a Google Admin User. We recommend using a service account for the installation.
- For third-party app support, your Google Drive tenant scopes for admin.report.audit.readonly and admin.reports.usage.readonly must be enabled.

Limitation

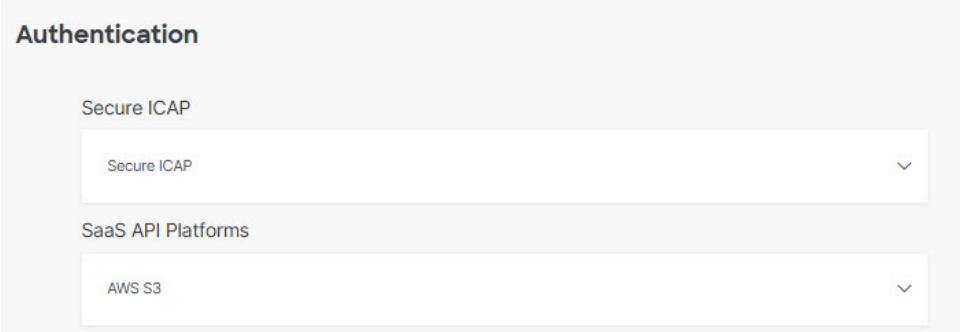
- A tenant that fails to authenticate cannot be deleted.

Authorize a Tenant

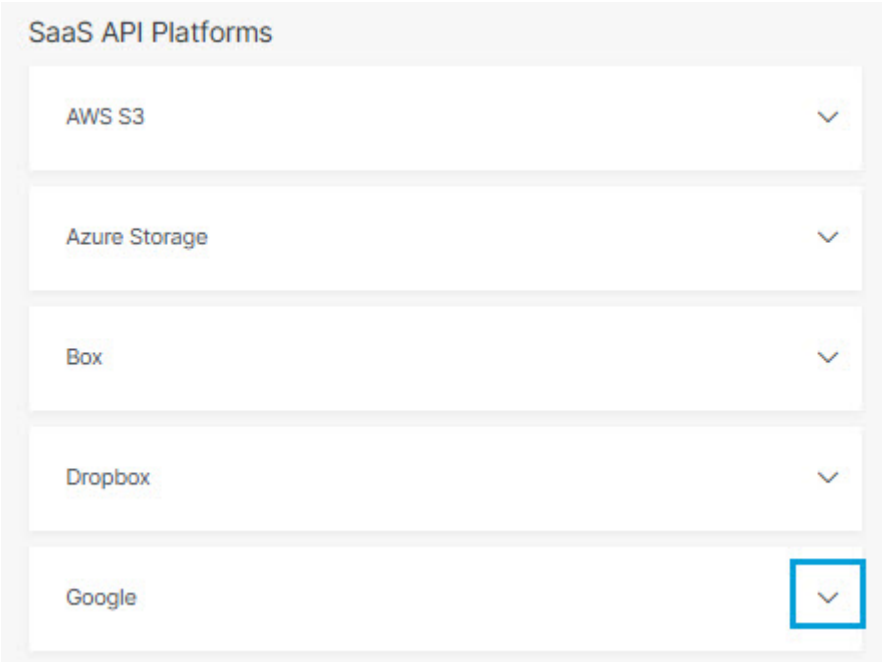
Provides instructions for completing the Authorize a Tenant workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

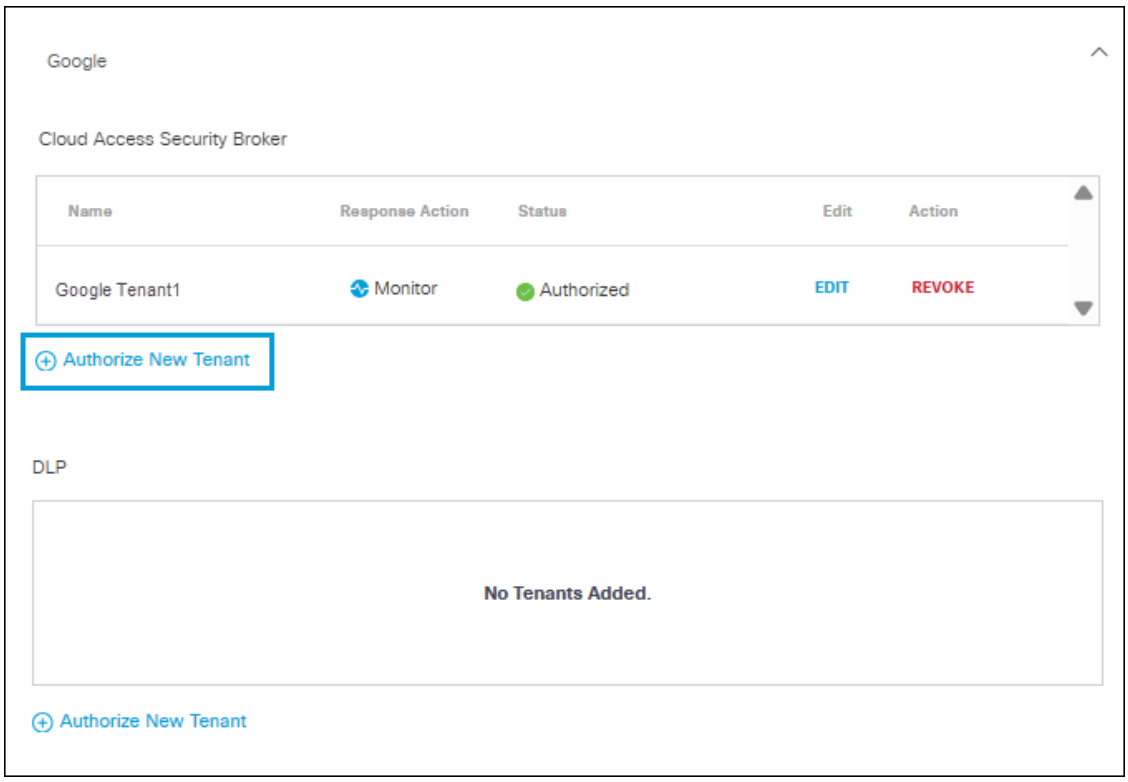
1. Navigate to **Admin** > **Authentication**.



2. Under **SaaS API Platforms**, click to expand **Google**.

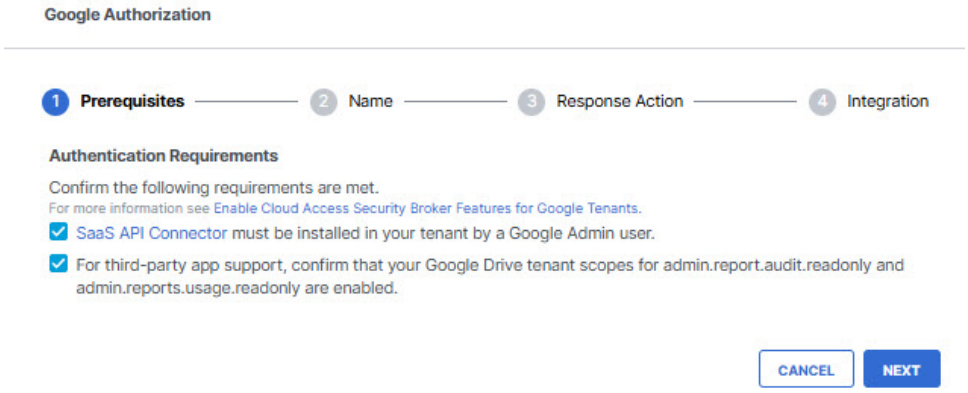


3. Under **Cloud Access Security Broker** click **Authorize New Tenant** to add a Google tenant to your Secure Access environment.

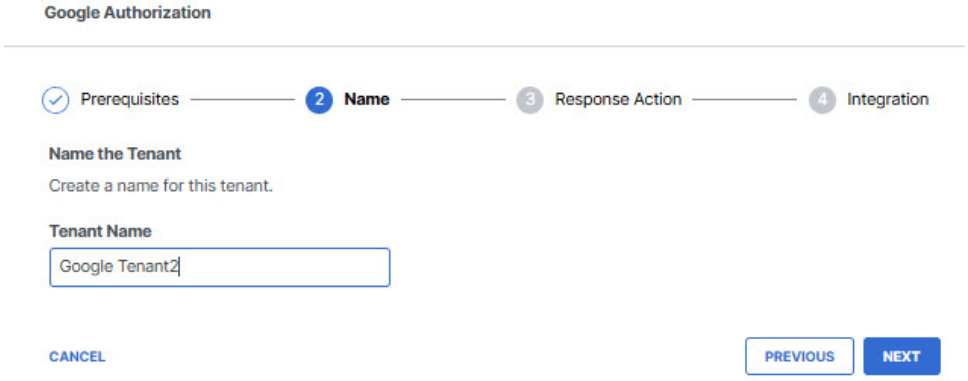


4. In the **Google Authorization** dialog box, check the checkboxes to verify you meet the prerequisites, then click **Next**.

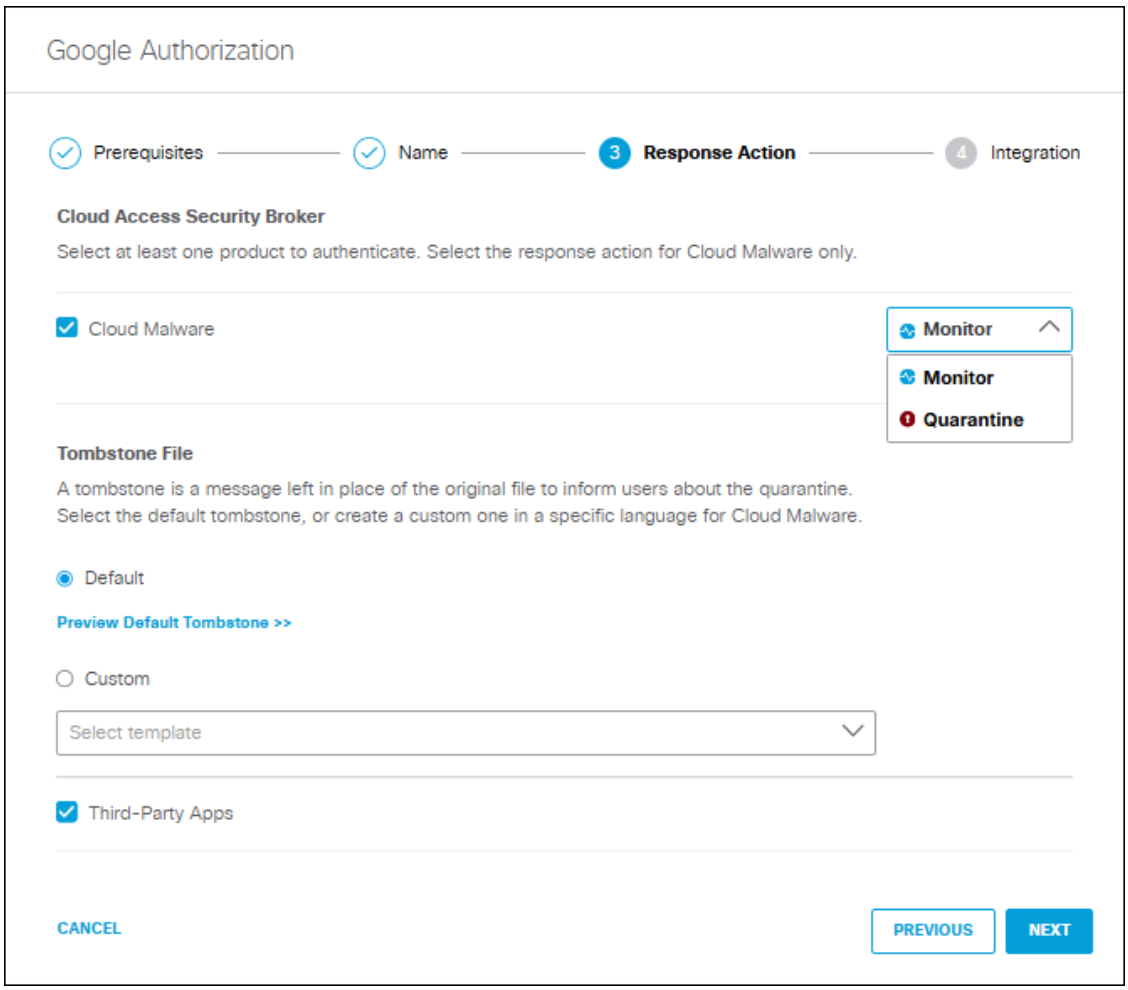
> **Note**
>
> The link to the SaaS API Connector brings you to the Umbrella DLP Connector site in the Google Workspace Marketplace. This is correct, despite the nomenclature difference.



5. Provide a name for your tenant, then click **Next**.



6. Choose to authorize your Google Drive tenant for Cloud Malware protection, or CASB detection for third-party cloud applications, or both.



If you choose to authorize for Cloud Malware protection, you must also select a **Response Action** for Secure Access to apply to Google Drive files found with malware.

- Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
- Choose **Quarantine** to:
  - Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Google admin.
  - Replace the file in its original location with a text file named *`filename`*`.ppt_Cisco_Quarantined.txt` explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

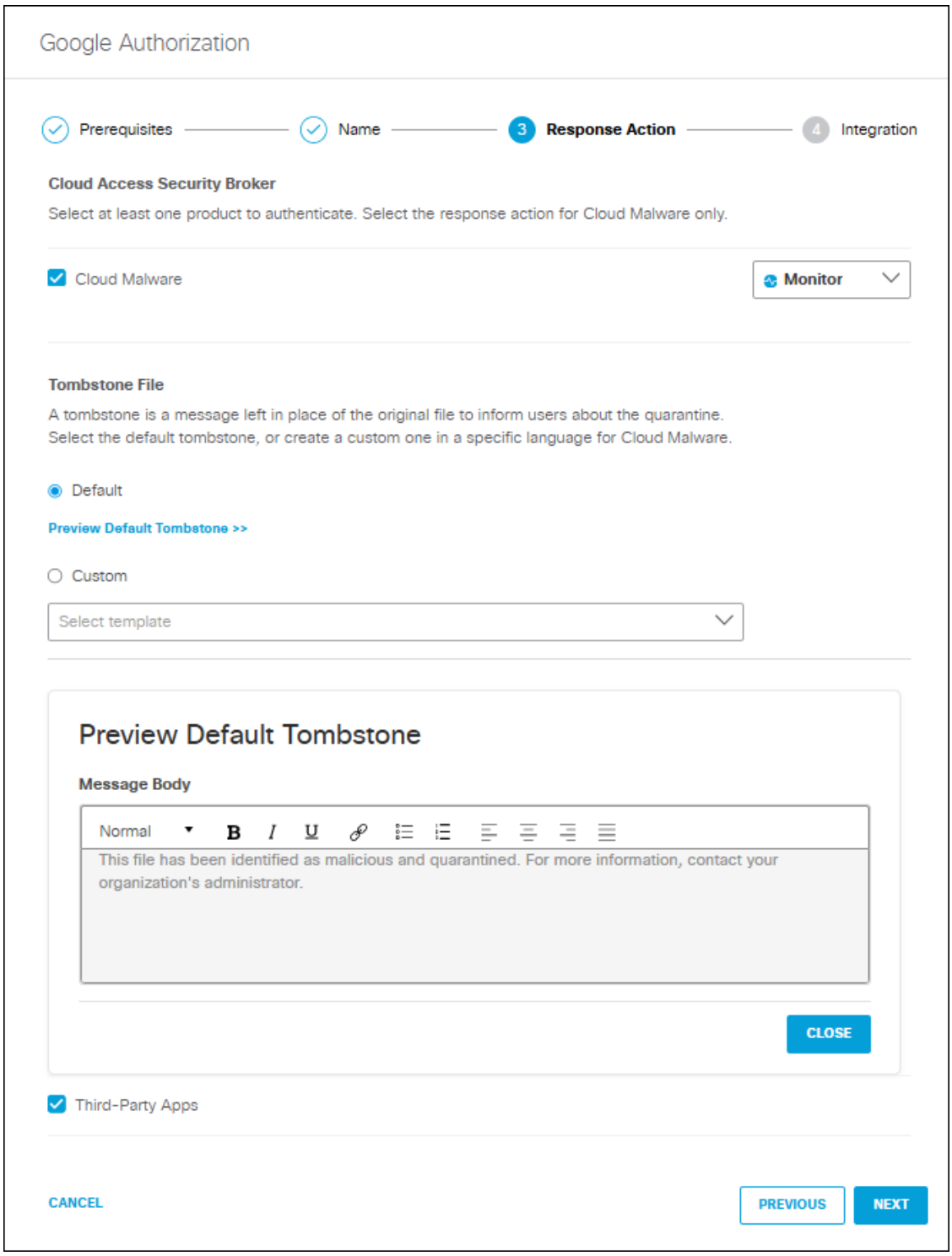
After making your selections, click **Next**.

7. Define the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**
     a. Click **Default**.

b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

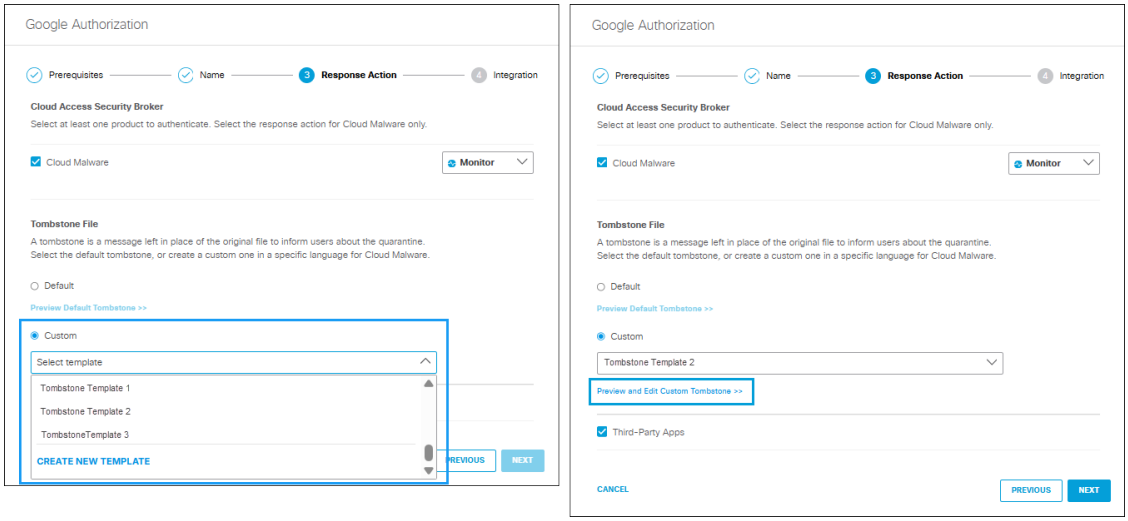


c. Click **CLOSE** to close the preview.

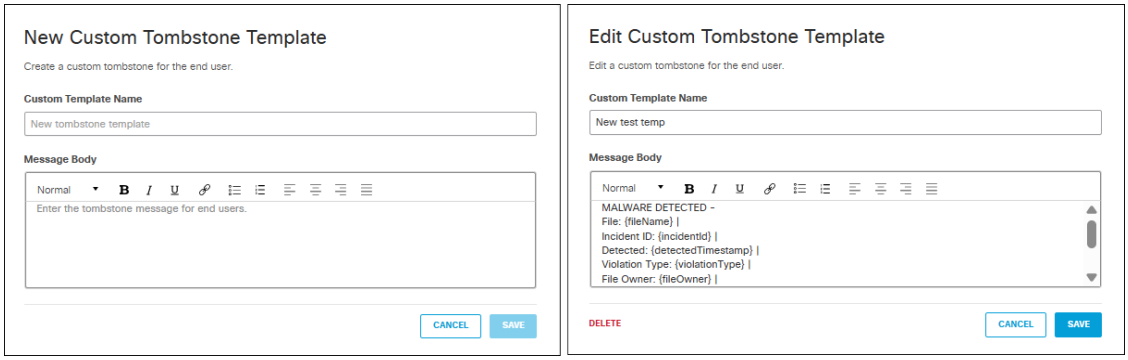
- **To Use a Custom Tombstone Template:**

a. Click **Custom**.

b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.



c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:



The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

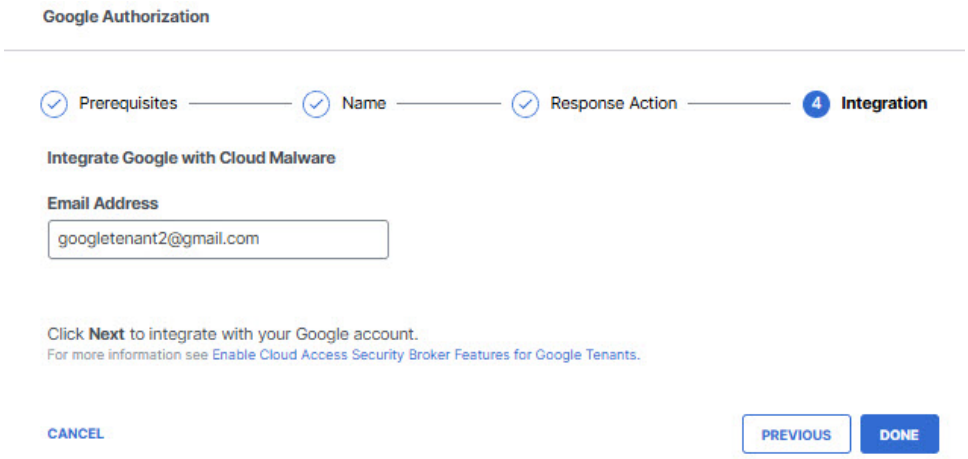
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.

- **{ruleName}** - Name of the rule that was triggered.
- **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)
- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

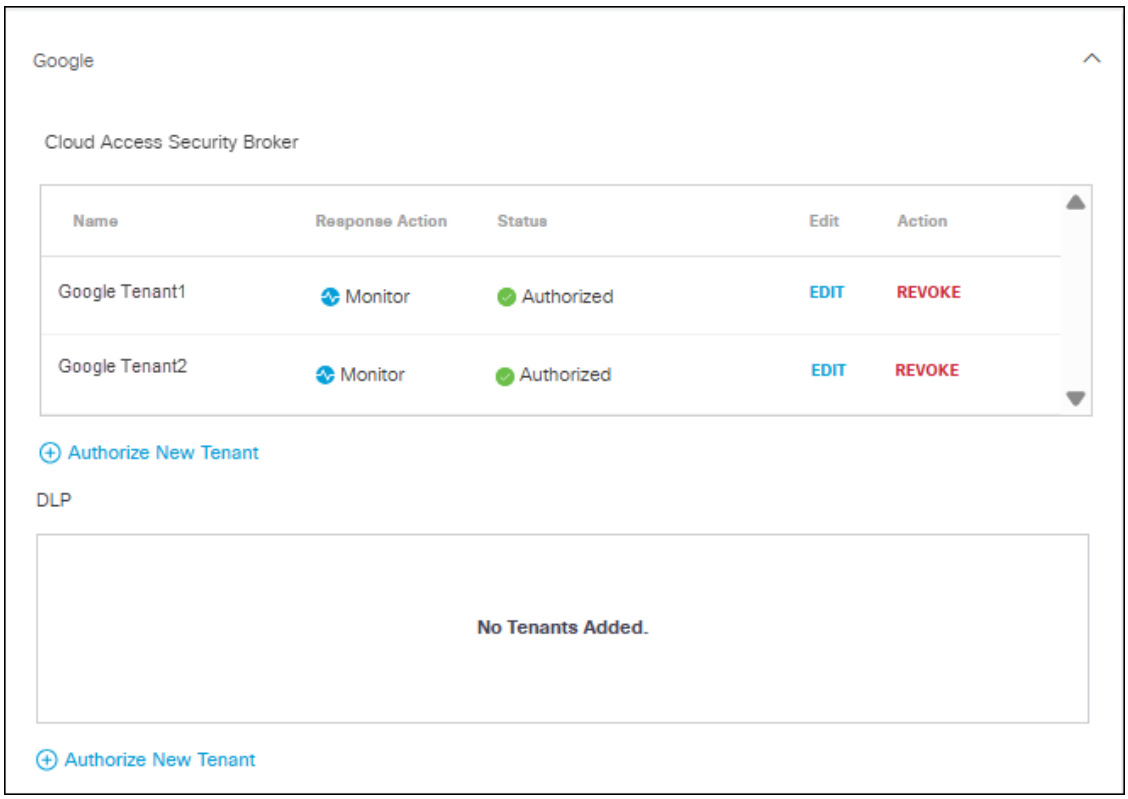
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

8. Click **Next** to proceed to **Integration**.
9. Enter a valid gmail address and then click **Done**.



10. The new tenant will appear in the list under **Cloud Access Security Broker**.



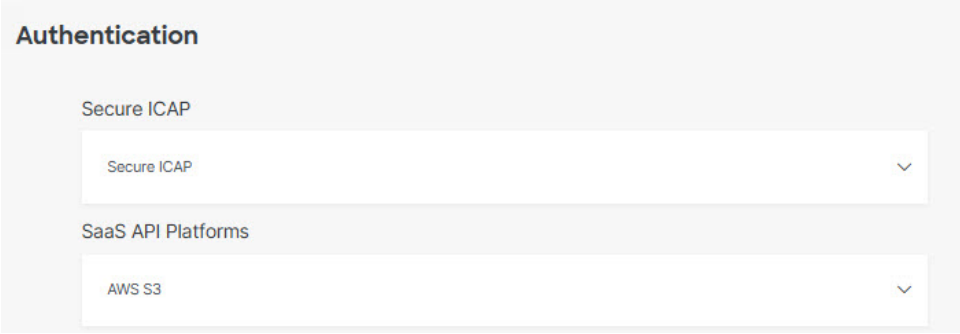
Edit a Tenant

Provides instructions for completing the Edit a Tenant workflow in Cisco Secure Access. You can change the Response Action you have selected for a tenant.

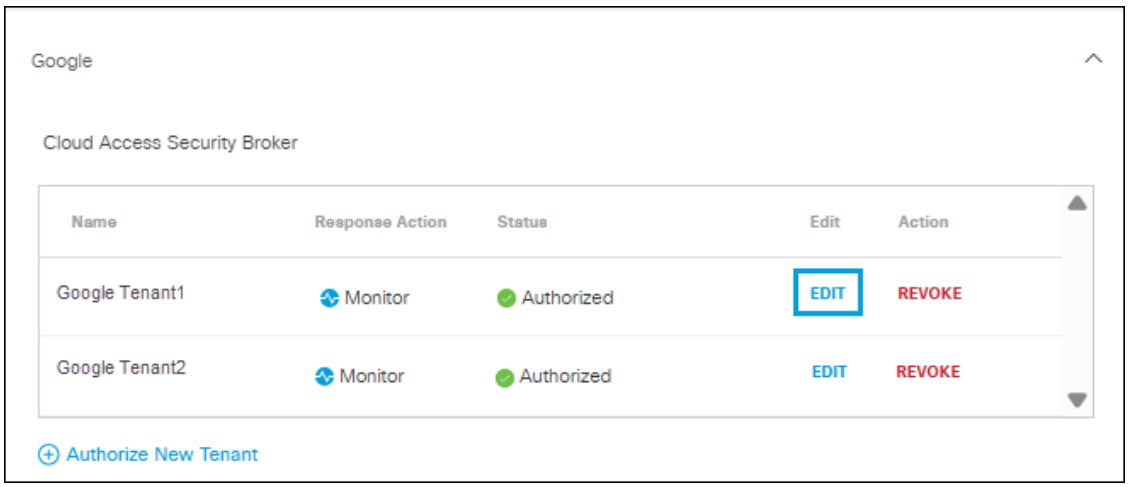
You can change the Response Action you have selected for a tenant.

Procedure

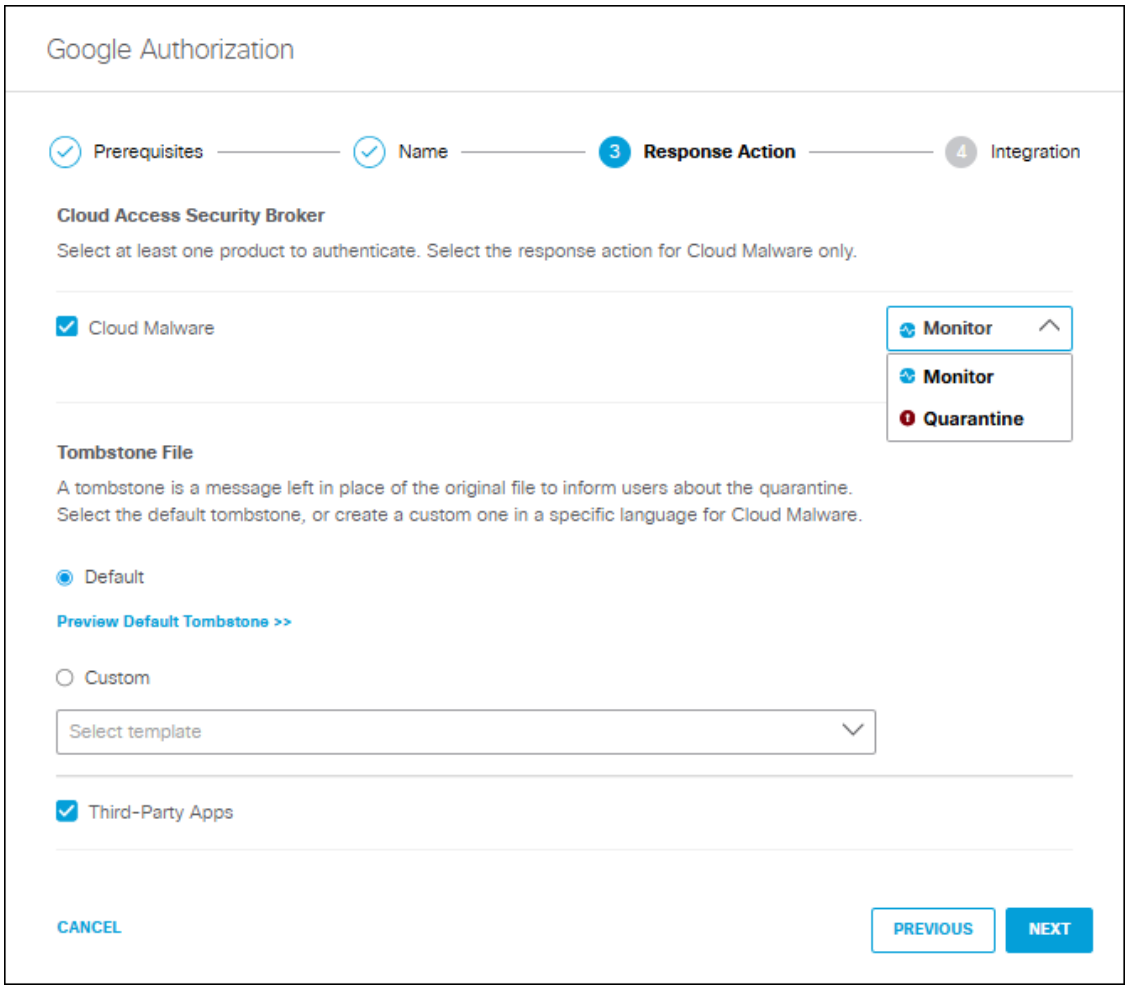
1. Navigate to **Admin** > **Authentication**.



2. Under **SaaS API Platforms**, click to expand **Google**.
3. In the **Cloud Access Security Broker** section , under **Action**, click **Edit**. You can edit any tenant.



4. Choose to authorize your Google Drive tenant for Cloud Malware protection, or CASB detection for third-party cloud applications, or both.



If you choose to authorize for Cloud Malware protection, you must also select a **Response Action** for Secure Access to apply to Google Drive files found with malware.

- Choose **Monitor** to cause Secure Access to log files detected with malware. You will be able to manually quarantine these files from the Cloud Malware report.
- Choose **Quarantine** to:

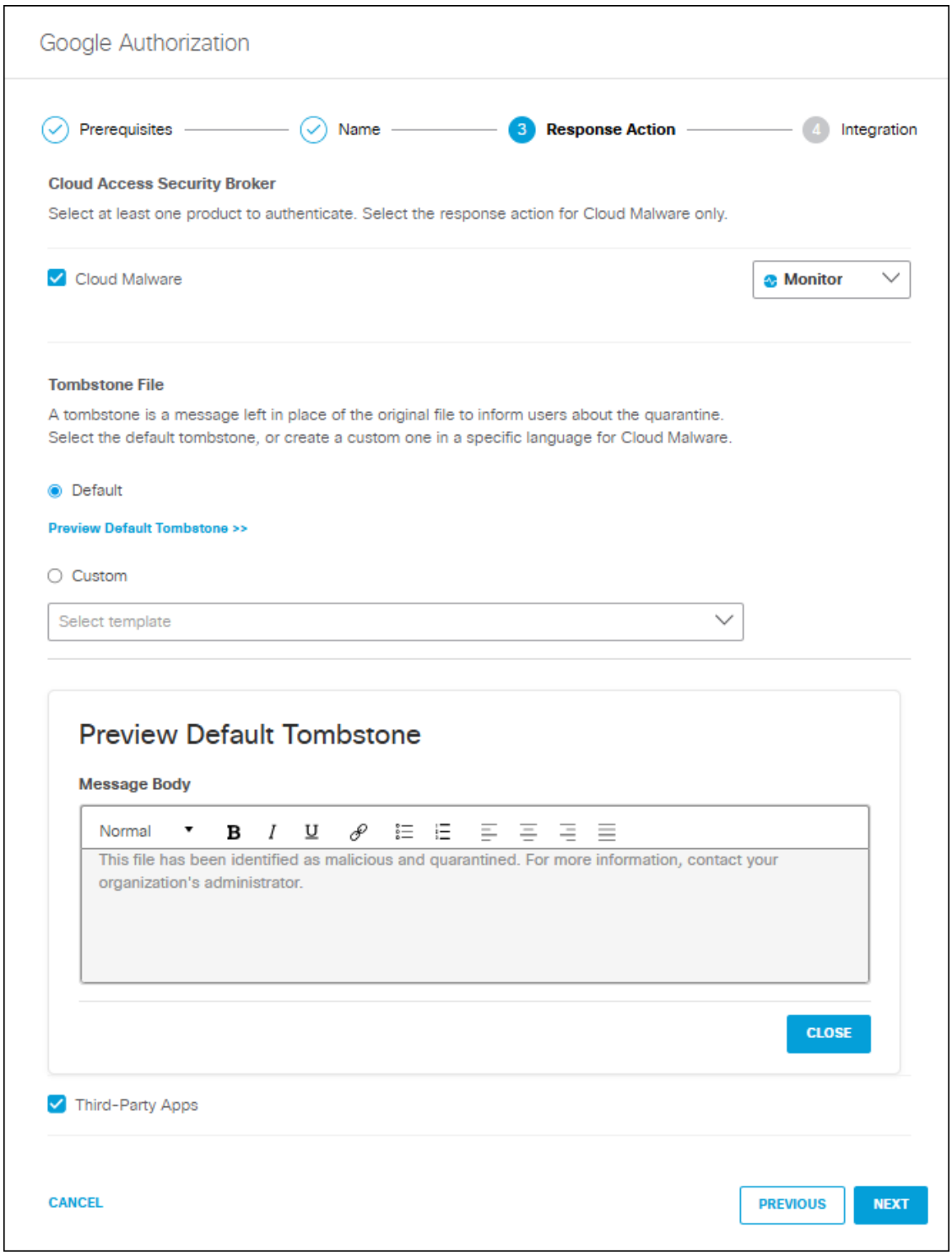
- Move the file into a folder named **Cisco_Quarantine_Malware** in the root path of the admin who authorized the tenant, remove all collaborators, and change the file owner to the Google admin.
- Replace the file in its original location with a text file named *filename*.ppt_Cisco_Quarantined.txt explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

After making your selections, click **Next**.

5. Change the message to appear in the **Tombstone File** when files are quarantined.

   A file with malicious content may be quarantined when first detected during the Cloud Malware scanning process, or the user may choose to manually quarantine a file when reviewing the Cloud Malware Report. In either case, when a file is quarantined Secure Access creates a tombstone file as described in the previous step. You determine the contents of this tombstone file:

   - **To Use the Default Tombstone Template:**
     a. Click **Default**.
     b. To preview the content of the tombstone text, click on **Preview Default Tombstone**. You can review the text, but you cannot change it.

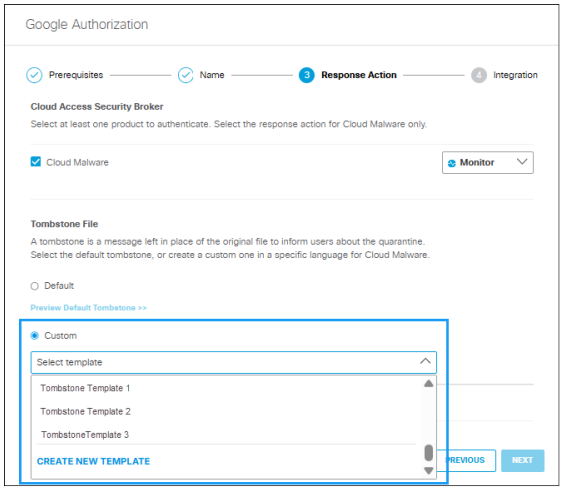


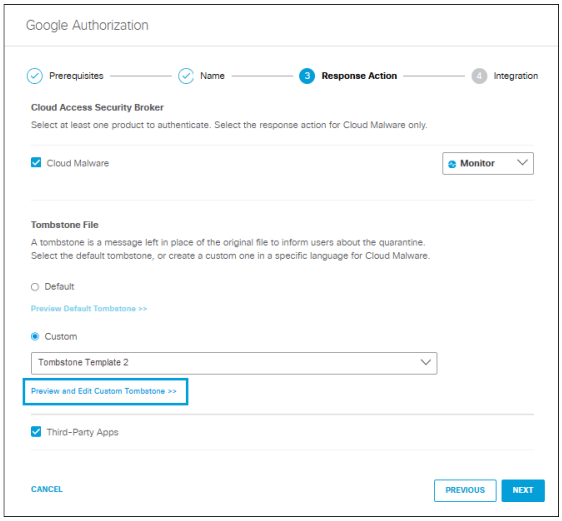
c. Click **CLOSE** to close the preview.

- **To Use a Custom Tombstone Template:**

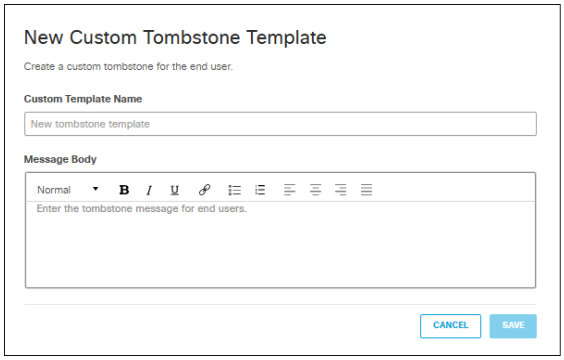
a. Click **Custom**.

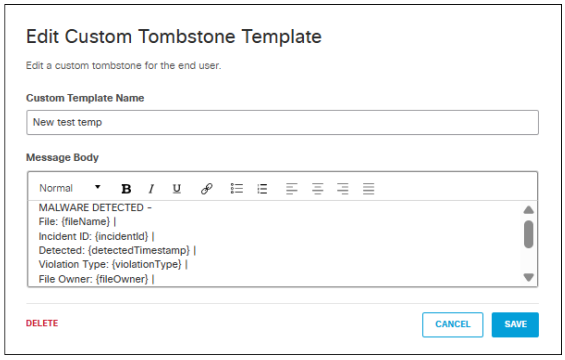
b. From the drop-down list, select an existing custom template, or choose **Create new tombstone Template**. If you select an existing custom template, you can click **PREVIEW AND EDIT** to review and change the template.





c. When you choose to create or edit a custom template for tombstone text you will see one of these two dialogs, which are almost identical:





The **Edit Custom Tombstone Template** includes a **DELETE** link which you can use to delete a custom template that is no longer needed. You cannot delete a template that is in use by any rule.

To create a new template or change an existing template:

1. Enter a unique **Custom Template Name**.
2. Enter the text of the tombstone file in the **Message Body** text box.

   The text can include the following variables, which you must enclose in braces (**{}**):

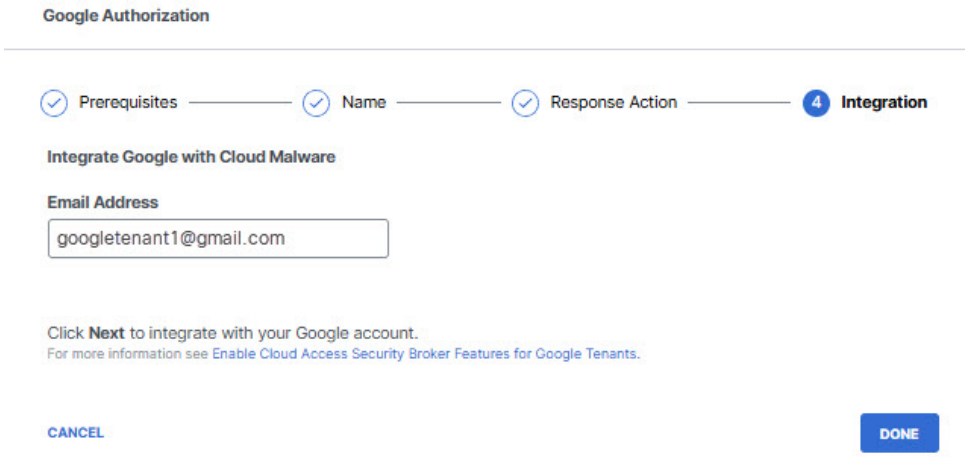
   - **{eventId}** - The unique identifier the system generates for the policy violation event.
   - **{detectedTimestamp}** - The date and time the violation was detected, formatted as shown in this example: "Oct 1, 2023 at 14:04 UTC"
   - **{actorName}** - Name of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
   - **{actorEmail}** - Email address of the user whose action triggered the violation. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the system replaces this variable with blank text.)
   - **{fileName}** - Name of the data file that triggered the violation.
   - **{ruleName}** - Name of the rule that was triggered.
   - **{matchedClassifications}** - The data classifications associated with the violation. (See Manage Data Classifications.)

- **{fileOwnerName}** - Name of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileOwnerEmail}** - Email address of the file owner. (The system gets this from the tenant associated with the violation. Depending on application and file settings, this information may not be available, in which case the the system replaces this variable with blank text.)
- **{fileLocation}** - The file URL.

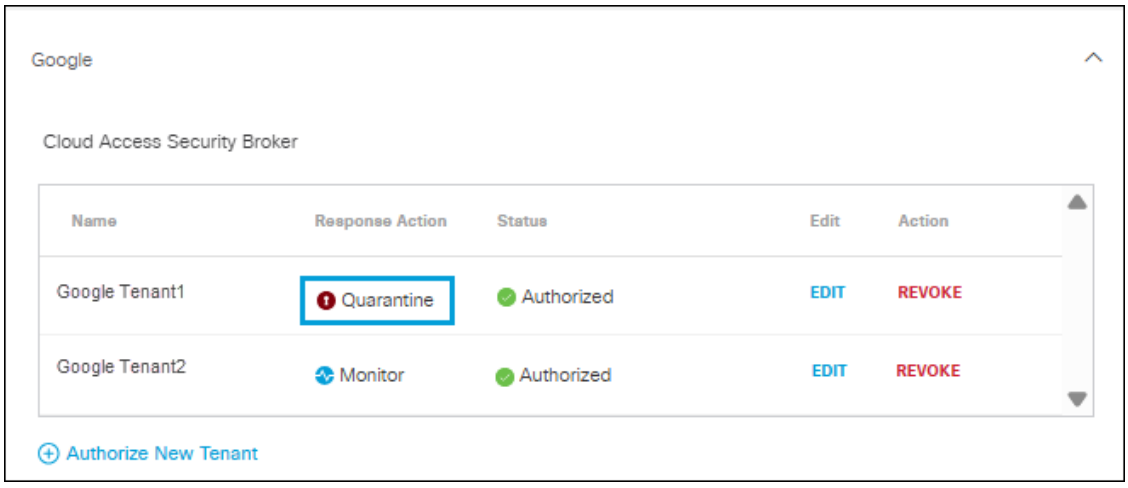
> **Note**
>
> The system replaces a variable with blank text if there is no value assigned to the variable or if an invalid variable name appears within the braces.

3. Click **SAVE** to complete the changes.

6. Click **Next** to proceed to **Integration**.
7. Click **Done** to continue.



8. The new **Response Action** is displayed.

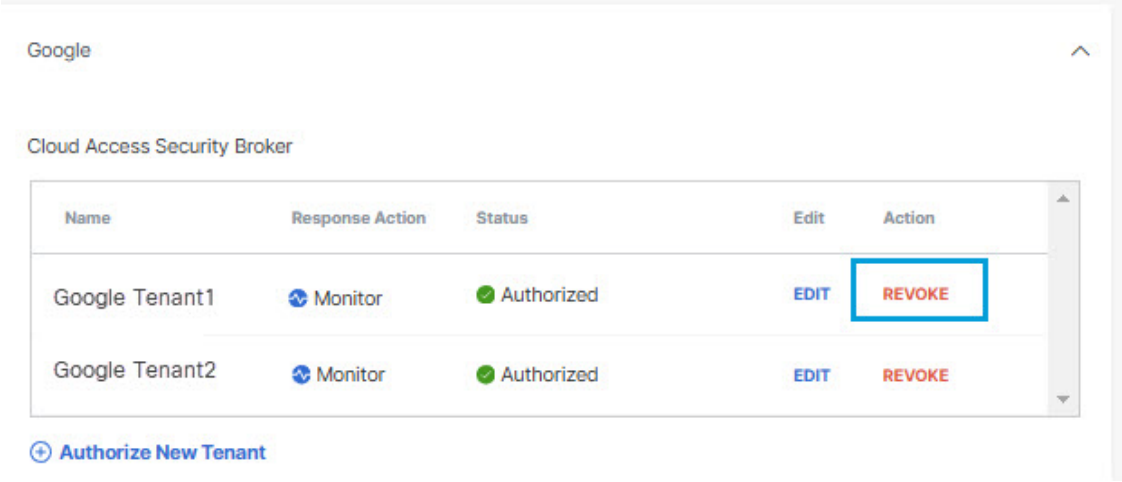


Revoke Authorization

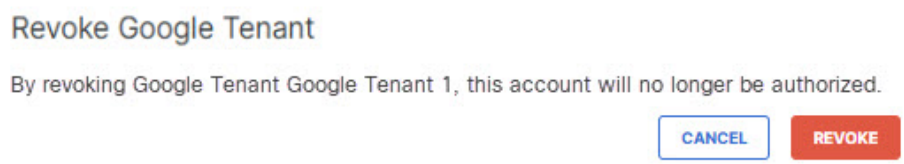
Provides instructions for completing the Revoke Authorization workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under **Action**, click **Revoke**. You can revoke any authorized tenant.



2. Confirm to proceed. The selected tenant will no longer be authorized.



52 Remote Browser Isolation

Topics:

- Get Started with Remote Browser Isolation
- Manage Remote Browser Isolation Profiles
- Remote Browser Isolation Advanced Isolation Controls Reference

Provides an overview of Remote Browser Isolation in Cisco Secure Access, including Get Started with Remote Browser Isolation, Manage Remote Browser Isolation Profiles, and Remote Browser Isolation Advanced Isolation Controls Reference. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with Remote Browser Isolation

Use Remote Browser Isolation (RBI) in Cisco Secure Access to protect your web sessions and documents. This topic helps you understand how to set up isolation profiles to control user interactions, reduce data exfiltration risks, and ensure safe document viewing.

Cisco Secure Access provides Remote Browser Isolation (RBI) for granular isolation controls, allowing administrators to define exactly how users interact with isolated web content and documents. By creating Isolation Profiles, you can control data exfiltration risks, such as copy-pasting and printing, and ensure safe document viewing through sanitization.

> **Note**
>
> Currently, isolation applies only to Internet Access rules.

Manage Remote Browser Isolation Profiles

Describes Manage Remote Browser Isolation Profiles in Cisco Secure Access. Remote Browser Isolation (RBI) profiles allow you to define granular security controls for web traffic that is redirected to an isolated browser.You can create a maximum of 100 isolation profiles for each organization.

Remote Browser Isolation (RBI) profiles allow you to define granular security controls for web traffic that is redirected to an isolated browser.

> **Note**
>
> You can create a maximum of 100 isolation profiles for each organization.

To view the RBI profiles, sign in to Secure Access and then navigate to Secure > Isolation Profiles. The Isolation Profiles page displays the available RBI profiles and includes each profile's name, description (if available), number of associated rules, watermarking status, copy and paste settings, keyboard control settings, file transfer settings, and last modified date.



System Default Profile

Describes System Default Profile in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access provides a System Default Profile. If no custom profile is selected, the system automatically applies this profile to any Internet Access Policy rule that uses the Isolate action.

- You cannot delete the System Default Profile, but you can modify its settings.
- You can change which profile acts as the default in **Secure** > **Access Policy** > **Rule Defaults and Global Settings**.

Create a Remote Browser Isolation Profile

Provides instructions for completing the Create a Remote Browser Isolation Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To create a Remote Browser Isolation Profile, perform the following steps:

Before you begin

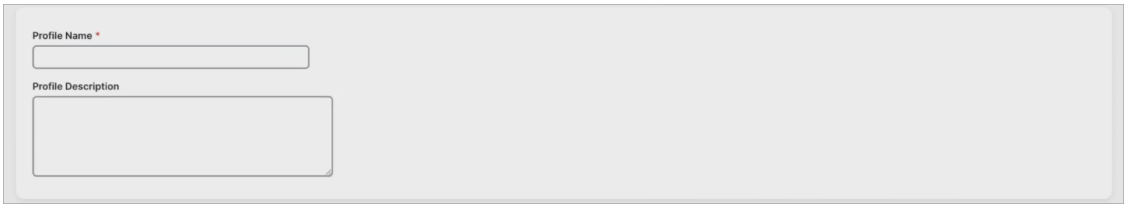
You must have Full Admin user role. For more information, see Accounts Overview.

Procedure

1. Navigate to **Secure** > **Isolation Profiles**.
2. Click **+ Add Profile**.

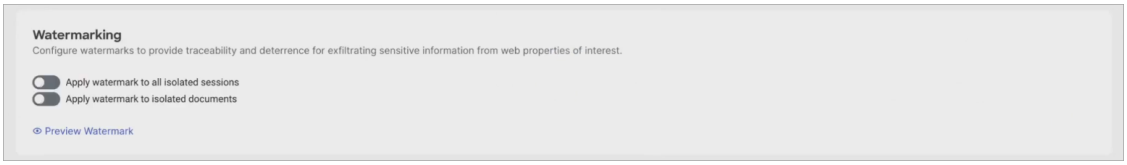


3. Enter a **Profile Name** and an optional **Description**.

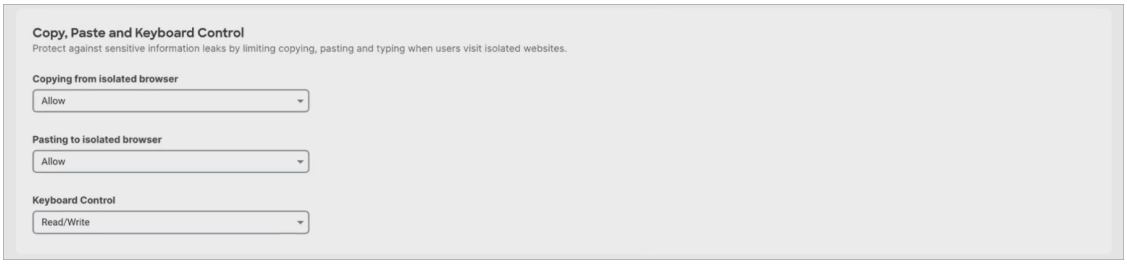


4. Configure the following control sections:
   - **Watermarking**: Enable to add a static watermark to the browser, isolated documents, or both.

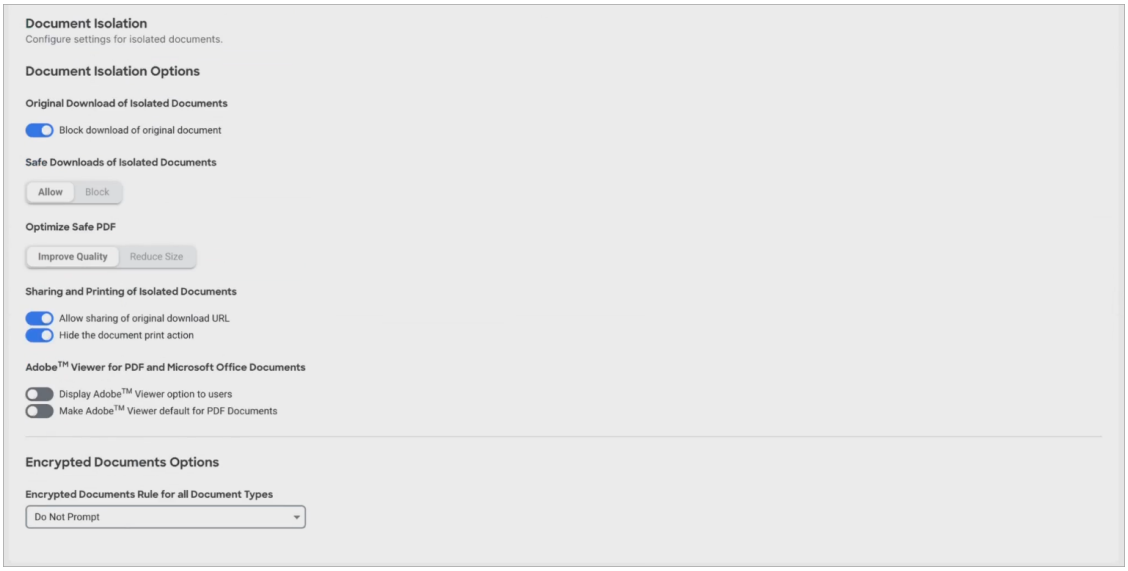
> **Note**
>
> The watermark includes a Source ID. While this ID is anonymous to the user, it allows administrators and support to trace the session back to a specific user for auditing.



   - **Copy, Paste, and Keyboard Control**:
     - **Copy/Paste**: Allow or block the ability to copy from or paste into the isolated browser. You can set a character limit for pasting (useful for passwords).
     - **Keyboard Control**:
       - **Read/Write**: Normal interaction.
       - **Read Only**: Users can view and click buttons but cannot input information into forms.



- **Document Isolation Options**:
  - **Original Download of Isolated Documents**: Configure to allow or block the download of original documents.
  - **Safe Downloads of Isolated Documents**: Allow or block the download of a sanitized PDF version of the original document where active code and links are stripped.
  - **Optimize Safe PDF**: Configure for improving or reducing the quality of the downloaded safe PDF.
  - **Sharing and Printing of Isolated Documents**: Configure to allow or block sharing and printing of the document.
  - **Viewers**: Choose the required options to use the Adobe viewer for PDF and Microsoft Office documents.
  - **Encrypted Documents Options**: Prompting for password allows access to encrypted documents. Setting **Do Not Prompt** disables access to all encrypted documents.



- **File Transfers**:
  - **Document Types**: These are governed by your existing File Type Control policies in Secure Access.
  - **Non-Document Types (for example, .exe)**: Use the Isolation Profile to specifically block or allow the upload or download of non-document files within the isolated session.



5. Click **Save**.

The Isolation Profiles page displays the saved RBI profile.

Edit or Delete a Remote Browser Isolation Profile

Provides instructions for completing the Edit or Delete a Remote Browser Isolation Profile workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To edit or delete a remote browser isolation profile, perform the following steps:

Procedure

1. Navigate to **Secure** > **Isolation Profiles**.
2. To modify a profile:
   - Click the options (ellipsis) icon next to the profile and select **Edit**.
   - Update the settings and click **Save**. Changes apply to all Access Policy rules associated with that profile.
3. To delete a profile:
   - Click the options (ellipsis) icon and select **Delete**.

> **Note**
>
> You cannot delete a profile that is currently associated with an active Access Policy rule. You must first change the profile in the policy rule or delete the rule itself.

Remote Browser Isolation Advanced Isolation Controls Reference

Refer to this topic to learn about the advanced isolation settings you can configure in Remote Browser Isolation profiles.

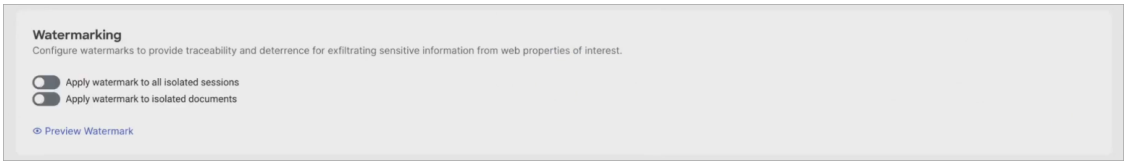
This topic provides detailed definitions for the settings available within a Remote Browser Isolation (RBI) profile.

- Watermarking
- Copy, Paste and Keyboard Control
- Document Isolation
- File Transfers

Watermarking

Describes Watermarking in Cisco Secure Access. Watermarks are a visual overlay to the isolated session to discourage unauthorized screen captures or data sharing.

Watermarks are a visual overlay to the isolated session to discourage unauthorized screen captures or data sharing. You can apply Watermark to isolated browser window, isolated documents, or both. You can click Preview Watermark to see a sample of the watermark.

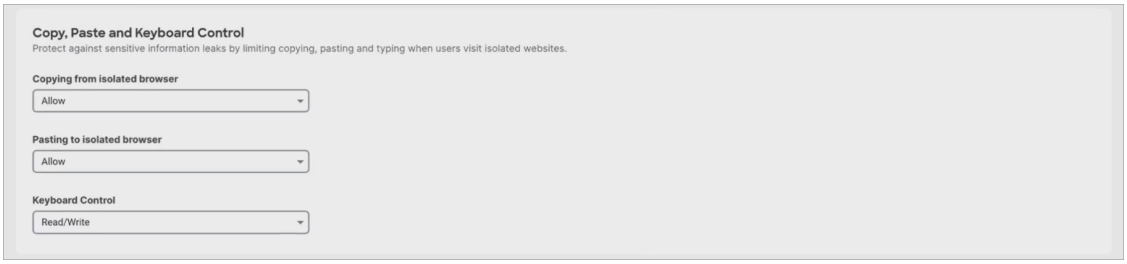


Copy, Paste and Keyboard Control

Describes Copy, Paste and Keyboard Control in Cisco Secure Access. You can define how users can interact with web content and their local clipboard.

You can define how users can interact with web content and their local clipboard.

- **Copying from isolated browser**:
  - **Allow/Block**: Controls if a user can copy text from the isolated browser to their local machine.
- **Pasting to isolated browser**:
  - **Allow/Block**: Controls if a user can paste text from their local machine into the isolated browser.
  - **Limit**: Sets the maximum number of characters allowed for a single paste operation.



- **Keyboard control**:
  - **Read/Write**: Users can interact with the website normally, including typing into text fields and forms.
  - **Read-Only**: Users can view content and click navigation elements (like buttons or links), but all text input fields and web forms are disabled.

Document Isolation

Describes Document Isolation in Cisco Secure Access. You can control how files are handled when opened within an isolated session.

You can control how files are handled when opened within an isolated session.

- **Original Download of Isolated Documents**: When enabled, the original file download is blocked.



- **Safe Downloads of Isolated Documents**: When allowed, the user is provided with a Safe Download – a sanitized PDF version of the document. Sanitization removes active code, macros, and embedded links to prevent malware execution.



- **Optimize Safe PDF**: You can set the optimization option to either improve the PDF quality or reduce the size.



- **Sharing and Printing of Isolated Documents**:
  - **Allow sharing of original download URL**: Enables the ability to generate a shareable URL for the original document.
  - **Hide the document print action**: Disables the print action for the document.



- **AdobeTM Viewer for PDF and Microsoft Office Documents**: When enabled, PDF and Microsoft Office documents are displayed using an integrated Adobe viewer within the isolated browser.



- **Encrypted Documents Options**:
  - **Do Not Prompt**: If a user attempts to open a password-protected file, they are not prompted to enter the password. Without authentication, encrypted documents are not accessible.
  - **Password Prompt**: If a user attempts to open a password-protected file, they are prompted to enter the password within the isolated session.



File Transfers

Describes File Transfers in Cisco Secure Access. You can manage the upload and download of files during an isolated session.

You can manage the upload and download of files during an isolated session. The transfer of document-style files (for example, .docx, .pdf) is governed by your organization's File Type Control policies. But using the Isolation profile, you can specifically Block or Allow the upload or download of non-document files (such as .exe or .zip) that occur within the isolated environment. This acts as a secondary layer of protection specific to isolation.



53 Internet Security

Topics:

- Manage Internet Security

Provides an overview of Internet Security in Cisco Secure Access, including Manage Internet Security. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internet Security

Describes Manage Internet Security in Cisco Secure Access. You can manage the Cisco Secure Access Internet Security settings in Secure Access to protect the user devices in your organization.

You can manage the Cisco Secure Access Internet Security settings in Secure Access to protect the user devices in your organization.

> **Note**
>
> User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file for the browsers in the environment.

Download Cisco Secure Client or Copy Secure Access PAC File URL

To deploy the Secure Access Internet Security on user devices, first download and install the software package for the Cisco Secure Client or copy the URL for the Secure Access PAC file from Secure Access.

You can also install custom PAC files in your environment. For more information about deploying PAC files, see Manage PAC Files.

Add Bypass Domains and Set Up Internet Security

Once you install and deploy the Cisco Secure Client or the Secure Access or custom PAC files in the environment, add bypass domains in Secure Access. Then, configure DNS and web security settings for the user devices in the organization.

Next Steps

- Set Up Internet Security on User Devices
- Manage Internet Security Bypass
- Configure Cisco Secure Client Settings

Set Up Internet Security on User Devices

Describes Set Up Internet Security on User Devices in Cisco Secure Access. Before you add DNS and web security in Cisco Secure Access for end users, deploy the Cisco Secure Client or the Secure Access or custom PAC files in your environment.

Before you add DNS and web security in Cisco Secure Access for end users, deploy the Cisco Secure Client or the Secure Access or custom PAC files in your environment. User devices with the Cisco Secure Client installed must also deploy the Umbrella Roaming Security module.

This guide describes the steps to download the software package for the Cisco Secure Client or copy the URL for the Secure Access PAC file to your environment.

To complete the setup, we recommend that you provision users and groups from the organization in Secure Access. For more information, see Manage User Directories and Device Management.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Visibility of User Identities in Policy Rules

- Deploy the Secure Access Active Directory (AD) Connector. For more information, see Connect Active Directory to Secure Access.
- Provision users and groups in Secure Access. For more information, see Provision Users and Groups from Active Directory.

Procedure for Setting Up Internet Security on User Devices

Describes Procedure for Setting Up Internet Security on User Devices in Cisco Secure Access. Download the Secure Access OrgInfo.json file for the organization or copy the Secure Access PAC file URL.

Download the Secure Access OrgInfo.json file for the organization or copy the Secure Access PAC file URL. Use the deployment configuration files to set up the Cisco Secure Client or browsers on the user devices.

For more information about deploying PAC files with Secure Access, see Manage PAC Files.

Download the OrgInfo.json File

Provides instructions for completing the Download the OrgInfo.json File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can deploy various modules with the Cisco Secure Client. The Cisco Secure Client may require a certain profile present to install a module successfully.

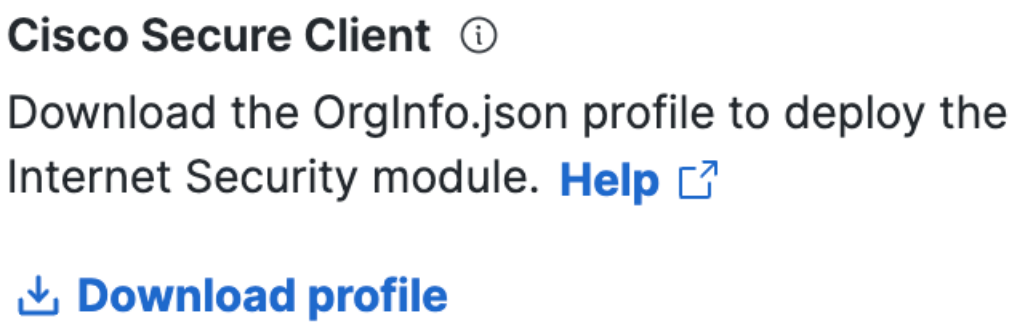
The Cisco Secure Client Umbrella Roaming Security module (DNS-layer and Web security) requires the Secure Access **OrgInfo.json** file. The Secure Access **OrgInfo.json** file associates a Cisco Secure Client deployment with the Umbrella Roaming Security module to a Secure Access user and organization. Once the module is deployed on the Cisco Secure Client, Secure Access applies the organization's configured policy rules to the device. The device's traffic events are visible in the Activity Search report.

If you use another **OrgInfo.json** file from a different organization in Secure Access to install the Cisco Secure Client Umbrella module, the roaming device is managed by that instance of Secure Access instead.

To deploy the Cisco Secure Client with the Umbrella Roaming Security module on a user device, download the **OrgInfo.json** file from Secure Access to the device.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. For **Cisco Secure Client**, click **Download profile**. Download the Secure Access OrgInfo.json file to the user devices where you have deployed the Cisco Secure Client.

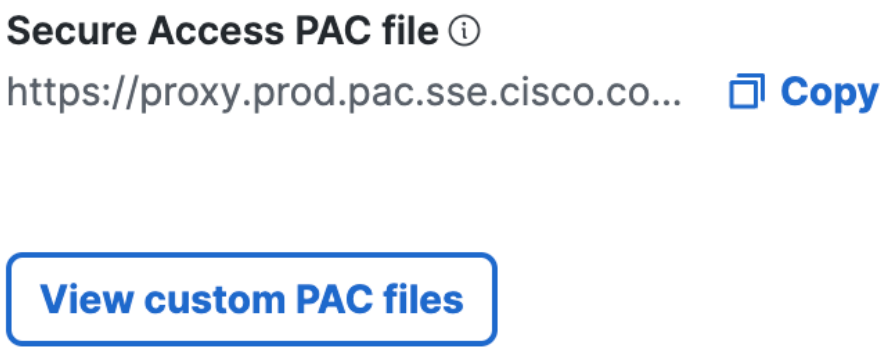


Copy the PAC File URL

Provides instructions for completing the Copy the PAC File URL workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. For **Secure Access PAC file**, click **Copy** to get the Secure Access PAC file URL. For more information about the Secure Access PAC file and deploying custom PAC files, see Manage PAC Files.



Manage Internet Security Bypass

Describes Manage Internet Security Bypass in Cisco Secure Access. You can configure Internet Security Bypass for web requests to destinations from end users in your organization.

You can configure Internet Security Bypass for web requests to destinations from end users in your organization. In Secure Access, add IP addresses, CIDR blocks, or domains for Internet Security Bypass. For more information, see Add Destinations for Internet Security Bypass.

Secure Access supports Internet Security Bypass for user devices with the Cisco Secure Client (formerly known as AnyConnect) and Umbrella Roaming Security module, or user devices with browsers that are configured with the Secure Access PAC file or a custom PAC file.

About Internet Security Bypass

Add destinations for Internet Security Bypass in Secure Access to either bypass the Secure Access DNS resolvers and Secure Web Gateway, or bypass the Secure Web Gateway only.

To bypass the Secure Access DNS resolvers and Secure Web Gateway, add the domains that are local to your organization or domains that should route to your organization's DNS resolvers only and not route to the Secure Access DNS servers. Your local DNS servers will resolve the DNS requests that are sent from end users in the organization. DNS requests for the destinations do not route to the Secure Access DNS servers and Secure Web Gateway.

To bypass the Secure Access Secure Web Gateway only, add destinations for trusted applications, applications that are not reachable through web proxies, or applications that end users can access only from specific public IP addresses. If you bypass the Secure Web Gateway only, the DNS requests from end users will be resolved by the Secure Access DNS servers. For more information about Reserved IP, see Secure Access NAT as a Service.

Internet Security Bypass Limits

When configuring domains and IP addresses in the Internet Security Bypass list, adhere to the following organization capacity limits:

List Type	Standard Limit (Default)	Extended Limit (On Request)
Internal and External Domains (Combined)	5,000	9,000
IP Addresses	5,000	9,000

Internal domains and external domains share a single combined limit per organization. By default, you can configure up to 5,000 total domains. If your organization requires additional capacity (up to 9,000 domains), contact your Cisco representative or Cisco Support to request an increase.

> ⚠ **Caution**
>
> While organizations with extended limits can configure up to 9,000 domain entries, deploying very large bypass lists to roaming devices running Cisco Secure Client increases local memory usage and configuration payload size. For optimal client performance and stability, keep active domain entries consolidated.

Add Destinations for Internet Security Bypass

Provides instructions for completing the Add Destinations for Internet Security Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add destinations in Secure Access to bypass internet security. Traffic for destinations that are added in Secure Access bypass the Secure Access DNS resolvers and Secure Web Gateway or the Secure Web Gateway only.

If you configure destinations to bypass the SWG and Secure Access DNS servers, the DNS requests are sent to the organization's local DNS resolvers.

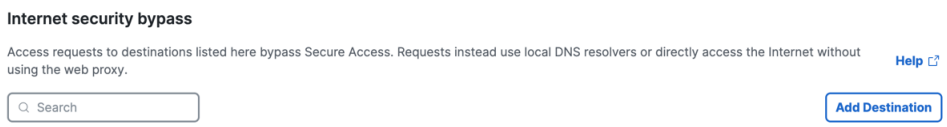
If you configure destinations to bypass the SWG only, the DNS requests are sent to the Secure Access DNS servers and directly to the Internet.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- User devices must have the Cisco Secure Client and Umbrella Roaming Security module or deploy the Secure Access PAC file or a custom PAC file on the browsers in the environment.

Procedure

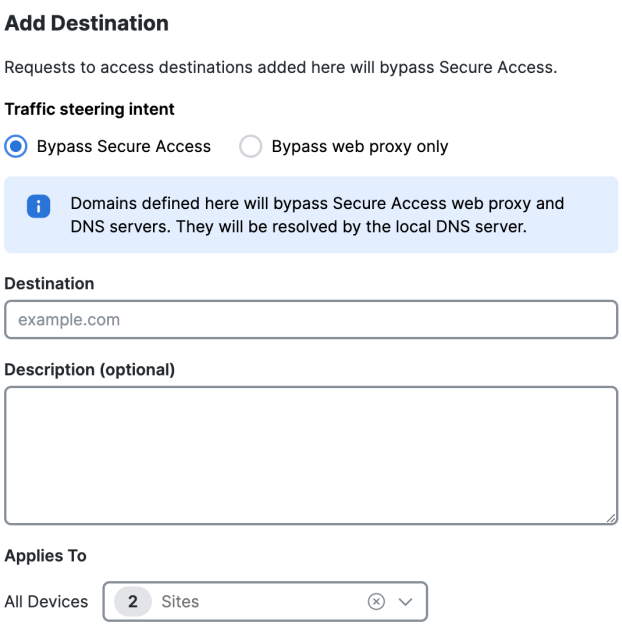
1. Navigate to **Connect** > **End User Connectivity** > **Internet Security** , and then click **Add Destination**.



2. Choose **Bypass Secure Access** to bypass the Secure Access SWG and DNS servers.

   Add the domains that are local to your organization or domains that should route to your organization's DNS resolvers and not route to the Secure Access DNS servers.

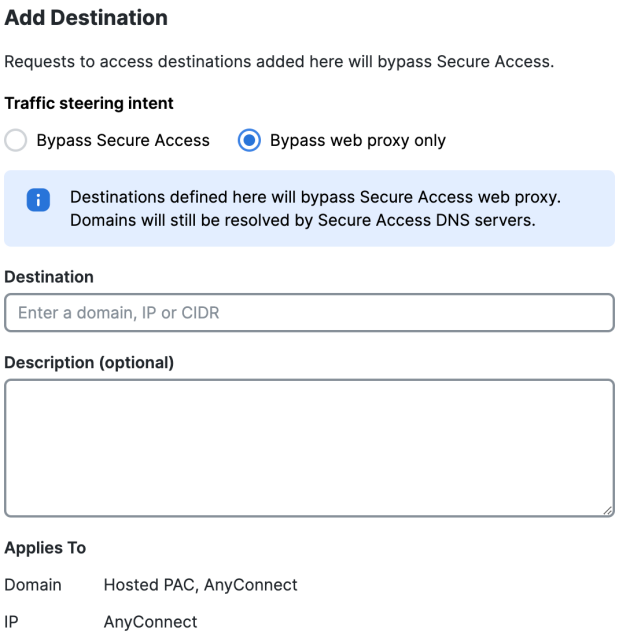
   DNS requests for the destination will be resolved by the organization's local DNS servers.



a) For **Destination**, enter a domain name.
b) (Optional) For **Description**, enter text that describes why the domain will bypass the Secure Web Gateway and DNS servers.
c) For **Applies To**, select the Secure Access Sites for all devices that should bypass Secure Access when requesting the domain. If you happen to select multiple sites and need to remove them from the configuration prior to saving, the "x" icon inside the drop-down bar of this step allows you remove all of the selected sites.

3. Choose **Bypass web proxy only** to bypass the Secure Web Gateway (SWG) only.

   Add destinations for trusted applications, applications that are not reachable through web proxies, or applications that end users can access only from specific public IP addresses.



a) For **Destination**, enter a domain name.
b) (Optional) For **Description**, enter text that describes why the domain will bypass the Secure Web Gateway.

4. Click **Save**.

View Destinations for Internet Security Bypass

Provides instructions for completing the View Destinations for Internet Security Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

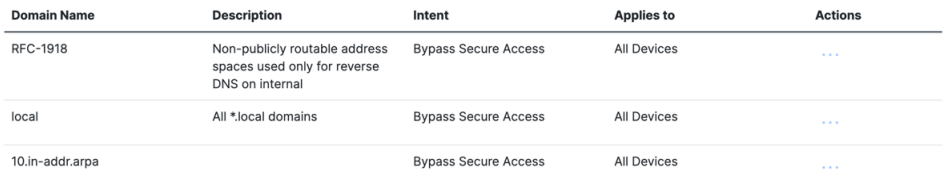
After you add the destinations in Secure Access to bypass internet security, you can view the details about the destinations.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. View the domains that you added to the bypass internet security list in Secure Access.



Domain Name	Description	Intent	Applies to	Actions
RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal	Bypass Secure Access	All Devices	...
local	All *.local domains	Bypass Secure Access	All Devices	...
10.in-addr.arpa		Bypass Secure Access	All Devices	...

- **Domain Name**–The name of the domain.
- **Description**–The text that describes the domain.
- **Intent**–The type of domain, for example: **Bypass Secure Access**.
- **Applies to**–The name of a Site or the location of the Secure Access Virtual Appliance (VA) where the domain is bypassed.
- **Actions**–The actions taken to manage the destination in Secure Access.

Edit Destination for Internet Security Bypass

Provides instructions for completing the Edit Destination for Internet Security Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a destination in Secure Access to bypass internet security, you can edit the destination. You can modify the internet security information for destinations that bypass the Secure Access Secure Web Gateway (SWG) and Secure Access DNS resolvers, or only bypass the Secure Web Gateway.

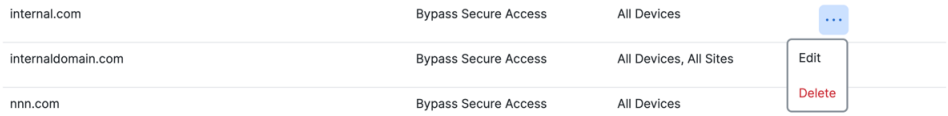
Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- User devices must have the Cisco Secure Client and Umbrella Roaming Security module or deploy the Secure Access PAC file or a custom PAC file on the browsers in the environment.

Procedure

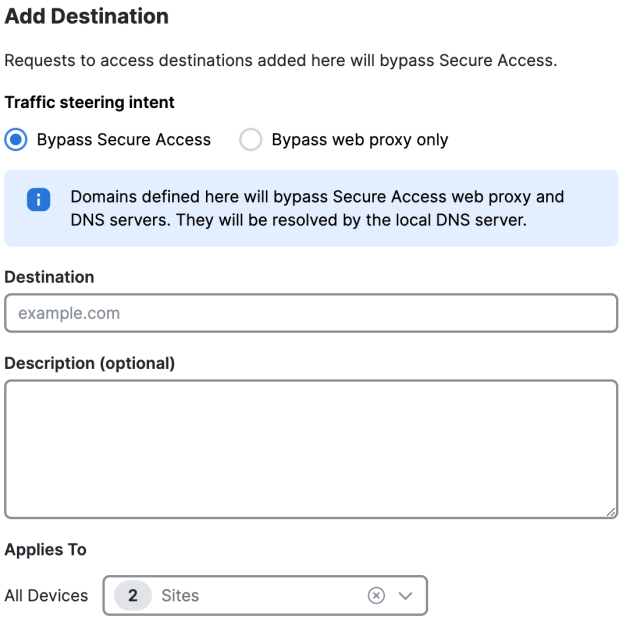
1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Navigate to **Internet security bypass**, navigate to a destination in the internet security bypass table, and then click the ellipsis (**...**).

3. Click **Edit** to modify the bypass information for the destination.



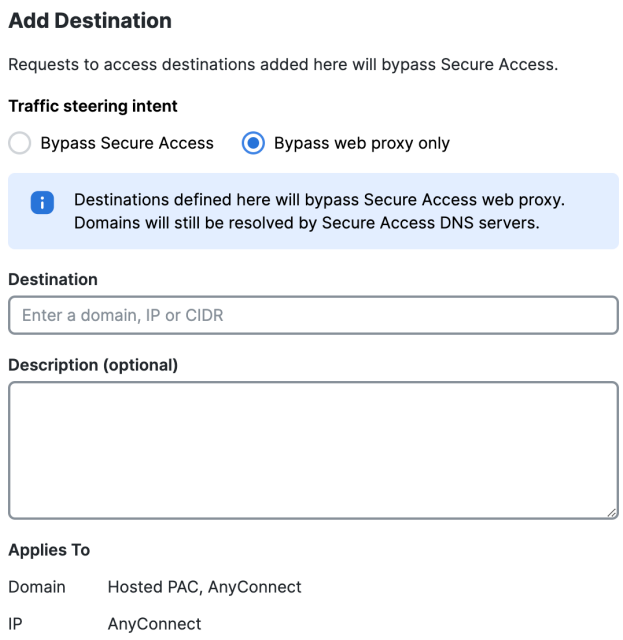
4. Choose **Bypass Secure Access** to bypass the Secure Access Secure Web Gateway and Secure Access DNS servers.

> **Note**
>
> DNS requests will be resolved by the organization's local DNS servers.



a) For **Destination**, enter a domain name.
b) (Optional) For **Description**, enter text that describes why the domain will bypass the Secure Web Gateway and Secure Access DNS servers.
c) For **Applies To**, select the Secure Access sites for all web requests on the devices that should bypass Secure Access. If you need to remove multiple sites, the "x" icon inside the drop-down bar of this step allows you remove all of the selected sites.

5. Choose **Bypass web proxy only** to bypass the Secure Web Gateway (SWG) only.



a) For **Destination**, enter a domain name.
b) For **Description** (optional), enter text that describes why the domain will bypass the Secure Web Gateway.

6. Click **Save**.

Delete Destinations for Internet Security Bypass

Provides instructions for completing the Delete Destinations for Internet Security Bypass workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a destination to bypass the Secure Access internet security, you can remove the destination. As a result of removing the destination, the DNS requests for the destination will resolve to the Secure Access DNS servers.

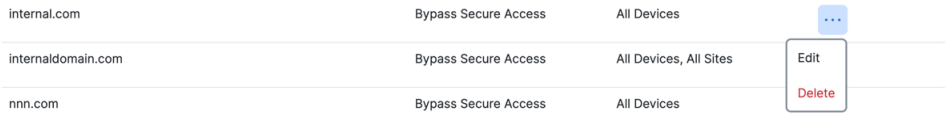
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Navigate to **Internet security bypass**, navigate to a destination in the internet security bypass table, and then click the ellipsis (**...**).
3. Click **Delete**.



4. Click **Delete** to confirm the removal of the destination.

Configure Cisco Secure Client Settings

Describes Configure Cisco Secure Client Settings in Cisco Secure Access. You can configure the Cisco Secure Access Internet Security in Secure Access for end users.

You can configure the Cisco Secure Access Internet Security in Secure Access for end users.

> **Note**
>
> User devices must have the Cisco Secure Client deployed with the Umbrella Roaming Security module or deploy a PAC file for the browsers in the environment.

This guide describes the steps to enable the DNS and web security settings and advanced internet security settings in Secure Access for the end user devices in the organization.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

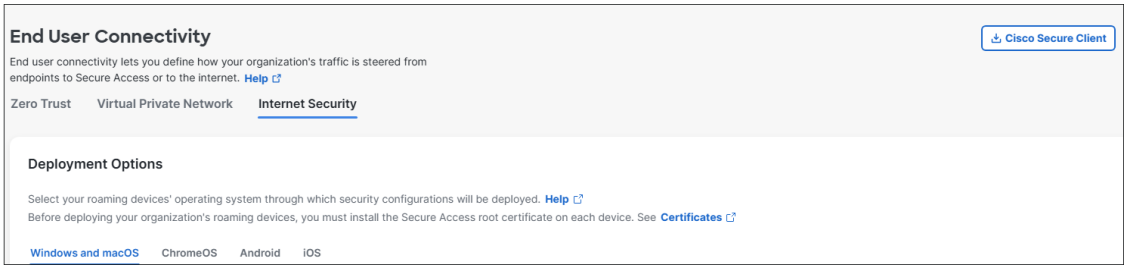
Configure the Cisco Secure Client internet security settings. The advanced internet settings contains several fields that provide additional control over user authentication, traffic bypass, and VPN compatibility.

Before you begin

Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. On the End User Connectivity page, click the **Internet Security** tab.



3. Select a tab and then options on that tab:
   - DNS and Web Security
     - Configure DNS and Web Security on page 1874
   - Advanced
     - Use Active Directory for Access Policy
     - Third Party VPN Compatibility on page 1875
     - DNS Protection on page 1875
     - Alternate Resolver IPs
     - DNS Backoff Settings on page 1877

- Secure Web Gateway Backoff Settings

Configure Security Settings

Describes Configure Security Settings in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Configure DNS and Web Security

Provides instructions for completing the Configure DNS and Web Security workflow in Cisco Secure Access. Configure DNS and web security settings for the Cisco Secure Client.

Configure DNS and web security settings for the Cisco Secure Client.

> **Note**
>
> The Secure Access DNS-layer security is always enabled on the Cisco Secure Client.

The Cisco Secure Client with the Umbrella Roaming Security module steers web traffic on ports 80/443 to the Secure Web Gateway (SWG). All web traffic is evaluated against the organization's policy and Internet Access rules when a VPN connection is not established.

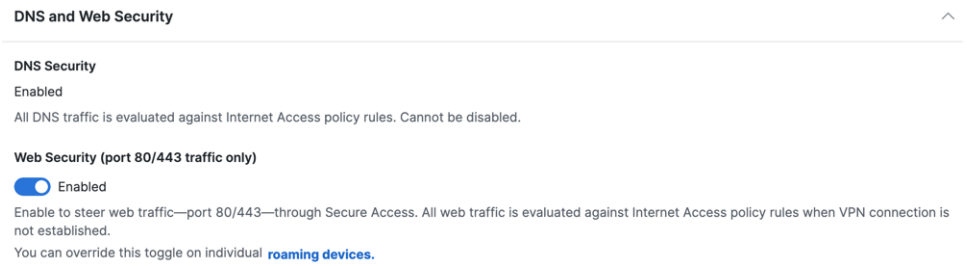
> **Note**
>
> You can override this option on individual roaming devices.

Before you begin

Full Admin user role. For more information, see Manage Accounts.

Procedure

Enable the **Web Security (port 80/443 traffic only)** toggle button.



Configure Advanced Security Settings

Describes Configure Advanced Security Settings in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

Use Active Directory for Access Policy

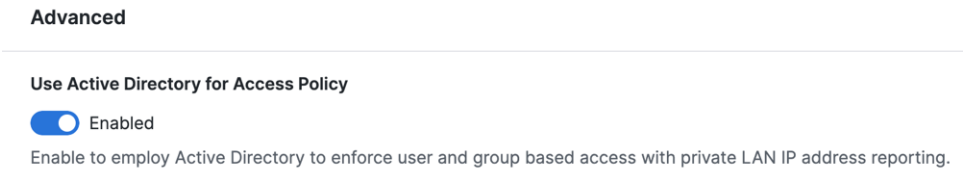
Provides instructions for completing the Use Active Directory for Access Policy workflow in Cisco Secure Access. Enable the Cisco Secure Client to synchronize users and groups identities with the Secure Access Active Directory (AD) Connector.

Enable the Cisco Secure Client to synchronize users and groups identities with the Secure Access Active Directory (AD) Connector. Secure Access applies Access rules for user identities, which are associated with devices that have deployed the Cisco Secure Client.

Before you begin
Full Admin user role. For more information, see Manage Accounts.

Procedure

Enable the **Use Active Directory for Access Policy** toggle button.



Third Party VPN Compatibility

Provides instructions for completing the Third Party VPN Compatibility workflow in Cisco Secure Access. Improve compatibility for third-party VPN clients on Windows 10 only, or if the local DNS is not resolving resources.

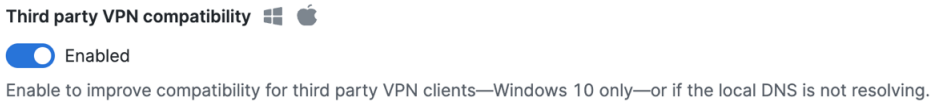
Improve compatibility for third-party VPN clients on Windows 10 only, or if the local DNS is not resolving resources.

The Cisco Secure Client with the Umbrella Roaming Security module works with most VPN software. However, the Cisco Secure Client with the Umbrella Roaming Security module and other VPN profiles may not resolve local DNS queries correctly on a VPN connection with Windows 10. The local LAN may bind above the VPN, failing to resolve local DNS requests over the tunnel. Select this setting to apply the legacy binding order behavior.

Before you begin
Full Admin user role. For more information, see Manage Accounts.

Procedure

Enable the **Third Party VPN Compatibility** toggle button.



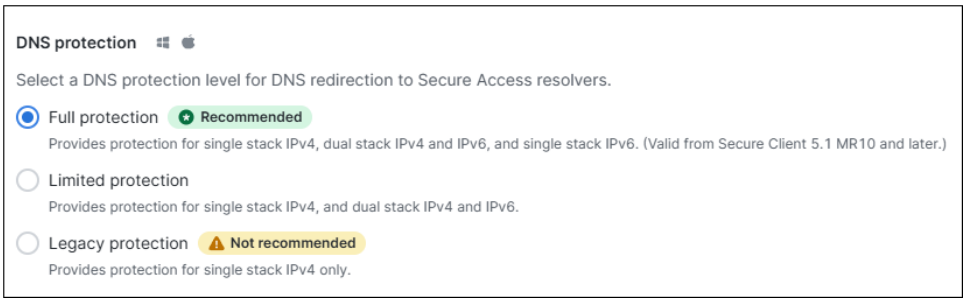
DNS Protection

Describes DNS Protection in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

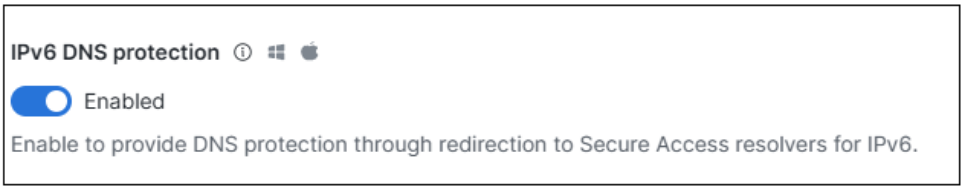
Choose one of the following options to provide DNS protection:

- **Full Protection:** Provides protection for single stack IPv4 network, dual stack IPv4 and IPv6 network, and single stack IPv6 network.

- **Limited Protection:**Provides protection for single stack IPv4 network, and dual stack IPv4 and IPv6 network.
- **Legacy Protection:**Provides protection for single stack IPv4 network only.



The previous dashboard configuration for IPv6 DNS protection allowed enabling protection over IPv6.



This earlier configuration is now replaced with the new DNS protection options described above.

- If the earlier **IPv6 DNS protection** configuration was disabled, the new configuration defaults to**Legacy Protection**.
- If the earlier **IPv6 DNS protection**configuration was enabled, the new configuration defaults to **Limited Protection**.

> **Note**
>
> For optimal security, we recommend using the **Full Protection** configuration, available in Cisco Secure Client 5.1.10.233 (MR 10) or later.

Alternate Resolver IPs

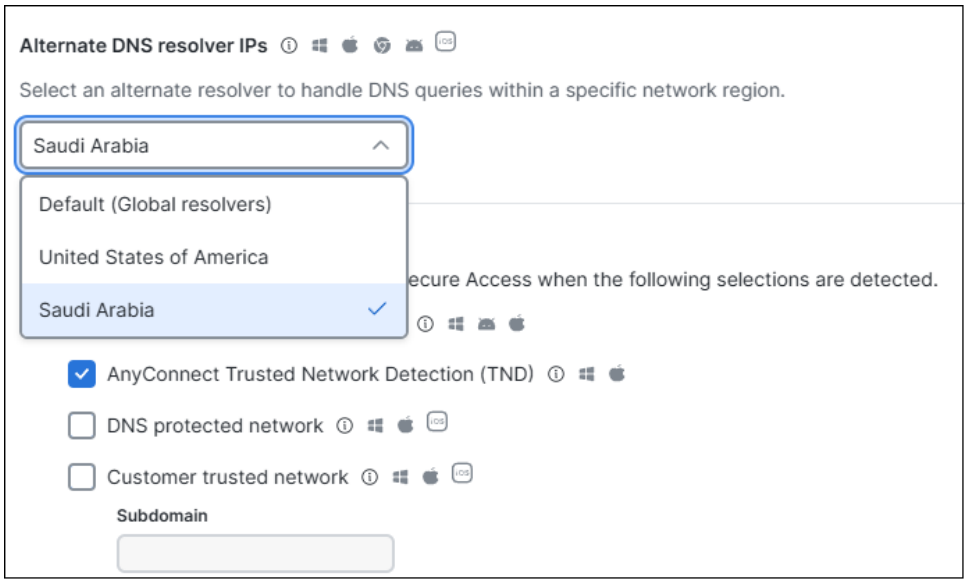
Describes Alternate Resolver IPs in Cisco Secure Access. Select an alternate resolver to handle DNS queries within a specific network region.

Select an alternate resolver to handle DNS queries within a specific network region. Ensure that the latest version of Client is installed on your remote device.

Note

Minimum client platform version requirement for:

Android:	Cisco Secure Client 5.1.8 or later
iOS:	Cisco Secure Client 1.7.3 or later
Windows and macOS:	Cisco Secure Client 5.1.9 or later



Important

For remote devices running **ChromeOS**, ensure that you deploy the Cisco Security for Chromebook client 2.2.0 or later in the Google Admin console after setting the Alternate DNS resolver IPs. For more information, see Deploy the Cisco Security for Chromebooks Client on page 2697.

DNS Backoff Settings

Provides instructions for completing the DNS Backoff Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Bypass DNS traffic from Secure Access for the following contexts:

Before you begin

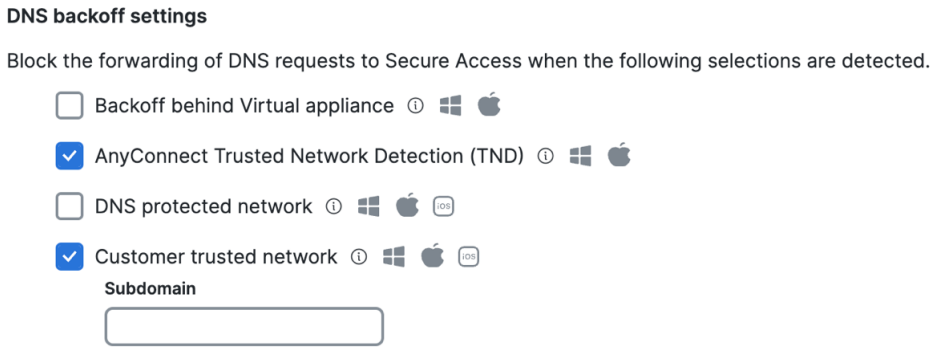
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Select **Backoff behind Virtual appliance**. When enabled and the Cisco Secure Client detects a Secure Access Virtual Appliance (VA), DNS traffic goes through the local network instead of redirecting to Secure Access.
2. Select **AnyConnect Trusted Network Detection (TND)** to disable DNS traffic forwarding from an endpoint to Secure Access if the network is trusted. This setting requires that you have the Trusted Network Detection (TND) setting enabled in the AnyConnect VPN profile for the user devices.

3. Select **AnyConnect VPN Detection** to disable DNS traffic forwarding to Umbrella when endpoint detects that a full-tunnel VPN session is active. This is specific to Cisco VPNs. Currently this feature is not compatible with Cisco Secure Access remote access VPN. However, this feature is compatible with other Cisco products that support full-tunnel VPN, such as the Cisco Adaptive Security Appliance (ASA).
4. Select **DNS protected network** to disable DNS traffic forwarding while on a network protected by Secure Access. Relies on the protection of the network. To trigger this setting, you must register the public network in Secure Access and add the network to a rule that has a higher priority than the roaming devices. In addition, the local DNS server egress network must have the same network registration as straight out from the computer to **208.67.222.222**.
5. Select **Customer trusted network** to disable DNS redirects to Secure Access if the domain name added to the **Subdomain** field is found on the network and resolves to an RFC-1918 local IP address.
   - For **Subdomain**–enter a domain that Secure Access uses to query the local DNS server.

> **Note**
>
> You must enable **Customer trusted network** to add the subdomain.



Secure Web Gateway Backoff Settings

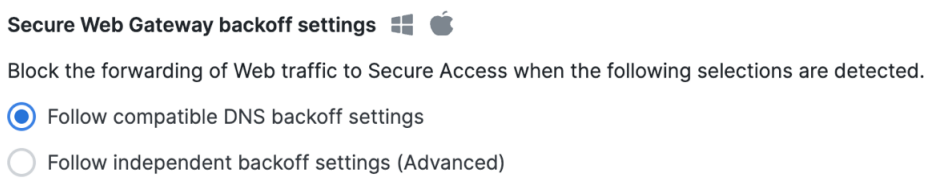
Provides instructions for completing the Secure Web Gateway Backoff Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Select **Follow compatible DNS backoff settings**. Enable this option to allow the Cisco Secure Client with the Umbrella Roaming Security module to follow the DNS backoff behavior for any of these DNS backoff settings: **Customer trusted network** or **AnyConnect Trusted Network Detection (TND)**.

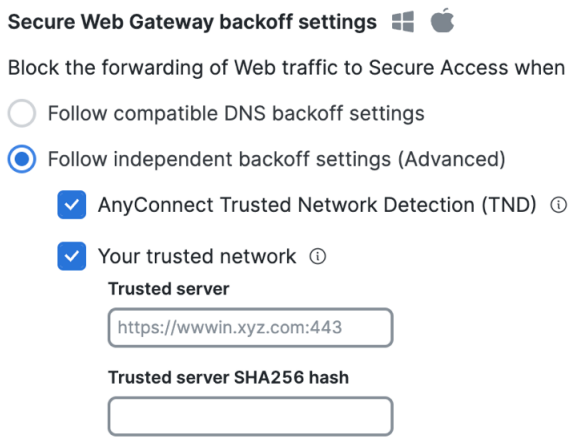


2. Select **Follow independent backoff settings (Advanced)**.

> **Note**
>
> The **AnyConnect Trusted Network Detection (TND)** and **Your trusted network** options are only supported with user devices that have version 5.1.3.62 or higher of the Cisco Secure Client with the Umbrella Roaming Security module deployed. For information about downloading the Cisco Secure Client software packages, see Cisco Secure Client Version 5.1.3.62 .

Bypass Web traffic from Secure Access for the following contexts:

- Select **AnyConnect Trusted Network Detection (TND)** to disable web traffic forwarding from an endpoint to Secure Access if the network is trusted. This setting requires that you have the Trusted Network Detection (TND) setting enabled in the AnyConnect virtual private network (VPN) profile for the user devices.
- Select **AnyConnect VPN Detection** to disable web traffic forwarding to Umbrella when the endpoint detects an active, full-tunnel VPN session. This is specific to VPNs within the Cisco VPN infrastructure with certificates and configurations issued and validated by Cisco VPN servers.
- Select **Your Trusted network** to enable endpoints to detect an organization's trusted network, which is identified by the **Trusted server** and **Trusted server SHA256 hash** fields. When the endpoint detects trusted networks, traffic from the endpoints bypass Secure Access and the endpoints rely on the network protections.
  - For **Trusted server**, enter the URL (`<domain>:<port>`) of the trusted network server, which hosts the trusted server certificate. This option disables redirects to Secure Access when on the trusted network identified by the trusted network server.
  - For **Trusted server SHA256 hash**, enter the SHA256 hash for the trusted network server's certificate. The ID of the trusted network server's certificate must match the configured SHA256 hash.



54 PAC Files

Topics:

- Manage PAC Files

Provides an overview of PAC Files in Cisco Secure Access, including Manage PAC Files. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage PAC Files

Describes Manage PAC Files in Cisco Secure Access. Cisco Secure Access provides several client configuration options to manage the web traffic and internet security for the user devices in the organization.

Cisco Secure Access provides several client configuration options to manage the web traffic and internet security for the user devices in the organization. You can integrate a proxy auto-config (PAC) file URL for the browsers that you use to reach web resources.

A PAC file is used by browsers to select the correct proxy server that can fetch a requested URL. The browser-based traffic is proxied through the Secure Access secure web gateway (SWG). After you integrate a PAC file on a user device, all traffic that is sent from the browser is redirected to the SWG. Secure Access applies DNS-layer security to browser traffic for non-web resources only, which bypasses the PAC file.

To download the Secure Access PAC file or custom PAC files to user devices, connect to Secure Access on a Registered Network or Network Tunnel. A roaming user device that has the Cisco Secure Client with the Umbrella Roaming security module deployed can also connect to Secure Access and download PAC files. For more information, see Requirements for Downloading PAC Files to User Devices.

Requirements for Downloading PAC Files to User Devices

Describes Requirements for Downloading PAC Files to User Devices in Cisco Secure Access and explains Supported Versions of the Secure Client for PAC Files. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To download the Secure Access PAC file or custom PAC files on a user device in the organization, the device must either:

- Connect to Secure Access on a Registered Network or Network Tunnel, or
- Deploy the Cisco Secure Client with the Umbrella Roaming Security module on the user device.

Supported Versions of the Secure Client for PAC Files

You must have a version of the Cisco Secure Client that supports the integration of PAC Files. The Secure Access PAC file and custom PAC files integrate with the Cisco Secure Client version 5.1.8.105 and newer. For information about downloading the Cisco Secure Client software packages, see Download Cisco Secure Client.

About Using the Secure Client with PAC Files

Describes About Using the Secure Client with PAC Files in Cisco Secure Access. The Cisco Secure Client sends the username and IP of the user device for authentication to Secure Access.

- The Cisco Secure Client sends the username and IP of the user device for authentication to Secure Access. If authenticated, the user device can download the Secure Access PAC file or the organization's custom PAC files.
- **Secure Access PAC file**—After you add bypass domains in Secure Access, you can download the Secure Access PAC file that includes the configured bypass domains. Then, when you deploy the Secure Access PAC file on the user device's browser, the browser and the Secure Client support the same bypass domains that are configured in Secure Access.
- **Custom PAC files**—Unless you add bypass domains to a custom PAC file manually or create the custom PAC file from the Secure Access PAC file, the custom PAC file does not include the bypass domains that are configured in Secure Access. When you deploy a custom PAC file on the user device's browser, the browser only supports any bypass domains that you add to the custom PAC file.

For information about configuring bypass domains, see Manage Internet Security Bypass.

Managing PAC File Deployments

Describes Managing PAC File Deployments in Cisco Secure Access. Integrating the Secure Access PAC file or custom PAC files on the user devices in your organization so that all browser-based traffic is proxied is straightforward.

Integrating the Secure Access PAC file or custom PAC files on the user devices in your organization so that all browser-based traffic is proxied is straightforward. For more information, see:

- Deploy the Secure Access PAC File for Windows
- Deploy the Secure Access PAC File for macOS
- Customize the Secure Access PAC File
- Upload Custom PAC Files to Secure Access

Note: Microsoft has deprecated PAC file support for the file:// and ftp:// protocols in Windows 10 on Edge. Hosting the PAC file on the local machine with the Edge browser is not supported. For more information, see Windows 10 does not read a PAC file referenced by a file protocol.

We recommend that you bypass these domains in your environment for traffic with TCP on ports 80 and 443:

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocsp.identrust.com
- *.opendns.com
- *.sse.cisco.com
- *.umbrella.com
- *.okta.com
- *.oktacdn.com
- *.pingidentity.com
- secure.aadcdn.microsoftonline-p.com

Deploy the Secure Access PAC File for Windows

Describes Deploy the Secure Access PAC File for Windows. The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a user device's browser to successfully reach web resources.

The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a user device's browser to successfully reach web resources. If you are behind a firewall, you may also need to deploy the Secure Access's PAC file on the browser so that it points to the correct proxy server. A PAC file is only used with the Secure Access Internet Security.

After an organization's administrator adds bypass domains in Secure Access, the Secure Access PAC file contains the list of configured bypass domains. Web traffic to these domains is not sent to the SWG. For more information, see Manage Internet Security Bypass.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- To download the Secure Access PAC file or custom PAC files on a user device in the organization, the device must either:
  - Connect to Secure Access on a Registered Network or Network Tunnel, or
  - Deploy the Cisco Secure Client with the Umbrella Roaming Security module on the user device.

Supported Versions of the Secure Client for PAC Files

You must have a version of the Cisco Secure Client that supports the integration of PAC Files. For information about downloading the Cisco Secure Client software packages, see Download Cisco Secure Client.

For Windows, download and deploy the Cisco Secure Client version 5.1.8.105 (**cisco-secure-client-win-5.1.8.105-predeploy-k9.msi**) or newer.

Copy URL for Default PAC File or Custom PAC File

Describes Copy URL for Default PAC File or Custom PAC File in Cisco Secure Access. Copy the URL for the default Secure Access PAC file or a custom PAC file that you uploaded to Secure Access.

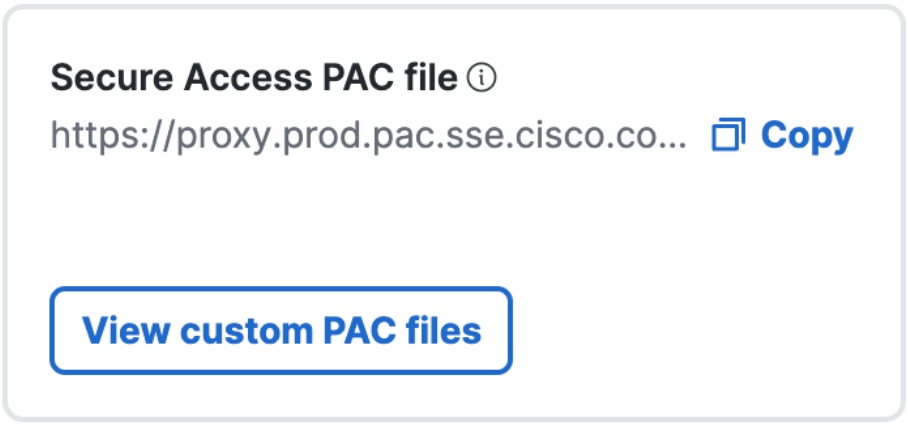
Copy the URL for the default Secure Access PAC file or a custom PAC file that you uploaded to Secure Access.

Copy URL for the the Secure Access PAC File

Provides instructions for completing the Copy URL for the the Secure Access PAC File workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Internet Security .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. For **Secure Access PAC file**, click **Copy** to get the URL for the Secure Access PAC file.

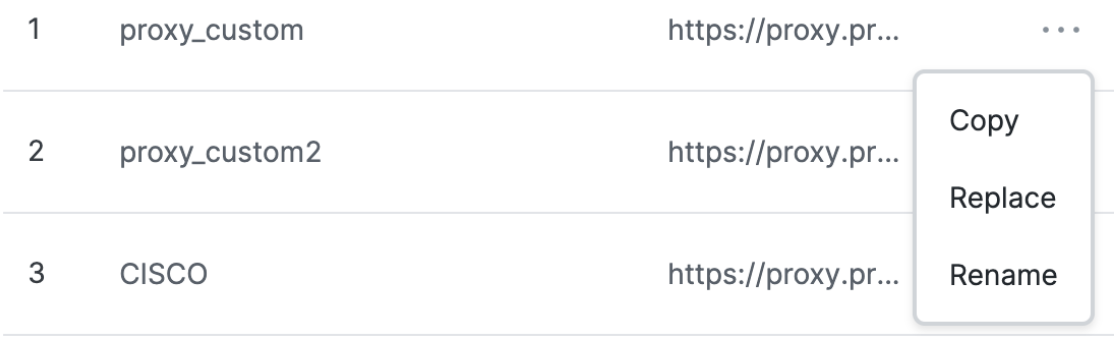


Copy URL for Custom PAC File

Provides instructions for completing the Copy URL for Custom PAC File workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Internet Security .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Click **View the custom PAC files**.
3. Navigate to a custom PAC file, and then click the ellipsis (**...**).



4. Click **Copy**, and then copy the URL for the custom PAC file.

Procedure for Deploying Secure Access PAC File URL

Describes Procedure for Deploying Secure Access PAC File URL. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Note**
>
> Operating system (OS) and browser functionality can change at any time. We can not guarantee that these third-party procedures will remain accurate. For more information on deploying a PAC file URL to your browser, see your OS and browser's Help.

Deploy the Secure Access PAC File URL for Chrome and Edge Browsers

Provides instructions for completing the Deploy the Secure Access PAC File URL for Chrome and Edge Browsers workflow in Cisco Secure Access. Get the URL for the Secure Access PAC file or a custom PAC file.

Get the URL for the Secure Access PAC file or a custom PAC file. For more information, see Copy URL for Default PAC File or Custom PAC File.

Procedure

1. In Windows, navigate to **Start** > **Settings** > **Network & internet**, and click **Proxy**.
2. For **Automatic proxy setup**, click **Set up**.
3. Set **Use setup script** to **On**.
4. For **Script Address**, paste the Secure Access PAC file URL.
5. Click **Save**.

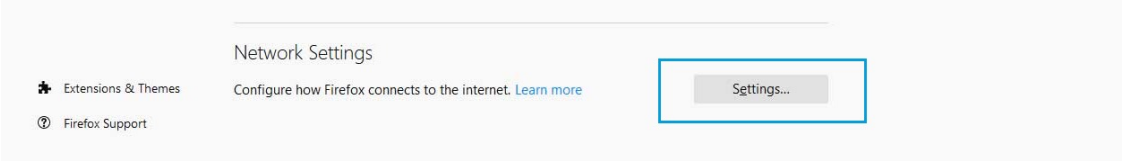
Deploy the Secure Access PAC File URL for Firefox

Provides instructions for completing the Deploy the Secure Access PAC File URL for Firefox workflow in Cisco Secure Access. Get the URL for the Secure Access PAC file or a custom PAC file.

Get the URL for the Secure Access PAC file or a custom PAC file. For more information, see Copy URL for Default PAC File or Custom PAC File.

Procedure

1. In Firefox, navigate to **Settings**, scroll to **Network Settings**, and then click **Settings**.



2. Select **Automatic Proxy Configuration URL** and paste the Secure Access PAC file URL.
3. Click **OK**.

Deploy the Secure Access PAC File for macOS

Describes Deploy the Secure Access PAC File for macOS. The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a user device's browser to successfully reach web resources.

The Cisco Secure Access secure web gateway (SWG) requires that you deploy a proxy auto-config (PAC) file URL on a user device's browser to successfully reach web resources. If you are behind a firewall, you may also need to deploy the Secure Access's PAC file on the browser so that it points to the correct proxy server. A PAC file is only used with the Secure Access Internet Security.

After an organization's administrator adds bypass domains in Secure Access, the Secure Access PAC file contains the list of configured bypass domains. Web traffic to these domains is not sent to the SWG. For more information, see Manage Internet Security Bypass.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- To download the Secure Access PAC file or custom PAC files on a user device in the organization, the device must either:
  - Connect to Secure Access on a Registered Network or Network Tunnel, or
  - Deploy the Cisco Secure Client with the Umbrella Roaming Security module on the user device.

Supported Versions of the Secure Client for PAC Files

You must have a version of the Cisco Secure Client that supports the integration of PAC Files. For information about downloading the Cisco Secure Client software packages, see Download Cisco Secure Client.

For macOS, download and deploy the Cisco Secure Client version 5.1.8.105 (**cisco-secure-client-macos-5.1.8.105-predeploy-k9.pkg**) or newer.

Copy URL for Default PAC File or Custom PAC File

Describes Copy URL for Default PAC File or Custom PAC File in Cisco Secure Access. Copy the URL for the default Secure Access PAC file or a custom PAC file that you uploaded to Secure Access.

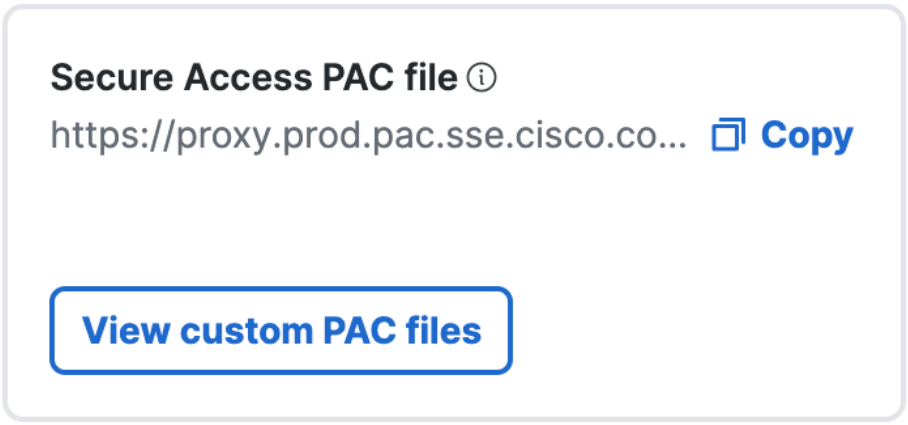
Copy the URL for the default Secure Access PAC file or a custom PAC file that you uploaded to Secure Access.

Copy URL for Secure Access PAC File

Provides instructions for completing the Copy URL for Secure Access PAC File workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Internet Security .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. For **Secure Access PAC file**, click **Copy** to get Secure Access PAC file URL.

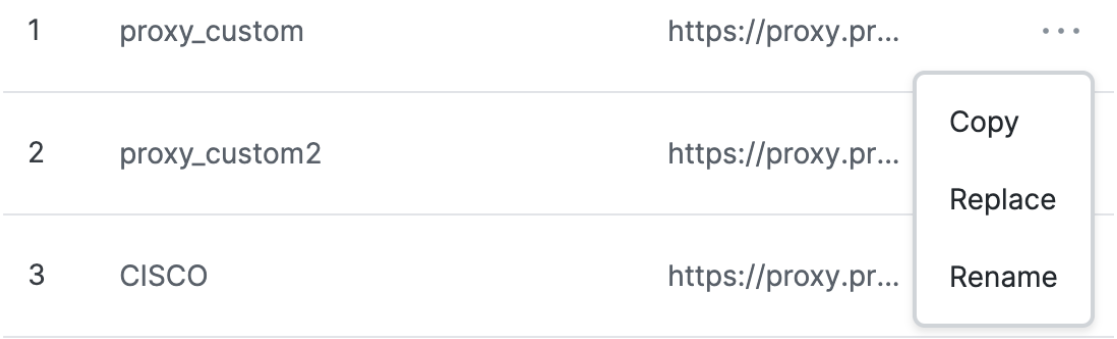


Copy URL for Custom PAC File

Provides instructions for completing the Copy URL for Custom PAC File workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Internet Security .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Click **View the custom PAC files**.
3. Navigate to a custom PAC file, and then click the ellipsis (**...**).



4. Click **Copy**, and then copy the URL for the custom PAC file.

Procedure

Describes Procedure in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

> **Note**
>
> Operating system (OS) and browser functionality can change at any time. We can not guarantee that these third-party procedures will remain accurate. For more information on deploying a PAC file URL to your browser, see your OS and browser's Help.

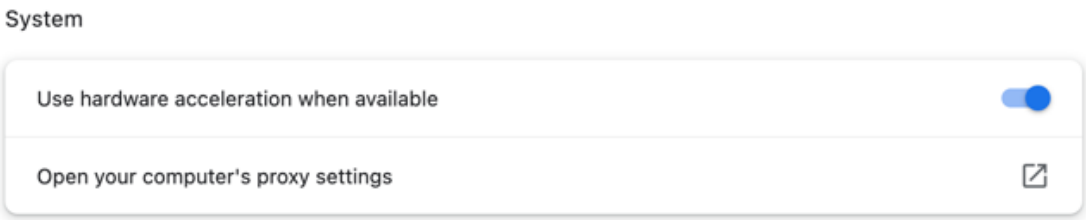
Deploy the Secure Access PAC File URL to Chrome

Provides instructions for completing the Deploy the Secure Access PAC File URL to Chrome workflow in Cisco Secure Access. Get the URL for the Secure Access PAC file or a custom PAC file.

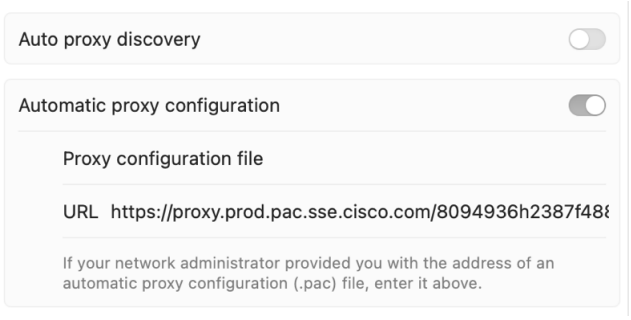
Get the URL for the Secure Access PAC file or a custom PAC file. For more information, see Copy URL for Default PAC File or Custom PAC File.

Procedure

1. In your Chrome browser, navigate to **chrome://settings/system** and click **Open your computer's proxy settings**.



2. Enable **Automatic proxy configuration** and paste the Secure Access PAC file URL.



3. Click **OK** and then **Apply**.

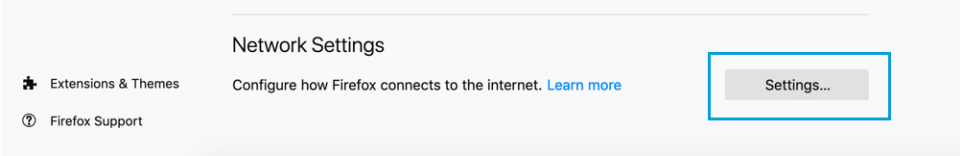
Deploy the Secure Access PAC File URL to Firefox

Provides instructions for completing the Deploy the Secure Access PAC File URL to Firefox workflow in Cisco Secure Access. Get the URL for the Secure Access PAC file or a custom PAC file.

Get the URL for the Secure Access PAC file or a custom PAC file. For more information, see Copy URL for Default PAC File or Custom PAC File.

Procedure

1. Open your Firefox browser, navigate to **Firefox** > **Preferences**, scroll to **Network Settings**, and click **Settings**.



2. Check **Automatic Proxy Configuration URL** and paste the Secure Access PAC file URL.
3. Click **OK**.

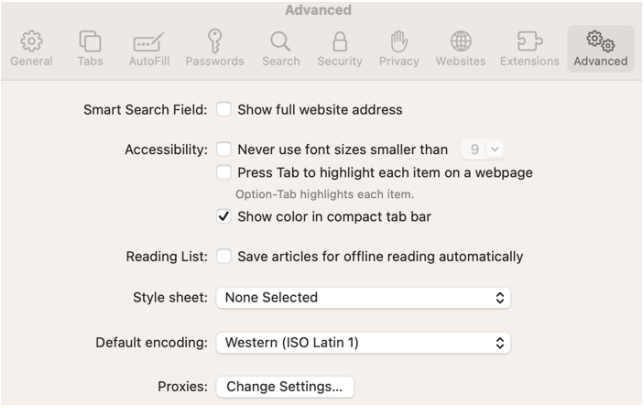
Deploy the Secure Access PAC File URL to Safari

Provides instructions for completing the Deploy the Secure Access PAC File URL to Safari workflow in Cisco Secure Access. Get the URL for the Secure Access PAC file or a custom PAC file.

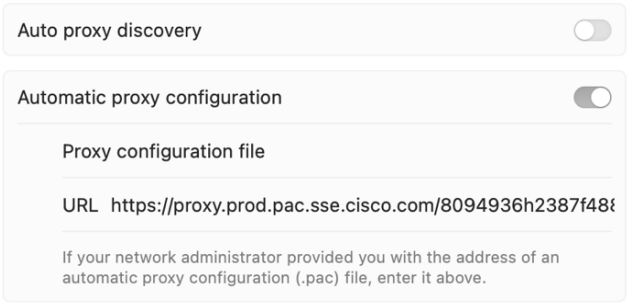
Get the URL for the Secure Access PAC file or a custom PAC file. For more information, see Copy URL for Default PAC File or Custom PAC File.

Procedure

1. Open your Safari browser, navigate to **Safari** > **Settings** > **Advanced**, and then click **Change Settings**.



2. Enable **Automatic proxy configuration** and paste the Secure Access PAC file URL.



3. Click **OK** and then **Apply**.

Customize the Secure Access PAC File

Describes Customize the Secure Access PAC File. You can create custom PAC files to use with the browsers on the user devices in the organization.

You can create custom PAC files to use with the browsers on the user devices in the organization.

To bypass domains, add domains in Secure Access where the web traffic on these domains will bypass the secure web gateway (SWG). Secure Access includes the configured bypass domains in the Secure Access PAC file. For information about bypass domains, see Manage Internet Security Bypass.

After you download the Secure Access PAC file from Secure Access, you can edit the file and add more domains. Then, upload the custom PAC file to Secure Access or host this PAC file in your environment. Secure Access does not modify a custom PAC file. Secure Access only modifies the Secure Access PAC file with the bypass domains that you add in Secure Access.

Note

Secure Access supports IP-based domains. You must enter the IP in the browser's address bar as the domain portion of the URL. For example, **https://1.2.3.4/URLpath/**. The PAC file does not resolve a domain to IP before matching an IP-based domain for bypass.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- To download the Secure Access PAC file or custom PAC files on a user device in the organization, the device must either:
  - Connect to Secure Access on a Registered Network or Network Tunnel, or
  - Deploy the Cisco Secure Client with the Umbrella Roaming Security module on the user device.

For more information, see Manage PAC Files.

Procedure for Customizing the Secure Access PAC File

Describes Procedure for Customizing the Secure Access PAC File. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

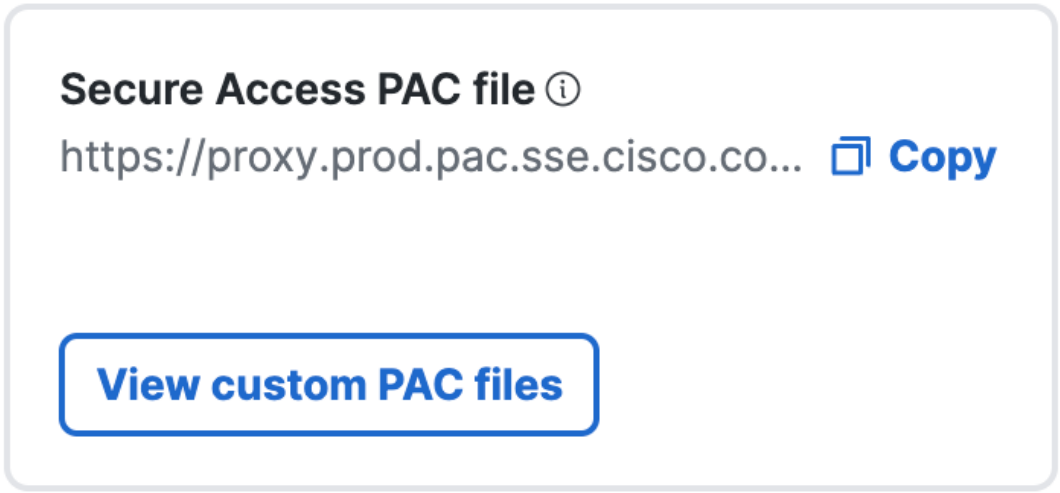
Copy the Secure Access PAC File URL. Then, enter the PAC file URL in your browser and download the PAC file. Open the Secure Access PAC file in an editor and update the file.

Copy the Secure Access PAC File

Provides instructions for completing the Copy the Secure Access PAC File workflow in Cisco Secure Access. Navigate to Connect End User Connectivity Internet Security .

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. For **Secure Access PAC File**, click **Copy** to get the PAC file URL.

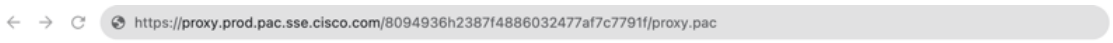


Download the Secure Access PAC File

Provides instructions for completing the Download the Secure Access PAC File workflow in Cisco Secure Access. Paste the copied PAC URL into a browser's address bar and then press Enter or Return to download the PAC file.

Procedure

Paste the copied PAC URL into a browser's address bar and then press **Enter** or **Return** to download the PAC file.



Edit the PAC File

Provides instructions for completing the Edit the PAC File workflow in Cisco Secure Access. Open the downloaded PAC file with a text editor.

Procedure

1. Open the downloaded PAC file with a text editor.
2. Add the internal domains that the web proxy will bypass to the PAC file, and then save the file.

   Note

   Provide a comma-delimited list of domain names and surround each domain name in the list with quotation marks. The wildcard character asterisk ***** is supported and treated as any value of any length. Use caution when using wildcards as well as periods. For example, ***.example.com** bypasses www.example.com, **mail.example.com**, and **c.23.example.com**. ***example.com** bypasses www.example.com as well as **phishingexample.com**.

3. Save the PAC file.

What to do next

```
function FindProxyForURL(url, host) {

        //------------------------Customer Section-----------------------
        //Add your internal domains within quotations marks like
"wwwin.acme.com"
        //after the right parenthesis below. Please remove the two examples
        //below and add your own internal domains.

        var dont_proxy_customer_list =
[redacted]


        //Warning to Administrators: Touching any section after this point
might
       //affect your users browsing experience and lead to considerable number

        //of issues and loading your customer support.
        //----------------------End Customer Section-----------------------

        for(var iter = 0; iter < dont_proxy_customer_list.length; ++iter) {
            if(shExpMatch(host, dont_proxy_customer_list\[iter\])) {
                return "DIRECT";
            }
        }
```

Upload Custom PAC Files to Secure Access

Provides instructions for completing the Upload Custom PAC Files to Secure Access workflow in Cisco Secure Access. Uploading custom PAC files to Secure Access requires the following.

You can create custom PAC files to manage web traffic on browsers. To bypass domains on the secure web gateway (SWG), add the bypass domains to the custom PAC files manually, and then upload the custom PAC files to Secure Access. Once uploaded, the custom PAC files are available on Secure Access for you to use in the organization's environment.

Secure Access supports IP-based domains. However, you must enter the IP in the browser's address bar as the domain portion of the URL. For example, `https://1.2.3.4/URLpath/`. The PAC file does not resolve a domain to IP before matching an IP-based domain for bypass.

Before you begin

Uploading custom PAC files to Secure Access requires the following.

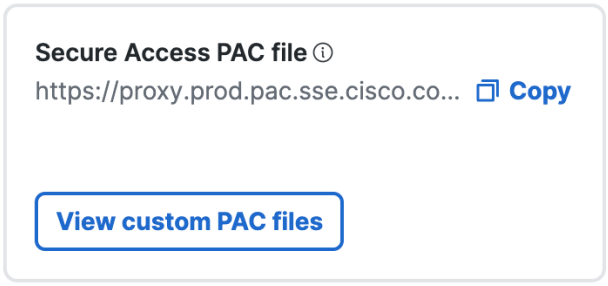
- Full Admin user role. For more information, see Manage Accounts.
- PAC files uploaded to Secure Access must meet the following requirements:
  - Each custom PAC file size is 500KB or less.
  - Filenames are unique.
  - Filenames are case sensitive.
  - Filenames can include alphanumeric characters, hyphens, and underscores.
  - Files have the `.pac` extension.

Note

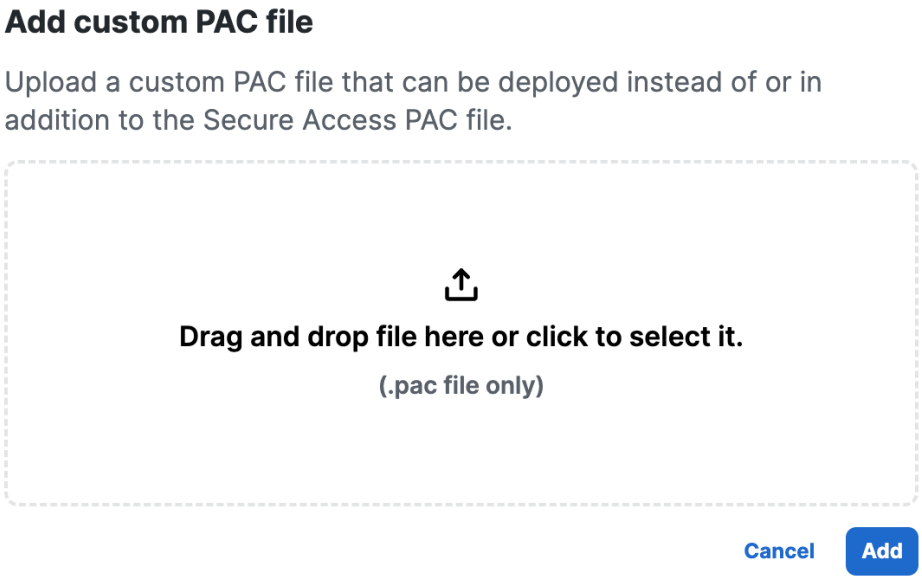
No more than ten custom PAC files can be uploaded in Secure Access.

Procedure

1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**, then click **View custom PAC files**.



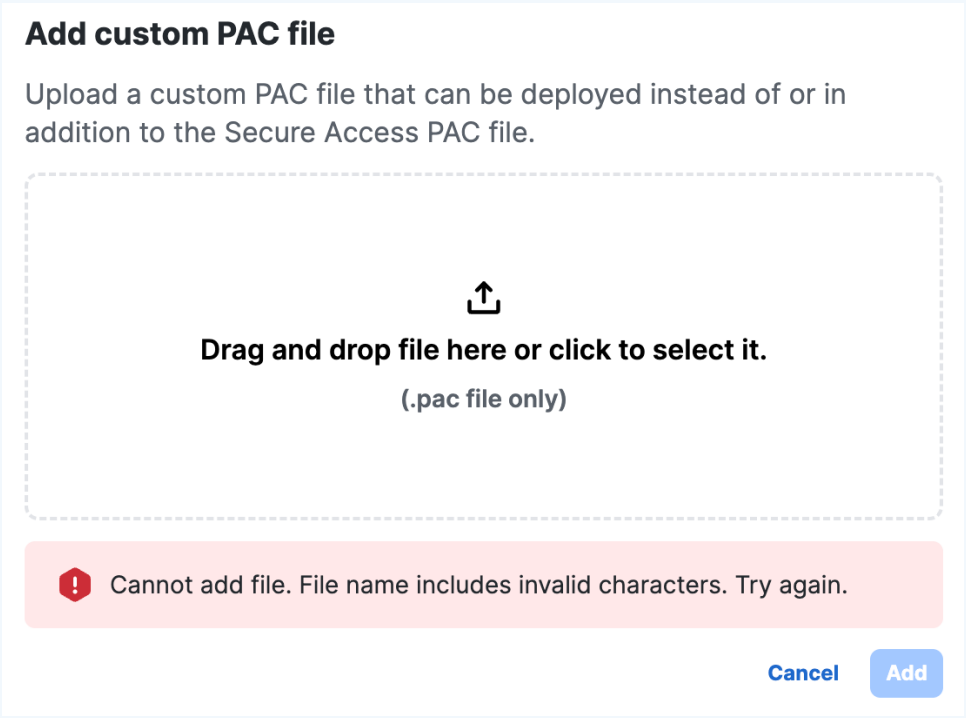
2. Under **Custom PAC Files**, click **Add custom PAC file**.
3. Drag and drop your custom PAC file or click the text area to select a custom PAC file from your local system.



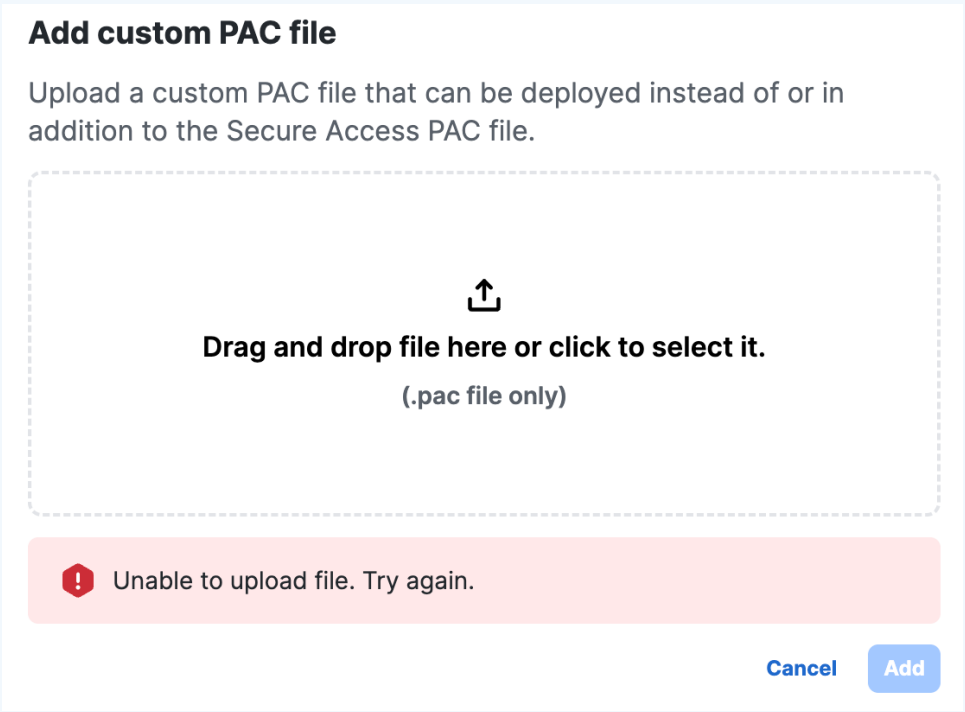
4. After you upload your custom PAC file, click **Add**.

Note

Uploading a PAC file with an invalid file name will result in an error. For more information, see the **Prerequisites** above.



Clicking **Add** without first uploading a file will result in an error.



Manage Uploaded Custom PAC Files

Provides instructions for completing the Manage Uploaded Custom PAC Files workflow in Cisco Secure Access. View uploaded custom PAC files, get the URL for a custom PAC file, replace the contents of the custom PAC file, or rename the custom PAC file in Secure Access.

View uploaded custom PAC files, get the URL for a custom PAC file, replace the contents of the custom PAC file, or rename the custom PAC file in Secure Access.

Procedure

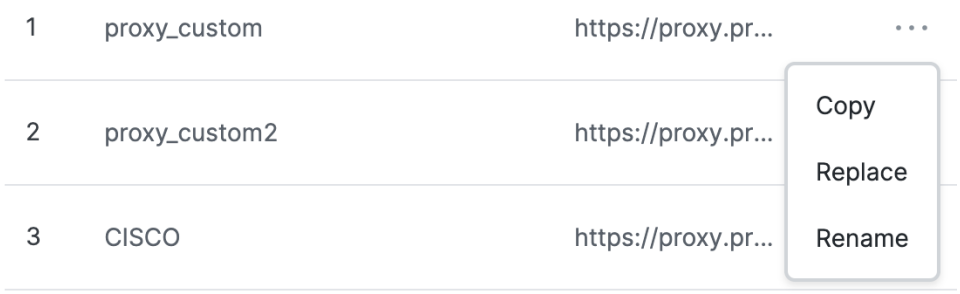
1. Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
2. Click **View the custom PAC files**.

#	PAC File Name	Link	
1	proxy_custom	https://proxy.pr...	···
2	proxy_custom2	https://proxy.pr...	···
3	CISCO	https://proxy.pr...	···

The table of PAC files shows the following information:

- **#** (pound sign)– The number of the custom PAC file.
- **PAC File Name**–The filename of the custom PAC file.
- **Link**–The link to the URL for the custom PAC file.

3. To copy a PAC file URL, replace a PAC file with a new uploaded file, or rename a custom PAC file, navigate to the PAC file in the table, click the **ellipsis (...)**, then click **Copy**, **Replace**, or **Rename**.



55 Certificates

Topics:

- Manage Certificates
- Certificates for Internet Decryption
- Manage Certificates for Private Resource Decryption
- Install the Cisco Secure Access Root Certificate
- Add Custom CA Signed Root Certificate
- View the Cisco Trusted Root Store
- Certificates for SAML Authentication
- VPN Certificates for User and Device Authentication
- Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment

Provides an overview of Certificates in Cisco Secure Access, including Manage Certificates, Certificates for Internet Decryption, and Manage Certificates for Private Resource Decryption. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Certificates

Describes Manage Certificates in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Certificates are used for various purposes in Secure Access:

- Decrypting traffic to private and internet resources for threat detection.
- Presenting notification pages for blocked and warned internet destinations.
- Establishing trust between Secure Access and your identity providers for SAML authentication. For more information, see Certificates for SAML Authentication.
- Authenticating users and devices in VPN connections. For more information, see VPN Certificates for User and Device Authentication.

Certificate Installation Methods

Describes Certificate Installation Methods in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Certificate installation can be done on a per-browser or per-machine basis. For larger deployments, you can perform an automatic installation through Group Policy Objects (GPO). Note that the automatic installation through GPO is only supported for the Edge or Chrome browsers on Windows systems. As such, for Firefox or Safari browsers, and for users on non-Windows operating systems, you must perform the manual installation procedure.

You can also install a certificate automatically—through Active Directory Group Policy Objects—for a group of users in Microsoft Windows Active Directory. This automatic installation of a certificate is only supported for Edge or Chrome browsers on Windows systems. For all other browsers and systems, you must perform the manual installation procedure.

For more information, see Install the Cisco Secure Access Root Certificate.

Certificates for Internet Decryption

Describes Certificates for Internet Decryption in Cisco Secure Access and explains Certificates for Displaying Notifications. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Certificates are required for secure internet access. Specifically, certificates are required to decrypt traffic in order to inspect it for threats, and to present notifications to end users when access is blocked or triggers a warning. Web security features and the intrusion prevention (IPS) feature all require decryption in order to be effective.

End-user devices that connect to resources through Secure Access must trust the connection with Secure Access. You must set up certificates to establish this trust.

For internet traffic, depending on the features you need, there are two ways for end-user devices to validate the certificate that Secure Access presents to end-user devices that connect to internet resources through Secure Access:

1. You can install the self-signed Secure Access certificate into the browser trust stores of all end-user endpoint devices, or
2. You can sign the Secure Access certificate using your corporate certificate authority (CA) so that it can be validated by an existing certificate in the trust store of end-user devices. This method also allows you to easily revoke the certificate if needed, without having to update all end-user devices.

Certificates for Displaying Notifications

You can use only this method:

- Option 1: Distribute Self-Signed Certificates to End-User Devices

Certificates for Decrypting Internet Traffic

Describes Certificates for Decrypting Internet Traffic in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can use either of these methods:

- Option 1: Distribute Self-Signed Certificates to End-User Devices
- Option 2: Use a Signed Certificate

Option 1: Distribute Self-Signed Certificates to End-User Devices

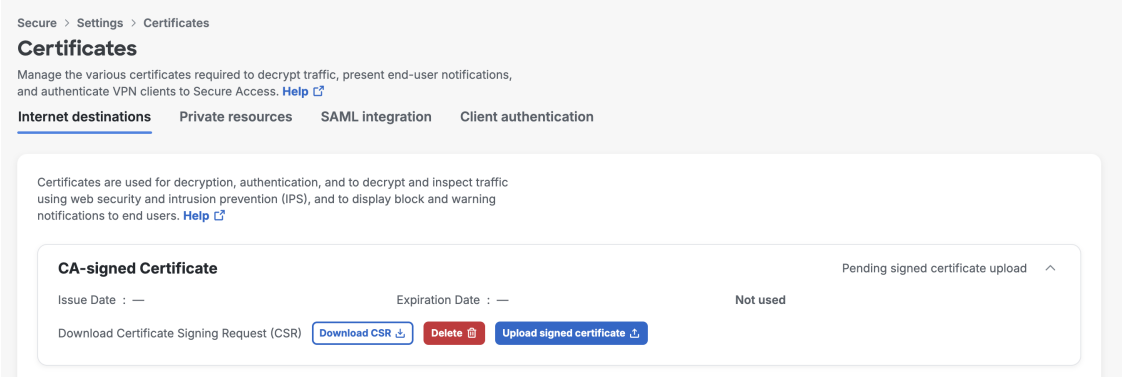
Provides instructions for completing the Option 1: Distribute Self-Signed Certificates to End-User Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Certificates** and click the **Internet destinations** tab.
2. Expand **CA-signed certificate**.



3. Download the certificate.
4. Install the downloaded certificate in the trust store of all devices in your organization. For more information, see Certificate Installation Methods.

What to do next

Identify the certificate

The SHA1 hash of the file uniquely identifies the certificate file; you can use it to determine whether a file is this file, and whether the file has been modified from the original.

Option 2: Use a Signed Certificate for Decrypting Internet Traffic

Describes Option 2: Use a Signed Certificate for Decrypting Internet Traffic in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

If your organization's managed devices already have the root certificate required to validate certificates signed by your corporate certificate authority (CA), you can sign the Secure Access certificate with your corporate CA, instead of installing the Secure Access self-signed certificate on every end-user device. This certificate cannot be used to display notifications. For more information, see Add Customer CA Signed Root Certificate.

Manage Certificates for Private Resource Decryption

Describes Manage Certificates for Private Resource Decryption in Cisco Secure Access. Private resources are applications, networks, or subnets that are not publicly accessible from outside your network.

Private resources are applications, networks, or subnets that are not publicly accessible from outside your network. Protect your private resources with the Secure Access Intrusion Prevention (IPS) profile and Data Loss Prevention (DLP) policy.

To connect user traffic with a private resource and decrypt that traffic for inspection by the IPS or the DLP policy, Secure Access requires a certificate. When you configure a private resource and enable decryption, you must upload the hosting server's certificate to Secure Access. Endpoint devices must be able to validate the certificates that you upload.

Include any intermediate certificates required to complete the certificate chain. If multiple resources are hosted from a single server, you can use a single certificate for all of those resources.

You can upload and manage the use of your certificates with private resources in Secure Access. For more information, see Upload Private Resource Certificates.

Install a Certificate Authority Certificate on a Private Resource

Describes Install a Certificate Authority Certificate on a Private Resource in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Before you install a certificate on a private resource, complete or meet these prerequisites:

- Add a private resource in Secure Access with decryption enabled. Secure Access uses decryption to inspect traffic with Intrusion Prevention (IPS) and the Data Loss Prevention policy or validate a custom domain. For more information about private resources, see Add a Private Resource.

Secure Access requires a Privacy-Enhanced Mail (PEM) formatted certificate and key. Install your corporate Certificate Authority (CA) root certificate on the private resource in your organization. For more information, see Upload Private Resource Certificates.

Upload Private Resource Certificates

Provides instructions for completing the Upload Private Resource Certificates workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can upload a certificate key pair directly on a private resource in Secure Access. For more information, see Add a Private Resource: Decryption.

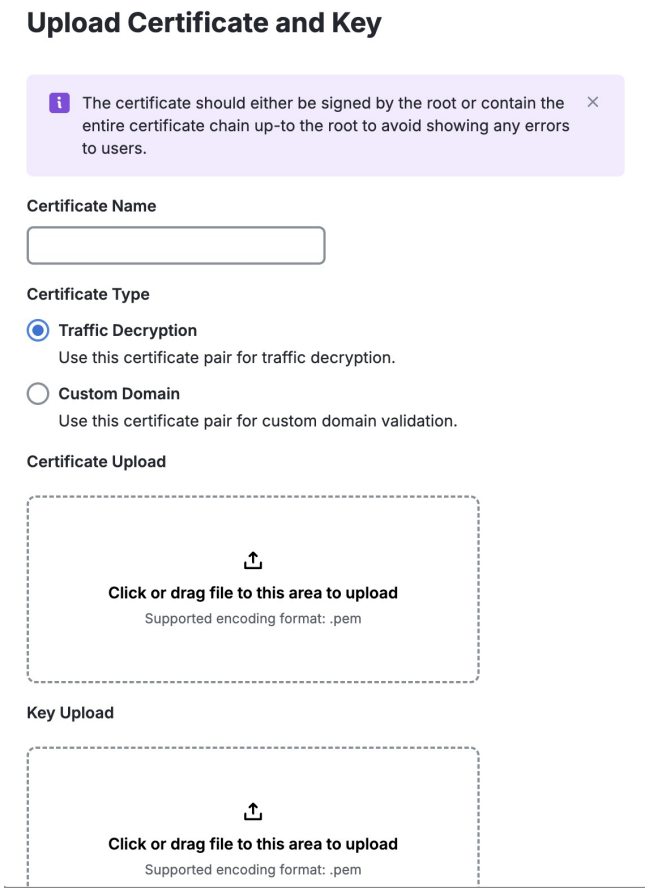
Alternatively, upload certificates for any private resources in Secure Access. When you configure a private resource you can select from the list of certificates.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Certificates** > **Private Resources**.
2. Click **Upload Certificate and Key**.



3. Customize the certificate name, upload the hosting server's certificate and any intermediate certificates required to complete the chain, then click **Save**.

What to do next

Navigate to **Resources** > **Private Resources** to configure the private resource to use this certificate-key pair.

View Notifications About Expired Private Resource Certificates

Provides instructions for completing the View Notifications About Expired Private Resource Certificates workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

When a certificate for the decryption of a private resource has expired or will expire within 90 days, Secure Access displays an expiry banner on the Private Resources page.

Users with the **Full Admin** or **Security Administrator** role can close the banner, or replace or delete the certificates. If the certificate is not updated, the expiry banner will reappear the next time you open the **Private Resources** page.

For information about uploading certificates, see Upload Private Resource Certificates.

For information about viewing the certificates for private resources in the organization or replacing or deleting the certificates, see View, Replace or Delete Private Resource Certificates

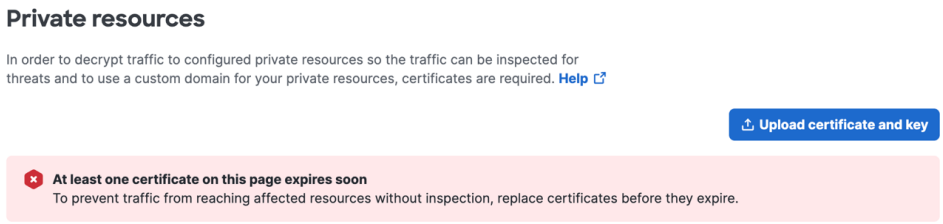
Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Certificates** .
2. Click the **Private resources** tab.

   If a certificate for the decryption of a private resource has expired or will expire within 90 days, Secure Access displays a notification.



View, Delete, or Replace a Private Resource Certificate

Provides instructions for completing the View, Delete, or Replace a Private Resource Certificate workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

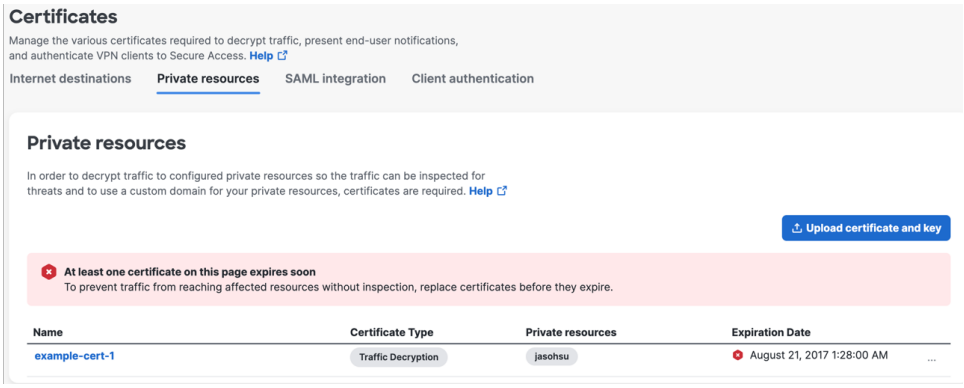
After uploading certificates for the private resources in an organization, administrators can view, replace, or delete the certificates.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Secure** > **Certificates**.



2. Click the **Private resources** tab and navigate to the table of certificate information.

   Secure Access displays the details about each certificate uploaded for the private resources in the organization.

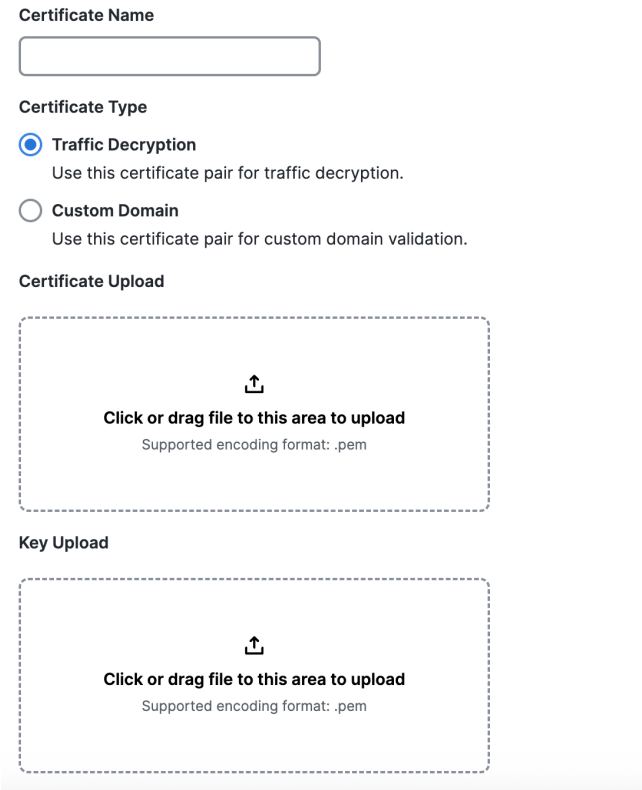
   - **Name**–The name used to identify the certificate in the organization.
   - **Certificate type**–The label that describes how the system uses the certificate, either **Traffic Decryption** or **Custom Domain**.
   - **Private resources**–The list of the private resources that are associated with the certificate.
   - **Expiration date**–The date and time when the certificate expires.

a) To modify a certificate, click on the name of certificate in the table and then choose **Delete** or **Replace certificate and key**, or click the ellipsis (**...**) at the end of a row in the table and then choose **Delete** or **Replace**.

You can modify the name of the certificate and the certificate and key.

3. To replace a certificate, upload a new certificate and key, and then click **Save**.

The certificate should either be signed by the root or contain the entire certificate chain up-to the root to avoid showing any errors to users.



4. To delete a certificate, click **Delete**.

If the certificate is in use by a private resource, you can not remove the certificate. Instead, modify or remove the private resource or replace the certificate.

a) Click **Delete** to confirm the deletion of the certificate.

Install the Cisco Secure Access Root Certificate

Describes Install the Cisco Secure Access Root Certificate. A root certificate or your own Certificate Authority (CA) signed root certificate is required where Cisco Secure Access must proxy and decrypt HTTPS traffic that requests a web resource.

A root certificate or your own Certificate Authority (CA) signed root certificate is required where Cisco Secure Access must proxy and decrypt HTTPS traffic that requests a web resource.

The procedures on this page describe how to download and install the Cisco Secure Access root certificate. You can also use these procedures to install your own CA signed root certificate.

Prerequisites

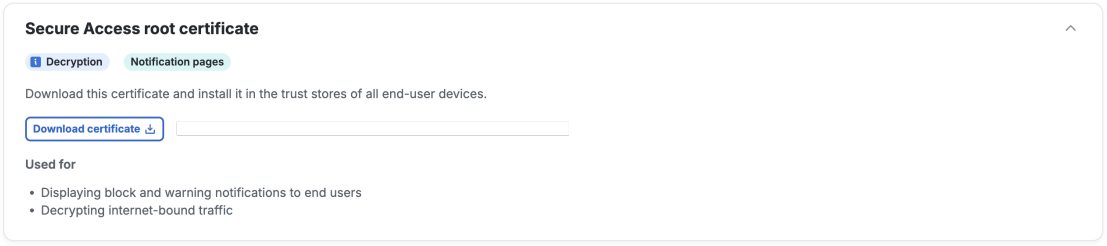
- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.
- Full Admin user role. For more information, see Manage Accounts.

Download the Cisco Secure Access Root Certificate

Provides instructions for completing the Download the Cisco Secure Access Root Certificate workflow in Cisco Secure Access. Navigate to Secure Certificates Internet destinations , and then expand Secure Access root certificate.

Procedure

1. Navigate to **Secure** > **Certificates** > **Internet destinations**, and then expand **Secure Access root certificate**.



2. Click **Download certificate** to download the **Cisco_Secure_Access_Root_CA.cer** file.

Automatically Install the Cisco Secure Access Root Certificate (For an Active Directory Network)

Describes Automatically Install the Cisco Secure Access Root Certificate (For an Active Directory Network). It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

As a network administrator of an Active Directory network environment, you can automatically install the Cisco Secure Access root certificate in all of your users' browsers by creating a Group Policy Object (GPO) on your Active Directory server. Create a GPO using either the Microsoft Management Console (MMC) or the Group Policy Management Console (GPMC).

- Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC)
- Install the Cisco Secure Access Root Certificate with Group Policy Using the Group Policy Management Console (GPMC)

Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC)

Provides instructions for completing the Install the Cisco Secure Access Root Certificate with Group Policy Using the Microsoft Management Console (MMC) workflow in Cisco Secure Access. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Log into your Active Directory server using a domain administrator account.
2. Select **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**. The Microsoft Management Console (MMC) is displayed.

3. To create a domain-wide policy, right-click your domain root Organizational Unit (OU), which is displayed as your domain name, and select **Properties** from the context menu.
4. In the <*OU_Name*> Properties dialog box, click the **Group Policy** tab.
5. Click **New**, name the policy Secure Access Certificate Installer, and press **Return / Enter**.
6. Select the new Group Policy Object and click **Edit**. The Group Policy Object Editor is displayed.
7. In the configuration options sidebar, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and select **Import**.
8. In the Certificate Import wizard, click **Next**, and in the File to Import page, click **Browse**. Navigate to where you downloaded the certificate authority on your local system, and double-click the **Cisco_Secure_Access_Root_CA.cer** file.
9. With the full path to the certificate displayed in the **File name** field, click **Next**.
10. Accept the default option, place all certificates in the following store (Trusted Root Certification Authorities), click **Next**, and then click **Finish** and **OK**.

What to do next

You have now created the Group Policy Object to install the Cisco Secure Access root certificate on all of the computers in your domain. The new policy may not take effect immediately on all client machines. By default, the background synchronization processing happens every 90 to 120 minutes at randomized times. Rebooting client machines forces the synchronization.

You can check that the Group Policy has propagated to all computers in the domain by opening your browser on a workstation, opening Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities, and ensuring that the Cisco Secure Access root certificate is present.

Install the Cisco Secure Access Root Certificate with Group Policy Using the Group Policy Management Console (GPMC)

Provides instructions for completing the Install the Cisco Secure Access Root Certificate with Group Policy Using the Group Policy Management Console (GPMC) workflow in Cisco Secure Access. The Microsoft Group Policy Management Console (GPMC) with Service Pack 1 (SP1) unifies the management of Group Policy across the enterprise.

The Microsoft Group Policy Management Console (GPMC) with Service Pack 1 (SP1) unifies the management of Group Policy across the enterprise. The GPMC consists of an MMC snap-in and a set of programmable interfaces for managing Group Policy.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

---

1. Log into your Active Directory server using a domain administrator account.
2. Select **Start** > **All Programs** > **Administrative Tools** > **Group Policy Management**. The Group Policy Management Console (GPMC) appears.
3. To create a domain-wide policy, right-click your domain root **Organizational Unit (OU)**, which is displayed as your domain name, and select **Create and Link a GPO Here** from the context menu.

   The New GPO dialog box appears.
4. In the **Name** field of the New GPO dialog box, enter a meaningful name for the policy object.
5. Right-click the new **Group Policy Object**, **Secure Access Certificate Installer**, on the right side of the window, and select **Edit** from the context menu. The Group Policy Object Editor appears.

6. In the left configuration options sidebar, expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and select **Import**from the context menu.
7. In the Certificate Import wizard click **Next**, and in the File to Import page, click **Browse** and navigate to where you downloaded the certificate authority on your local system, and double-click the **Cisco_Secure_Access_Root_CA.cer** file.
8. With the full path to the certificate displayed in the **Filename** field, click **Next**.
9. Accept the default option, Place all certificates in the following store (Trusted Root Certification Authorities), click **Next**, then click **Finish** and **OK**.

What to do next

You have now created the Group Policy Object to install the Cisco Secure Access root certificate on all of the computers in your domain. The new policy may not take effect immediately on all client machines. By default, the background synchronization processing “only” happens every 90 to 120 minutes (at randomized times). Rebooting client machines forces the synchronization.

You can check that the Group Policy has propagated to all computers in the domain by opening your browser on a workstation, opening Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities, and ensuring that the Cisco Secure Access root certificate is present.

Install the Cisco Secure Access Root Certificate in Firefox Using Group Policy

Describes Install the Cisco Secure Access Root Certificate in Firefox Using Group Policy. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By default, Group Policy cannot configure Firefox. In general, deploying the Cisco Secure Access root certificate can be difficult in Firefox because there is no built-in way to centrally manage Firefox.

Install the Cisco Secure Access Root Certificate on Chromebooks Using the Google Admin Console

Describes Install the Cisco Secure Access Root Certificate on Chromebooks Using the Google Admin Console. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Using the Google Admin console, you can deploy certificates to your Chromebooks. For more information, see Google Support-Set Up Certificates.

Manually Install the Cisco Secure Access Root Certificate (Single Computer)

Describes Manually Install the Cisco Secure Access Root Certificate (Single Computer). It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows
- Install the Cisco Secure Access Root Certificate in Firefox on Windows
- Install the Cisco Secure Access Root Certificate in All Browsers on Mac OS X
- Install the Cisco Secure Access Root Certificate on Mac OS X Through the Command Line
- Install the Cisco Secure Access Root Certificate in Chromium or Chrome on Linux

Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows

Provides instructions for completing the Install the Cisco Secure Access Root Certificate in Edge or Chrome on Windows workflow in Cisco Secure Access. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Click **Install Certificate**.
2. In the Certificate Import wizard, click **Next**.
3. In the Certificate Store window, select **Place all certificates in the following store** and then click **Browse**.
4. In the Select Certificate Store window, select **Trusted Root Certification Authorities** and click **OK**.

   In the Certificate Store window, the Certificate store shows **Trusted Root Certification Authorities**.
5. Click **Next** and then click **Finish**.
6. In the Security Warning windows, click **Yes** to install the certificate.

   If the certificate installed successfully, the Certificate Import wizard displays "The import was successful.".
7. Click **OK**.
8. Restart the browser.

Install the Cisco Secure Access Root Certificate in Firefox on Windows

Provides instructions for completing the Install the Cisco Secure Access Root Certificate in Firefox on Windows workflow in Cisco Secure Access. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Click the **Open Menu** icon near the top right-hand corner of the browser window.
2. Click **Options** > **Advanced** > **Certificates** > **View Certificates** > **Authorities** > **Import**.
3. Browse for and select the Cisco Root Cert, downloaded in the first step.
4. Select **Trust this Certificate to identify websites**, then click **OK** and **OK** again.
5. Restart Firefox.

   To interact with the Firefox certificate store from the command line, use the **certutil** tool from the NSS Tools package. For more information, see Using the Certificate Database Tool.

Install the Cisco Secure Access Root Certificate in All Browsers on Mac OS X

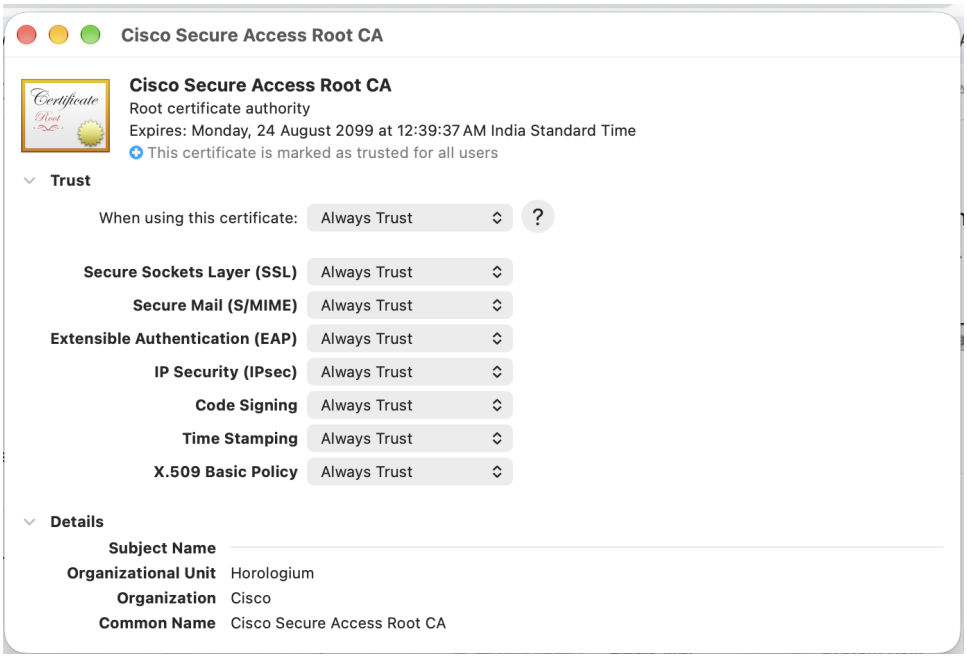
Provides instructions for completing the Install the Cisco Secure Access Root Certificate in All Browsers on Mac OS X workflow in Cisco Secure Access. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

1. Double-click the file or drag and drop it on top of the Keychain Access icon in the `Applications | Utilities` folder. The Add Certificate window appears.

2. Click **Always Trust**.
3. Double-click the Cisco Secure Access root certificate to open its properties window. From the **When using this certificate** drop-down menu, choose **Always Trust**.



Install the Cisco Secure Access Root Certificate on Mac OS X Through the Command Line

Provides instructions for completing the Install the Cisco Secure Access Root Certificate on Mac OS X Through the Command Line workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

Run the following command:

What to do next

```
sudo /usr/bin/security add-trusted-cert -d -r trustRoot -p ssl -p basic -k
/Library/Keychains/System.keychain /path/to/Cisco_Secure_Access_Root_CA.cer
```

Install the Cisco Secure Access Root Certificate in Chromium or Chrome on Linux

Provides instructions for completing the Install the Cisco Secure Access Root Certificate in Chromium or Chrome on Linux workflow in Cisco Secure Access. Before you begin, download the Cisco Secure Access root certificate.

Before you begin, download the Cisco Secure Access root certificate. See Download the Cisco Secure Access Root Certificate.

Procedure

---

1. Open Chromium Settings.
2. Scroll down to **HTTPS/SSL**.

3. Click **Manage certificates**.
4. Click **Authorities**.
5. Click **Import**.
6. Select the **Cisco_Secure_Access_Root_CA.cer** file and click **Open**.
7. Select **Trust this CA to identify Websites**.
8. Click **OK**.

Add Custom CA Signed Root Certificate

Describes Add Custom CA Signed Root Certificate in Cisco Secure Access. You can use a certificate signed by your Certificate Authority (CA) to enable secure connections between user devices in your organization and Cisco Secure Access.

You can use a certificate signed by your Certificate Authority (CA) to enable secure connections between user devices in your organization and Cisco Secure Access.

A root certificate is required for Block Pages and Internet Decryption.

- For Block Pages, if you visit a blocked domain through HTTPS, a certificate must be installed so that Secure Access presents a block page rather than a browser error. For more information, see Manage Notification Pages.
- For HTTPS decryption and inspection, if a domain is proxied, install a certificate so that Secure Access can decrypt HTTPS traffic without the browser presenting an error. For more information, see Manage Traffic Decryption.

You can use either the Cisco Secure Access root certificate or your own CA-signed certificate. To use your own CA-signed certificate, upload a certificate signed by your CA to Secure Access.

Prerequisites

- A Certificate Signing Request (CSR) file downloaded from Secure Access.
- Microsoft Certificate Services, Active Directory Certificate Services, or OpenSSL to sign the CSR with your CA.

Certificate Requirements

Describes Certificate Requirements in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

When you issue a certificate signed by your own CA, you must meet the following requirements:

- The encoding must use UTF8String.
- You must use the same character encoding for all certificates in your certificate chain.
- The “Subject Name” in the CSR file downloaded from Secure Access must be honored.
  - The certificate must be valid for no more than three years.
  - The certificate must be an X509v3 certificate with an RSA public key not less than 2048 and no more than 4096.
- Use one of the following signature algorithms:
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
- Include the following X509v3 extensions:
  - X509v3 Basic Constraints marked as critical: **CA:TRUE**
  - X509v3 Key Usage, marked as critical: **Certificate Sign**, **CRL Sign**

Install Root Certificate in Browsers

Describes Install Root Certificate in Browsers in Cisco Secure Access. For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

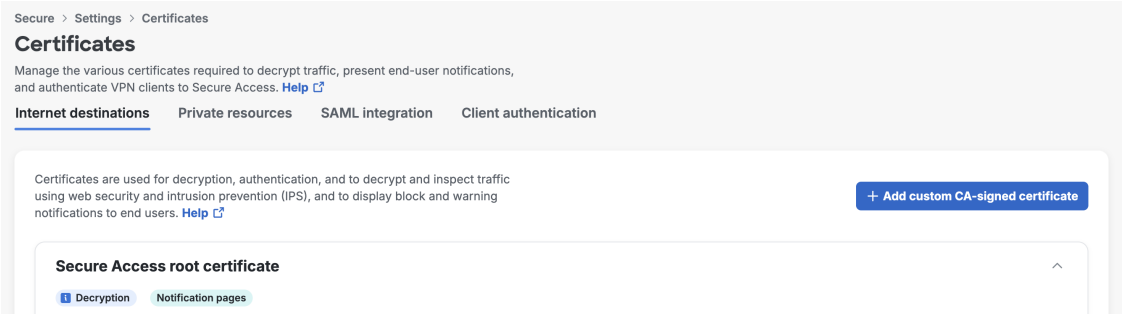
For information about how to install certificates in browsers, see Install the Cisco Secure Access Root Certificate.

Adding a Custom CA Signed Root Certificate

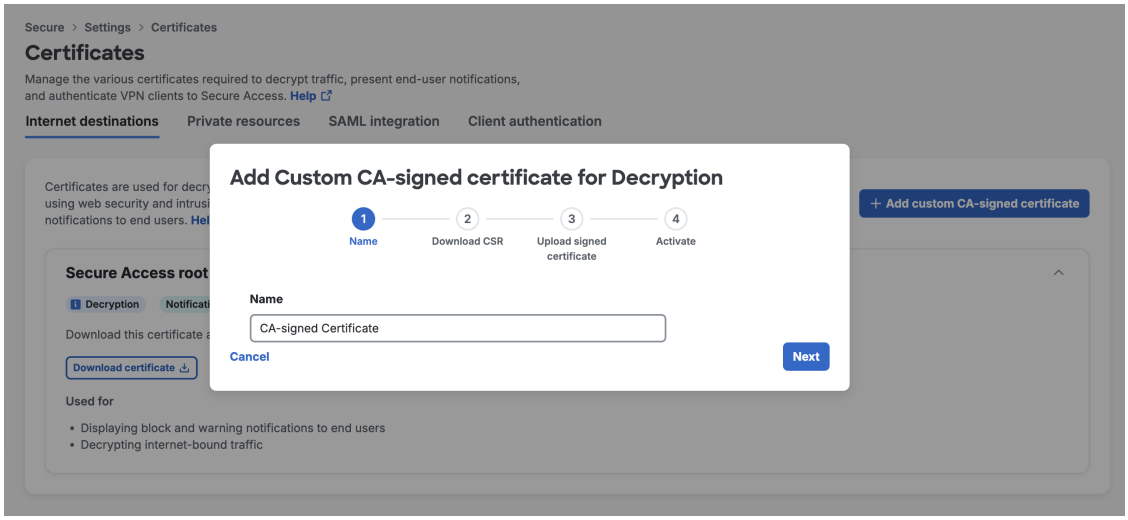
Provides instructions for completing the Adding a Custom CA Signed Root Certificate workflow in Cisco Secure Access. Navigate to Secure Certificates Internet destinations , and click Add custom CA-signed certificate.

Procedure

1. Navigate to **Secure** > **Certificates** > **Internet destinations** > , and click **Add custom CA-signed certificate**.



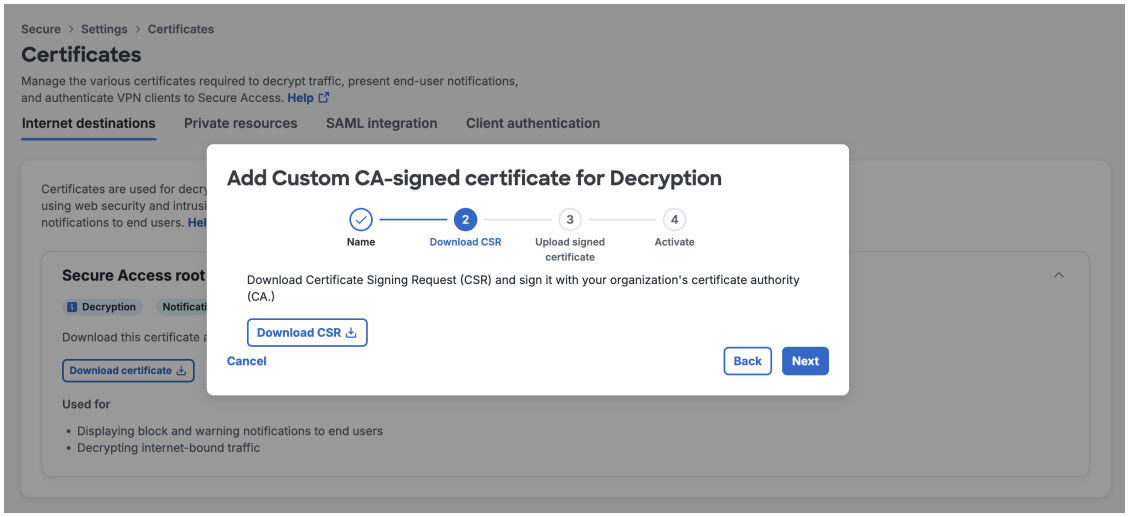
2. Enter a descriptive name for your certificate, and then click **Next**.



3. Click **Download CSR** to save the Secure Access Certificate Signing Request (.csr) file to the local system, and then click **Next**.

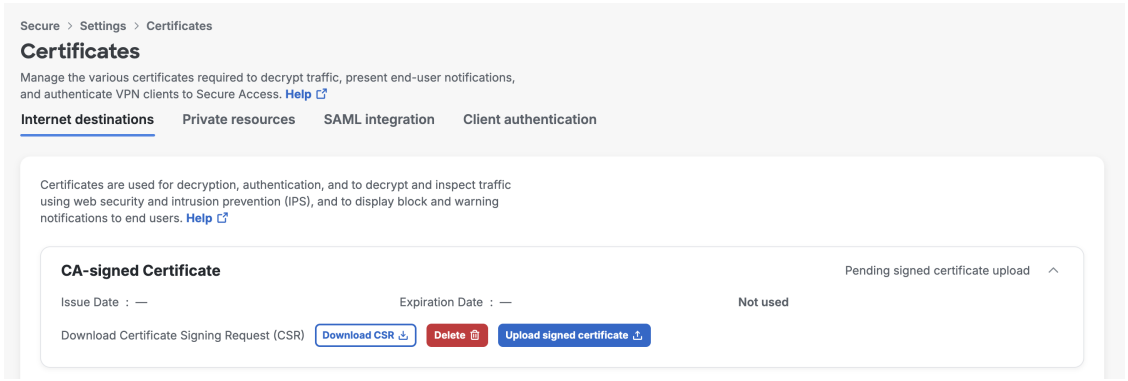
   Use a tool such as Microsoft Certificate Services or OpenSSL to sign the CSR with your corporate certificate signing authority (CA).

> **Note**
>
> You must download the Secure Access CSR file to complete the step.



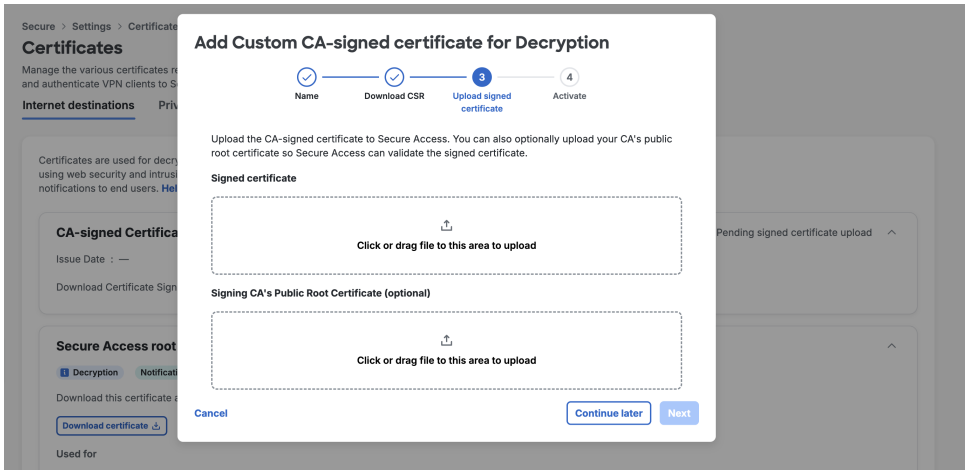
4. Sign the downloaded CSR file with your corporate certificate authority (CA).
5. Once you have signed the downloaded .csr file, click **Upload signed certificate**.

   Certificate status is `Pending signed certificate upload` until you upload your own CA signed root certificate.

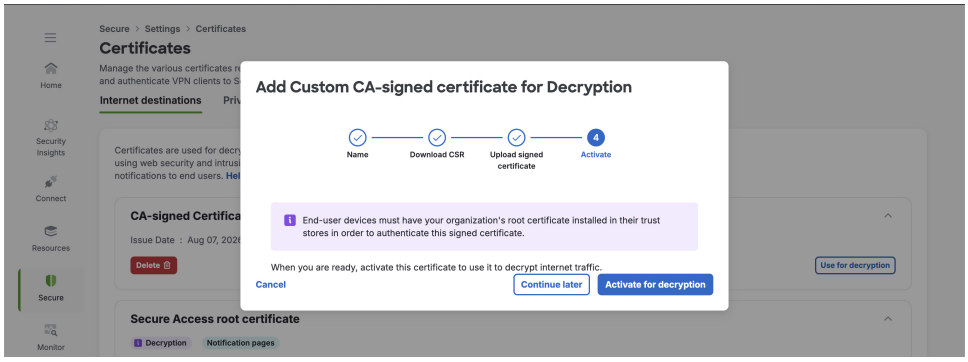


6. Browse to the certificate that you have generated with the Secure Access CSR or drag the signed certificate file onto Secure Access, and then click **Next**.

   You can optionally also upload your signing certificate authority's public root certificate to Secure Access. This allows Secure Access to validate the signed certificate that you uploaded.



7. Confirm that end-user devices have the root certificate required to validate server certificates that are signed by your organization's CA. Managed devices typically already have the required certificate.
8. For **Activate**, click **Use for decryption** to activate the CA signed certificate in Secure Access, and then click **Start using for decryption**.



Renew the Custom CA Signed Root Certificate

Provides instructions for completing the Renew the Custom CA Signed Root Certificate workflow in Cisco Secure Access. This document explains how to renew your custom CA signed root certificate before the certificate expires.

This document explains how to renew your custom CA signed root certificate before the certificate expires. Renewing the certificate is a streamlined process that does not interrupt your traffic flow; you can also stage a certificate to be deployed at a later time. Note that this option is only available if you already have a CA cert uploaded to Secure Access.

If your current certificate is nearing expiration or is already expired, the **Certificates** page displays a colored banner to alert you to the certificate status. Examine these banners to ensure that your certificate renewal occurs at a reasonable time without endangering your environment.

Alerts for certificate expiration dates are only displayed in the **Certificates** page.

Important

At this time, you can only renew certificates for Internet Destinations.

Procedure

1. Navigate to **Secure** > **Certificates**.

2. Select the **Internet Destinations** tab.
3. Click **Renew custom CA-signed certificate**.
4. In the **Renew Custom CA-signed certificate for Decryption** window, enter a unique **name** for the certificate; duplicate or repeat names for certificates is not supported. This is the name displayed in the **Certificates** page.
5. Click **Next**.
6. Click **Download CSR** and download the Certificate Signing Request (.csr) file to the local system, and then click **Next**. Use a tool such as Microsoft Certificate Services or OpenSSL to sign the CSR with your corporate certificate signing authority (CA).
7. Sign the downloaded CSR file with your corporate certificate authority (CA).
8. Browse to the certificate that you have generated with the Secure Access CSR or drag the signed certificate file onto Secure Access, and then click **Next**. You can optionally also upload your signing certificate authority's public root certificate to Secure Access. This allows Secure Access to validate the signed certificate that you uploaded.

   Note

   Confirm that end-user devices have the root certificate required to validate server certificates that are signed by your organization's CA. Managed devices typically already have the required certificate.

9. Click **Next**.
10. Click **Activate for decryption** if you want to immediately deploy the certificate. Secure Access automatically replaces the new certificate with the previous certificate without disrupting connectivity. This action also removes the previous certificate from the dashboard. Click **Continue later** if you want to deploy the certificate at a later time.

    Note

    If you opt to delay the deployment of your certificate by selecting **Continue later**, deploy at your desired date and time by navigating back to the **Certificates** page and click **Use for decryption**.

View the Cisco Trusted Root Store

Describes View the Cisco Trusted Root Store in Cisco Secure Access. A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website.

A root certificate is required when Secure Access proxies and decrypts HTTPS traffic intended for a website. Cisco provides trusted root store bundles, which contain information about certificates used by Cisco products. Within a bundle, you can view the list of trusted Cisco Certification Authorities (CA), type of root certificate, and certificate fingerprint (SHA-1).

The Secure Access trusted root certificate information is stored in the Cisco Trusted Union Root bundle. The Cisco Trusted Union Root bundle is a PKCS#7 bundle file (.p7b). The Cisco Trusted Union Root bundle is signed with a digital signing certificate, which you use to verify the bundle.

Prerequisites

- You must have administrative privileges on the devices in the organization or network administrative permissions over the network.

- Use a version of OpenSSL v1.0 or greater to extract the root bundle.

Download the Cisco Trusted Union Root Bundle

1. Navigate to the Cisco Cryptographic Services site at Cisco PKI: Policies, Certificates, and Documents.
2. Under **Trusted Root Stores**, download the Cisco Trusted Union Root Bundle: https://www.cisco.com/security/pki/trs/ios_union.p7b.

Extract the Certificates

Describes Extract the Certificates in Cisco Secure Access. Extract the signing certificate from the Trusted Union Root bundle (ios_union.p7b) and save the signing certificate in a file named RootBundleSigningCertificate.cer.

Step 1: Extract the Signing Certificate

Extract the signing certificate from the Trusted Union Root bundle (**ios_union.p7b**) and save the signing certificate in a file named **RootBundleSigningCertificate.cer**.

```
openssl pkcs7 -in ios_union.p7b -inform DER -print_certs >
RootBundleSigningCertificate.cer
```

Step 2: Extract Certificate Bundle as Message

Use the extracted signing certificate (**RootBundleSigningCertificate.cer**) to verify the Trusted Union Root bundle (**ios_union.p7b**).

```
# This command extracts the certificate bundle as a message into the
#   file iosBundleBodyVerified.p7b if the signature verifies
openssl cms -verify -nointern -noverify -inform DER -in ios_union.p7b -outform
 DER \
  -out iosBundleBodyVerified.p7b -certfile RootBundleSigningCertificate.cer
```

The output is similar to:

```
Verification successful
```

Step 3: Extract PEM-Formatted Certificates From Bundle

```
# This command extracts the certificates from the bundle into a separate
#   file, iosCerts.PEM, containing only the PEM-formatted certificates from
the bundle.
openssl pkcs7 -inform DER -print_certs -outform PEM < iosBundleBodyVerified.p7b
 \
  |grep -v 'subject=' |grep -v 'issuer=' |sed '/^$/d' > iosCerts.PEM
```

Step 4: Generate Individual Certificate Files

Linux

```
# If you are on Linux, use this command to split the PEM bundle into individual
 certificate files
# (Does not work on a Mac due to GNU awk)
awk 'BEGIN {c=0;} /BEGIN CERT/{c++} {print > c ".pem"}' < ../iosCerts.PEM
```

macOS

```
# If you are on a Mac, use this command to split the PEM bundle into individual
 certificate files
# (Does not work on Linux due to split not supporting the -p flag)
split -p "-----BEGIN CERTIFICATE-----" iosCerts.PEM individual-
```

View an Individual Certificate File

Describes View an Individual Certificate File in Cisco Secure Access. Use openssl x509 to view the contents of an individual certificate file as plain text.

Use `openssl x509` to view the contents of an individual certificate file as plain text. Provide the name of the individual file as an argument to the `openssl` command.

```
openssl x509 -in <individual-file> -text
```

Certificates for SAML Authentication

Describes Certificates for SAML Authentication in Cisco Secure Access. Cisco Secure Access integrates with various Security Assertion Markup Language (SAML) identity providers (IdPs) that authenticate users.

Cisco Secure Access integrates with various Security Assertion Markup Language (SAML) identity providers (IdPs) that authenticate users. When a user requests a resource, Secure Access verifies the identity of the user through a trusted exchange with the integrated IdP and authorizes the user to get the resource. Users on devices must authenticate with Secure Access before connecting to private or web resources. The Secure Access services–Zero Trust (ZT), secure web gateway (SWG), and virtual private networks (VPNs)–must trust the connections from users and devices.

To set up a trust relationship between Secure Access (service provider) and an SAML IdP, an administrator imports the SAML IdP XML Metadata in to Secure Access, and then uploads the Secure Access XML Metadata to the SAML IdP's platform. The administrator adds the service provider's certificates to the IdP platform's trust store.

After you integrate an SAML IdP with Secure Access, you can manage the certificates in Secure Access for both the service provider (Secure Access) and your organization's IdPs. Secure Access lists a certificate's subject name, serial number, and expiration date and displays notifications about certificates that may expire.

- Manage SAML Certificates for Service Providers
- Manage SAML Certificates for Identity Providers

Manage SAML Certificates for Service Providers

Describes Manage SAML Certificates for Service Providers in Cisco Secure Access. To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP.

To establish a trust relationship between Cisco Secure Access (service provider) and an integrated SAML identity provider (IdP), certificates are exchanged between Secure Access and the SAML IdP. An administrator uploads the service provider's certificates from the Secure Access XML Metadata to the IdP platform's trust store. Then, an administrator imports the SAML IdP's XML Metadata that contains the IdP's certificates in to Secure Access.

After you integrate an SAML identity provider (IdP) in Secure Access, you can manage the service provider's certificates. Secure Access displays notifications about certificates that may expire. When the service provider certificates expire, an administrator must upload new certificates from the Secure Access XML Metadata to the integrated SAML IdP platform's trust store to prevent connection disruptions.

Secure Access manages the expiration of service provider certificates for various connection methods and SAML IdP integrations. Service provider certificates are used to establish the trust relationship between the service provider and the IdP. The IdP authenticates users that connect to Secure Access with:

- Zero Trust (ZT)
- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile
- SSO Authentication for Secure Web Gateway and Zero Trust Access

Prerequisites

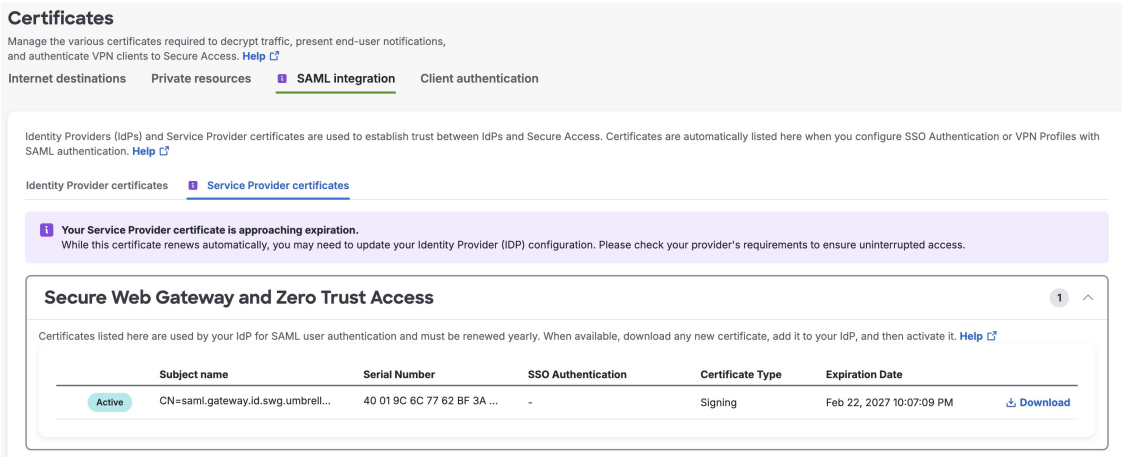
- Full Admin user role. For more information, see Manage Accounts.
- Configure Identity Providers.
- An integration of an SAML IdP with Secure Access. For more information, see Configure Integrations with SAML Identity Providers.

View Notifications About Expired Service Provider Certificates

Provides instructions for completing the View Notifications About Expired Service Provider Certificates workflow in Cisco Secure Access. Navigate to Secure Certificates SAML Authentication Service Provider Certificates Secure Web Gateway and Zero Trust Access .

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Authentication** > **Service Provider Certificates** > **Secure Web Gateway and Zero Trust Access**.
2. Secure Access displays any notifications about certificates that may expire.



See SAML Certificate Renewal Options for more information on how to renew.

Download Web Security and Zero Trust Service Provider Certificates

Provides instructions for completing the Download Web Security and Zero Trust Service Provider Certificates workflow in Cisco Secure Access. SSO Authentication: The service provider certificate is used by multiple IdP's for SAML user authentication, and the certificate must be renewed yearly.

SSO Authentication: The service provider certificate is used by multiple IdP's for SAML user authentication, and the certificate must be renewed yearly.

To set up the trust between Secure Access and the user devices in the organization that login via SSO, install a certificate on all devices and upload your organization's certificate to Secure Access. The certificate enables Secure Access to authenticate users and devices that connect via SSO.

Secure Web Gateway and Zero Trust Access table displays:

- **Subject name**– The certificate's common name, which defines the entity that manages the certificate.
- **Serial number**–The certificate serial number.
- **SSO Authentication**–This shows multiple IdPs that are configured.
- **Certificate Type**–shows if this is a signing certificate or encryption certificate.
- **Expiration date**–The date when the certificate is no longer valid.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML integration** > **Service Provider Certificates** > **Secure Web Gateway and Zero Trust Access**.
2. Click **Activate** next to the new certificate to launch the activation modal.
3. Next, click **Download Signing Certificate** to download the service provider certificate.
4. Navigate to your IdP and update with the new certificate.
5. Select the SSO authorization profile in the SSO Authentication list.
6. Click Activate to confirm your choice.

   A notification appears once the certificate is activated.
7. Verify that the new certificate is active in the Secure Web Gateway and Zero Trust Access list.

Download Virtual Private Network Service Provider Certificates

Provides instructions for completing the Download Virtual Private Network Service Provider Certificates workflow in Cisco Secure Access. Navigate to Secure Certificates SAML Authentication Service Provider Certificates .

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Authentication** > **Service Provider Certificates**.



2. For **VPN Service Provider**, click **download** on a certificate in the list to save the certificate to your local system. Then, upload the certificate to the SAML IdP.
   - **Subject name**–The certificate's common name, which defines the entity that manages the certificate.
   - **Serial number**–The serial number of the certificate.
   - **Expiration date**–The date when the certificate is no longer valid.

Manage SAML VPN Service Provider Certificate Rotation

Describes Manage SAML VPN Service Provider Certificate Rotation in Cisco Secure Access. Secure Access manages the expiration of service provider certificates for various connection methods and SAML IdP integrations.

Secure Access manages the expiration of service provider certificates for various connection methods and SAML IdP integrations. Service provider certificates are used to establish the trust relationship between the service provider and the IdP. The IdP authenticates users that connect to Secure Access with Virtual Private Networks (VPNs) with a configured VPN profile.

When Secure Access retires a service provider certificate, you need to rotate the service provider certificate used by your identity provider (IdP) to ensure admins and end users maintain successful access to applications.

> **Note**
>
> You must download the new Service Provider certificate, update your IdP with this new certificate, and activate the certificate within 24 hours before the current certificate expires. Failure to do this will result in SAML user authentication and connection failures.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- An integration of an SAML IdP with Secure Access. For more information, see Configure Integrations with SAML Identity Providers and Manage Virtual Private Networks.

Procedure

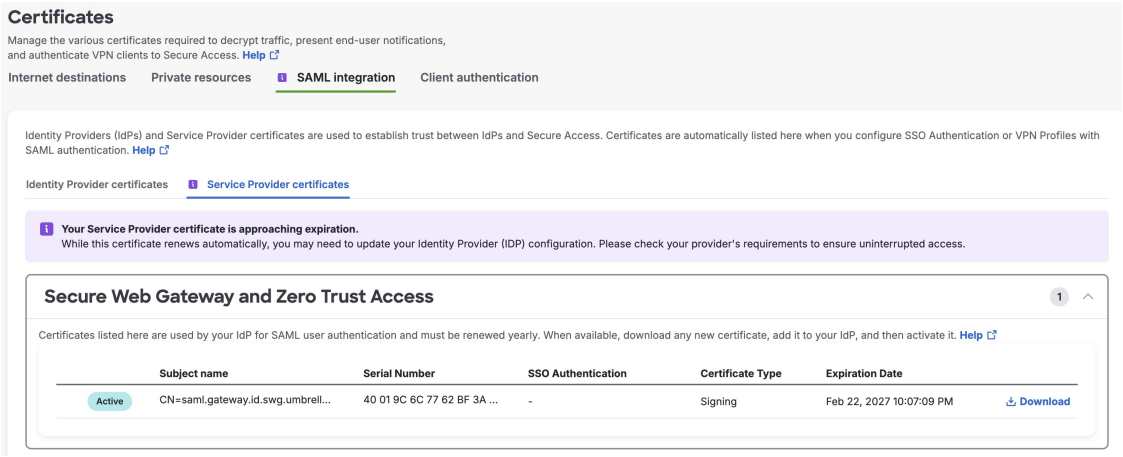
- View notifications about the expiration of Secure Access certificates that are deployed in SAML IdP integrations and VPN Profiles.
- Identify those service provider certificates with pending expiration dates.

View Notifications About Expired Service Provider Certificates

Provides instructions for completing the View Notifications About Expired Service Provider Certificates workflow in Cisco Secure Access. Navigate to Secure Certificates SAML Authentication Service Provider Certificates .

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML Authentication** > **Service Provider Certificates**.



2. Secure Access displays any notifications about certificates that may expire. The certificate dashboard displays an alert icon next to certificates with a pending expiration date.

Activate a New VPN Service Provider Certificate

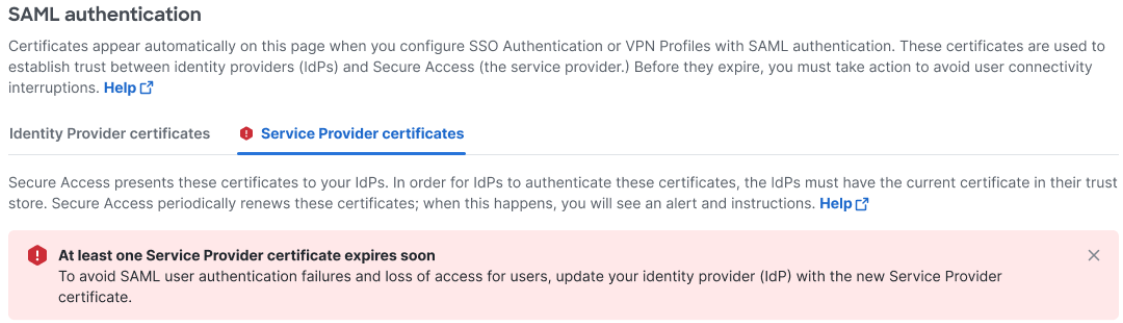
Provides instructions for completing the Activate a New VPN Service Provider Certificate workflow in Cisco Secure Access. You must update your Identity Provider (IdP) with the new Service Provider certificate before making this certificate active.

You must update your Identity Provider (IdP) with the new Service Provider certificate before making this certificate active. You cannot roll back to the old certificate.

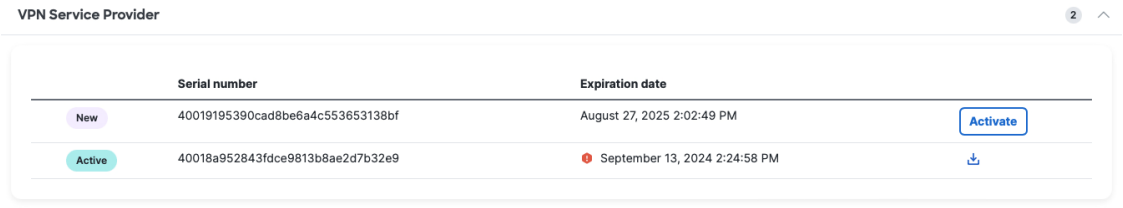
Procedure

---

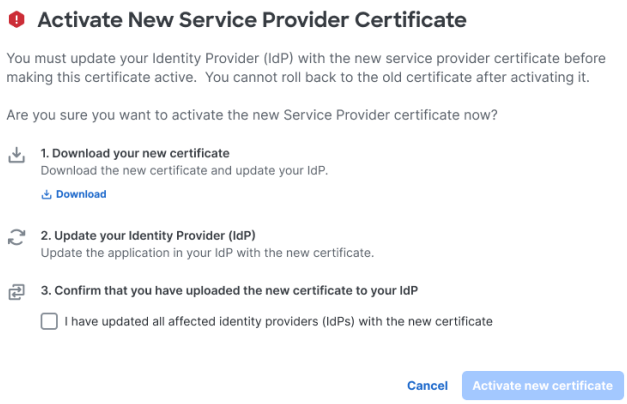
1. Navigate to **Secure** > **Certificates** > **SAML Authentication** > **Service Provider Certificates**.



2. For the **VPN Service Provider** certificate, click **Activate** on the new certificate to launch the activation modal.



3. To activate a new VPN Service Provider certificate:



a. Click the **Download** link to download the new VPN Service provider certificate.

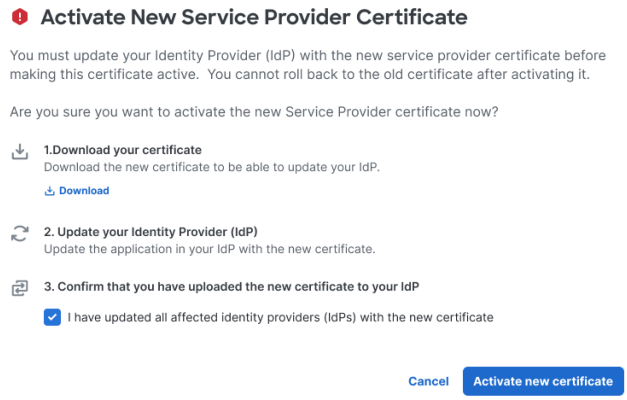
b. Update your IdP with this new certificate; see <xref href="../configure-integrations-with-saml-identity-providers/saml_certificate_renewal_options.xml" format="dita" scope="local">SAML Certificate Renewal Options</xref> for more information.

c. Check the box that confirms you uploaded the new certificate to your IdP.

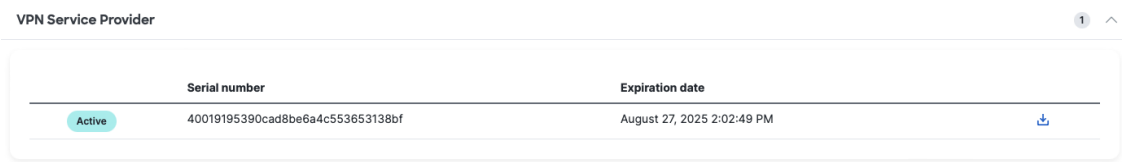
d. Click **Activate new certificate** to confirm your choice.

Important

You must update your IdP before activating the certificate. Failure to do this will result in SAML user authentication and connection failures.



4. Verify that the new certificate is **Active** in the **VPN Service Provider** certificates list.



Manage SAML Certificates for Identity Providers

View and manage the SAML certificates that your identity providers use to authenticate with Cisco Secure Access.

To establish a trust relationship between Cisco Secure Access (the service provider) and a SAML identity provider (IdP), you must exchange certificates between the two platforms. Import the Secure Access service provider certificates from the Secure Access XML metadata into the IdP trust store. Then, import the IdP XML metadata, which contains the IdP certificates, into Secure Access.

After you integrate an SAML identity provider (IdP) in Secure Access, you can manage the identity provider's certificates. Secure Access displays notifications about certificates that will expire. When the IdP certificates expire, an administrator must import new IdP certificates (XML Metadata) in Secure Access to prevent connection disruptions.

Secure Access manages the expiration of IdP certificates for various connection methods and SAML IdP integrations. IdP certificates are used to establish the trust relationship between the service provider and the IdP. The IdP authenticates users that connect to Secure Access with:

- Zero Trust (ZT)
- Networks and network tunnels protected by Internet Security
- Virtual Private Networks (VPNs) with a configured VPN profile
- SSO Authentication for Secure Web Gateway and Zero Trust Access

Before you begin

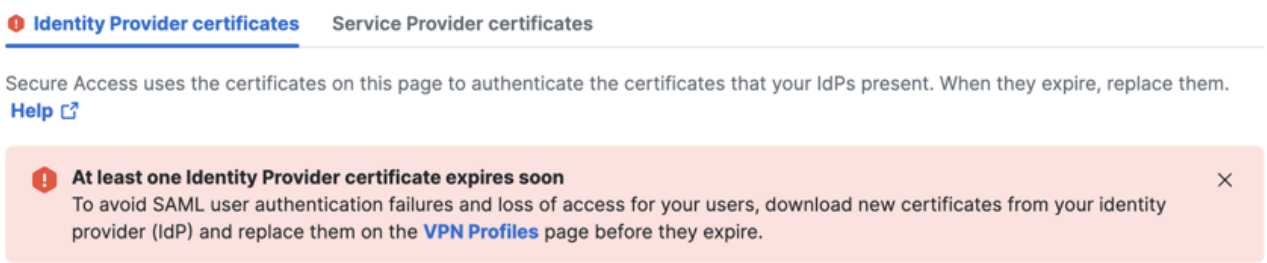
- Ensure that your account has the **Full Admin role** in Secure Access. For more information, see Manage Accounts.
- Ensure that Secure Access is integrated with a **SAML identity provider (IdP)**. For more information, see Configure Integrations with SAML Identity Providers. If you use VPN authentication, see Manage Virtual Private Networks.
- Ensure that IdP certificates use **RSA 2048-bit (or larger) keys** and **SHA-256 (or stronger) signature algorithms**. Secure Access does not support 1024-bit RSA keys or SHA-1 signatures.

Procedure

1. Navigate to **Secure** > **Certificates** > **SAML integration** > **Identity Provider certificates** > **Secure Web Gateway and Zero Trust Access**.

   Note

   If any certificates are approaching expiration, Secure Access displays a warning banner at the top of the page.

2. Review the certificates.

   Secure Access uses these certificates to authenticate the certificates that your IdPs present.

Table 26: Identity Provider certificate fields

Field name	Description
Serial number	The unique serial number of the certificate. The link opens a drawer to view additional certificate information.
Issuer	The Certificate Authority (CA) that issued the certificate. Includes the common name (CN), organization unit (OU), and country of origin (C).
SSO Authentication	The link brings you to the Configuration Management page for Users, Groups, and Endpoint Devices. You can upload the XML configuration file there. For more information, see Manage Users, Groups, and Endpoint Devices.
IdP	The name of the identity providers (IdPs) you are using.
Expiration date	The date when the certificate is no longer valid.

VPN Certificates for User and Device Authentication

Describes VPN Certificates for User and Device Authentication in Cisco Secure Access. Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access.

Users that connect over virtual private networks (VPNs) to private resources are protected by Cisco Secure Access. The user devices must trust their network communications with Secure Access.

To set up the trust between Secure Access and the user devices in the organization that connect over a VPN, install a certificate signed by your organization's Certificate Authority (CA) on all devices and upload your organization's signed CA root certificate to Secure Access. CA root certificates enable Secure Access to authenticate users and devices that connect over VPNs.

Once you upload signed CA certificates for VPN connections to Secure Access, you can view the details about the certificates, revoke a certificate, and delete a certificate. For more information about VPN Certificate Authority certificates, see Manage CA Certificates for VPN Connections.

Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment

Describes Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment in Cisco Secure Access. Secure Access authenticates users and devices using the organization's Certificate Authority (CA) certificate.

Secure Access authenticates users and devices using the organization's Certificate Authority (CA) certificate.

Certificates described in this section are used for the following purposes:

- When devices connect to networks using virtual private networks (VPNs).
- To enroll in Zero Trust Access (ZTA) using certificates or to renew ZTA enrollment. For more information, see Enroll Devices in Zero Trust Access Using Certificates.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Install an Identity Certificate on User Devices

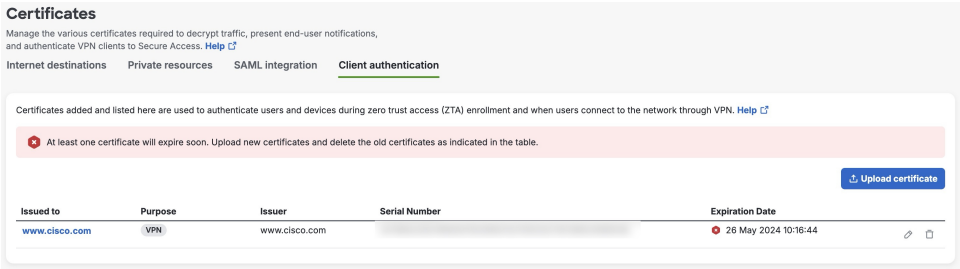
Install on the user devices in your organization an identity certificate signed by your corporate Certificate Authority (CA) and validated by the certificate you will upload.

View Notifications About Expired CA Certificates for Client Authentication

Provides instructions for completing the View Notifications About Expired CA Certificates for Client Authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Secure Access displays a banner if a certificate has expired or will expire within 90 days:

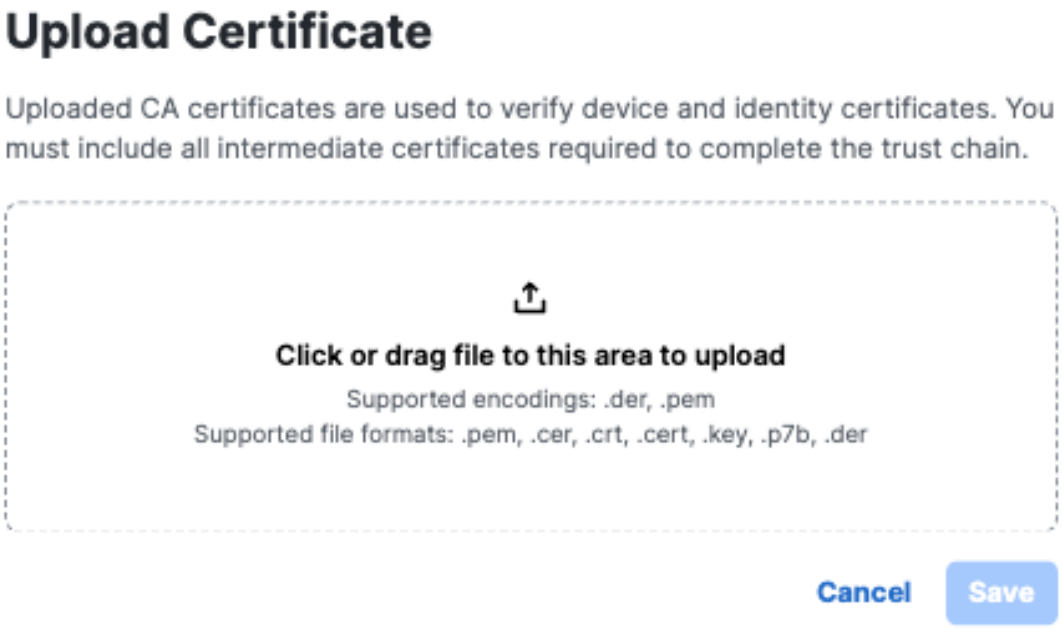


Upload Certificate Authority (CA) Certificates for client authentication

Provides instructions for completing the Upload Certificate Authority (CA) Certificates for client authentication workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Click **Upload certificate**.



3. Upload your signed CA root certificate.
4. Select **VPN Authentication** or **ZTA enrollment** or **Endpoint DLP Enrollment** both purposes for the certificate.

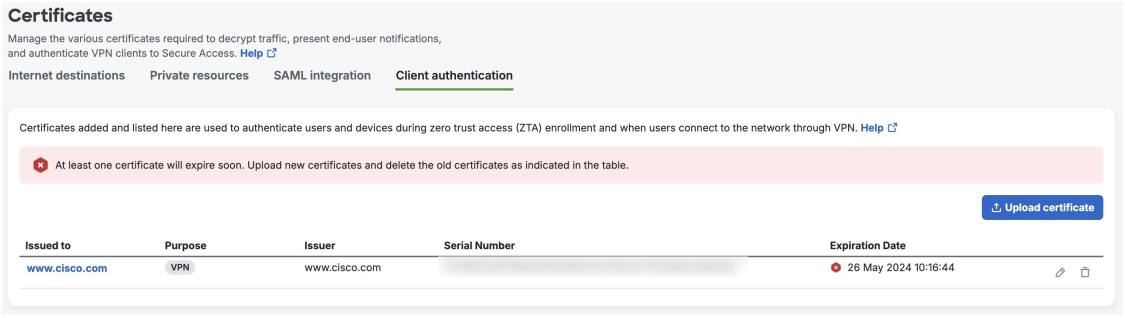
   Certificates must have at least one purpose selected.
5. (Optional) Configure certificate revocation settings. For details, see Manage Certificate Revocation Settings.
6. Click **Save**.
7. If you enabled **ZTA enrollment**, download and distribute the configuration file that is generated after you click Save. See Enroll Devices in Zero Trust Access Using Certificates.
8. If you enabled **Endpoint DLP Enrollment**, download and distribute the choice file that is generated after you click Save. See Enroll Devices in Endpoint DLP Using Certificates.

View Uploaded CA Certificates

Provides instructions for completing the View Uploaded CA Certificates workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

Navigate to **Secure** > **Certificates** > **Client authentication**. Secure Access lists the certificates uploaded by your organization.



What to do next

Issued to–The name issued to the CA certificate.

Purpose –Whether the certificate is used for VPN authentication or Zero Trust Access enrollment or Endpoint DLP enrollment or multiple purposes.

Issuer–The CA that issued the certificate.

Serial Number–The serial number of the certificate.

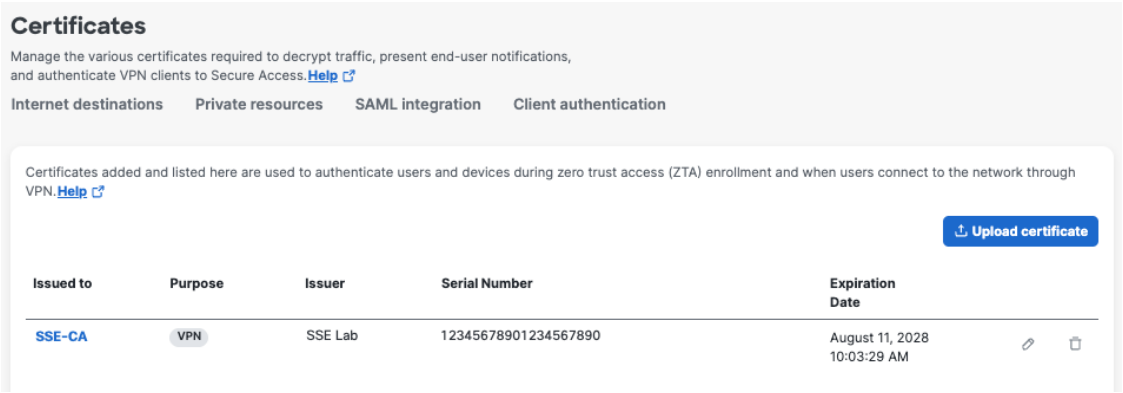
Expiration Date–The date when the certificate is no longer valid.

Manage Certificate Revocation Settings

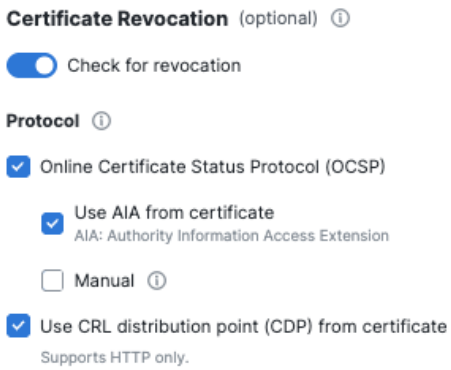
Provides instructions for completing the Manage Certificate Revocation Settings workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Click a CA certificate **Issued to** link to open the certificate details.



3. For **Revocation settings**, enable **Check for revocatione**.
4. For **Protocol**, check **Online Certificate Status Protocol** both **Use AIA from certificate** and **Manual**.
5. For **Protocol**, check **Use CRL distribution point (CDP) from certificate**.



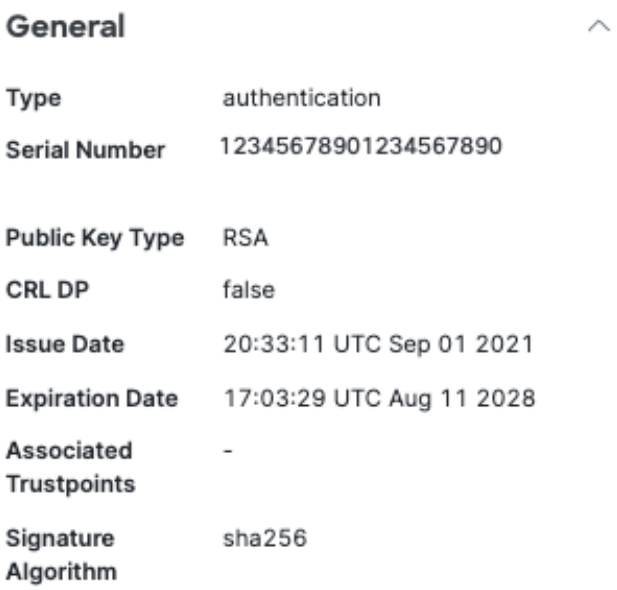
6. Click **Save**.

View CA Certificate Details

Provides instructions for completing the View CA Certificate Details workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

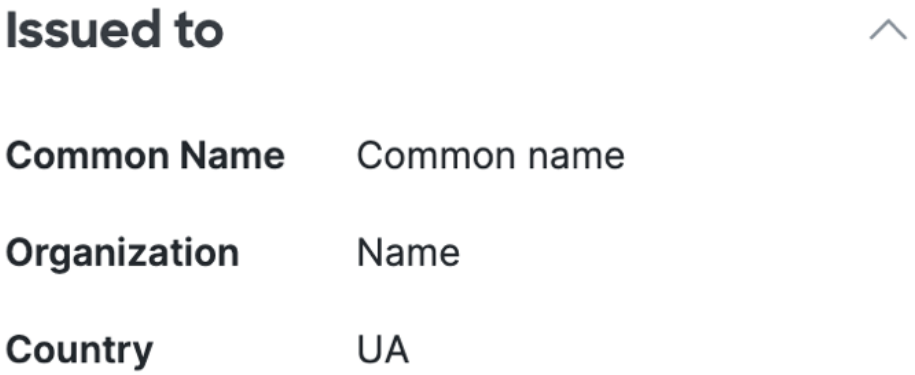
1. Click a certificate name to view details.
2. **General** certificate details:
   - **Type**–The type of the certificate.
   - **Serial Number**–The serial number of the certificate
   - **Purpose** –Whether the certificate is used for VPN authentication or Zero Trust Access enrollment or Endpoint DLP enrollment or multiple purposes.
   - **Public Key Type**–The type of the public key.
   - **CRL DP**–Certificate Revocation List (CRL) Distribution Point. The location where you can check the revocation of the certificate.
   - **Issue Date**–The date from which the certificate is valid.
   - **Expiration Date**–The date when the certificate is not valid.
   - **Associated Trustpoints**
   - **Signature Algorithm**–The cryptographic hash algorithm (Secure Hashing Algorithm 256).



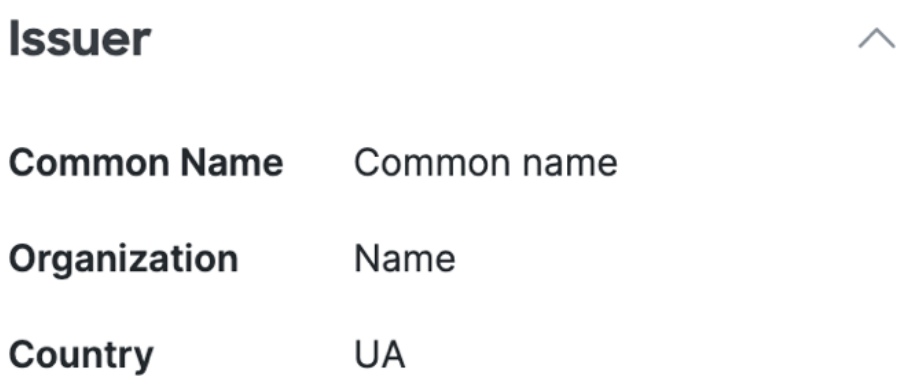
3. **Issued to** certificate details.

   The entity that uses the certificate to build a trust relationship with Secure Access.

   - **Common Name**–The fully-qualified domain name that is secured by the certificate.
   - **Organization**–The organization that is issued the certificate.
   - **Country**–The country where the certificate was issued specified in the two-character country code.



4. **Issuer** certificate details. The issuer is the entity (trusted authority) that issues the certificate.
   - **Common Name**–The fully-qualified domain name that is secured by the certificate.
   - **Organization**–The organization that issued the certificate.
   - **Country**–The country where the certificate was issued specified in the two-character country code.



Change the Purpose of an Uploaded CA Certificate

Provides instructions for completing the Change the Purpose of an Uploaded CA Certificate workflow in Cisco Secure Access. Certificates must have at least one purpose selected.

Certificates must have at least one purpose selected.

Deselecting a purpose is the equivalent of deleting a certificate that is used for that purpose. For the effects of doing so, see Delete a CA Certificate, below.

If you enable "ZTA enrollment" or "Endpoint DLP Enrollment", a corresponding new configuration file is generated after you click Save. You must download and distribute this file to user devices that will depend on this certificate for Zero Trust Access or Endpoint DLP certificate-based enrollment.

If your organization has a Cisco-provided CA certificate intended to authenticate VPN connections: This certificate cannot be used for Zero Trust Access enrollment and the option is not available for that certificate.

To change the purpose of a CA certificate:

Procedure

1. Navigate to **Secure** > **Certificates** > **Client authentication**.
2. Click the pencil icon to modify the certificate.
3. Click **Save**.
4. If you enabled ZTA enrollment or Endpoint DLP enrollment, download and distribute the corresponding newly generated configuration file to user devices.

Delete a Client Authentication CA Certificate

Provides instructions for completing the Delete a Client Authentication CA Certificate workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

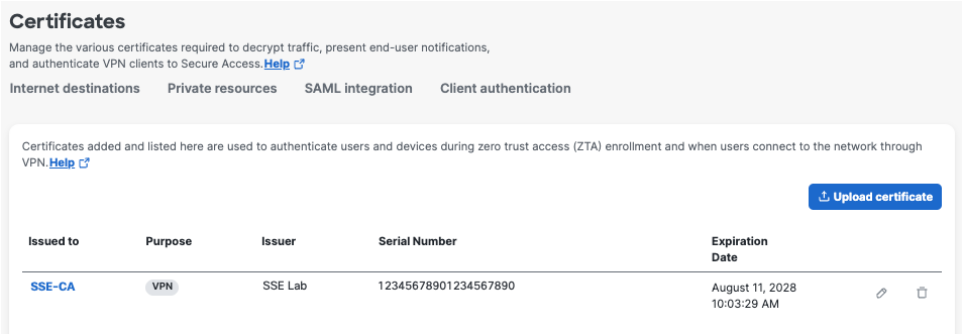
Deleting a CA certificate has different effects depending on the configured purpose of the certificate:

1. Deleting a CA certificate used for VPN authentication immediately prevents access.
2. Deleting a CA certificate used for Zero Trust Access enrollment prevents new enrollments and enrollment renewals authenticated by that certificate, but does not terminate existing connections or immediately prevent further access. See Unenroll a Device from Zero Trust Access.

To delete a CA certificate:

Procedure

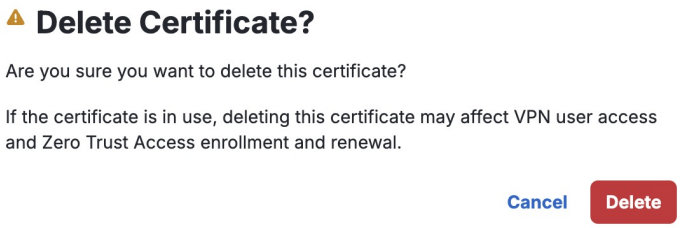
1. Navigate to **Secure** > **Certificates** > **Client authentication**.



2. To remove a certificate, follow the steps in one of the options:

   a. Click on a certificate **Issued to** link to open the certificate details, and then click **Delete**. Click **Delete** again to confirm the removal of the certificate.

   b. Click on the delete icon to **Delete**. Click **Delete** again to confirm the removal of the certificate.



What to do next

Expired Certificates

For certificates used for Zero Trust Access enrollment: If a CA certificate expires and you replace it, you must re-generate the configuration file and distribute it to all user devices that use Zero Trust Access.

56 Secure Access Investigate

Topics:

- Manage Secure Access Investigate
- About the Investigate Domain Summary
- About WHOIS Record Information
- About the ASN View

Provides an overview of Secure Access Investigate, including Manage Secure Access Investigate, About the Investigate Domain Summary, and About WHOIS Record Information. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Secure Access Investigate

Describes Manage Secure Access Investigate. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

Cisco Secure Access Investigate provides detection, scoring, and prediction of emerging threats. You can predict the likelihood that a domain, an IP address, or entire ASN may contribute to the origin of an attack or pose a security threat before an attack or threat occurs. Secure Access Investigate is based on domain information gathered by the Secure Access Global Network.

In the past, internet security has been largely predicated on researchers obtaining a sample of an attack, a binary file, or an exploit and then publishing the static detection after the attack. For the most part, methods are still reactive: infections occur and then detection happens. Secure Access Investigate leverages an extraordinary amount of data from the Secure Access security network and applies big data storage, data mining methods, machine learning, graph theory, vector analysis, anomaly detection, contextual search, and scoring to categorize and predict attacks before they occur.

Access Secure Access Investigate

You access Secure Access Investigate through the Secure Access dashboard.

Getting Started with Investigate

Describes Getting Started with Investigate in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Investigate provides search functionality through Smart Search and Pattern Search. Use Smart Search to search directly for a certain domain, IP, AS, file hash, or email address. An Investigate Pattern Search enables you to flexibly search for a domain using regular expression (RegEx) pattern search. An Investigate search generates multiple, graphical views of security scores and threat indicators.

To get started with Investigate, log into Secure Access with your Secure Access account credentials.

Smart Search

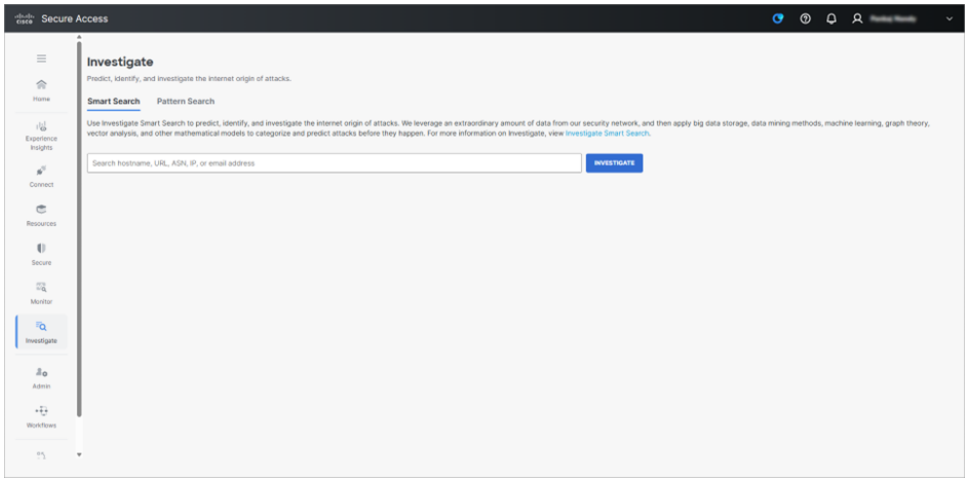
Provides instructions for completing the Smart Search workflow in Cisco Secure Access. Search the Investigate database for data related to a domain, email address, file checksum, IP address, or AS number.

Search the Investigate database for data related to a domain, email address, file checksum, IP address, or AS number.

To execute a smart search, perform the following steps:

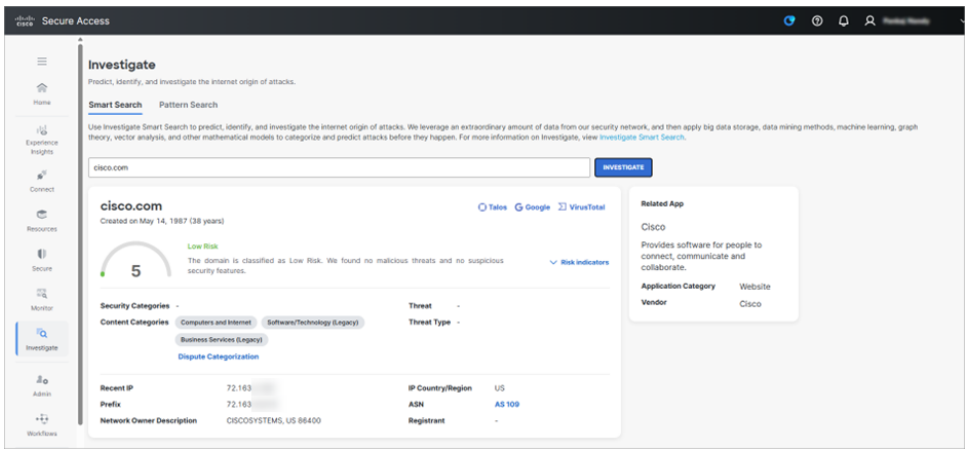
Procedure

1. Enter a domain name, an IP address, email address, or an Autonomous System Number (ASN) into the search bar.



2. Click **INVESTIGATE**.

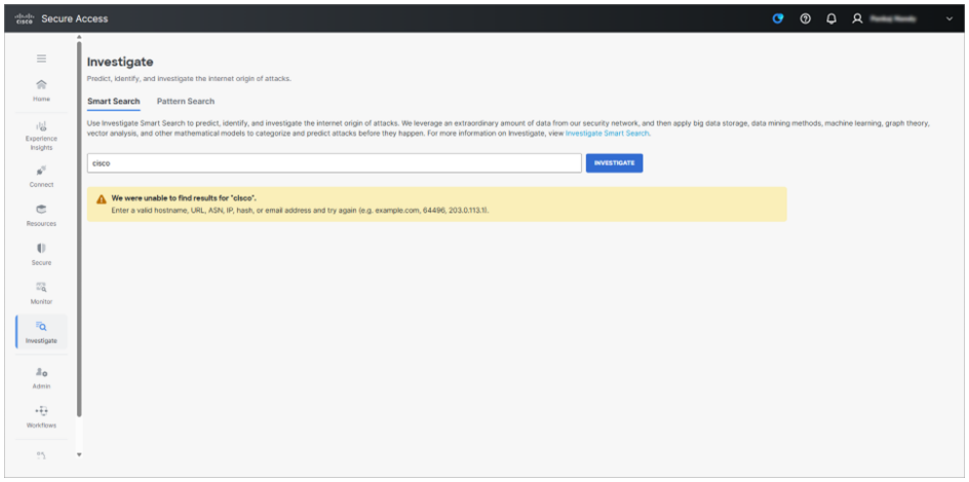
   Investigate returns a summary, risk score, security categories, content categories, and security indicators about the internet destination.



Smart Search Best Practices

Describes Smart Search Best Practices in Cisco Secure Access. To generate search results, enter a fully qualified domain name, URL, IP address, hash, or email address in the Smart Search search bar.

To generate search results, enter a fully qualified domain name, URL, IP address, hash, or email address in the Smart Search search bar. If you enter a malformed or incomplete destination, Secure Access Investigate raises an error and returns an example of the correct syntax to use in order to complete a successful search.



Pattern Search

Describes Pattern Search in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Investigate supports pattern search functionality for flexible and extensive searches of domains. We encourage you to use Pattern Search to discover co-occurrences between domains and related IP addresses.

Conduct a Pattern Search

Describes Conduct a Pattern Search in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Investigate supports standard regular expression pattern search functionality. You can search the Investigate database for a domain using a regular expression (RegEx).

The Investigate database contains information about domains that were looked up within a specific period. As such, when you query Investigate, you may find results that do not match a domain that resolves, but match domains in which Secure Access receive DNS lookups.

Investigate Pattern Search enables you to discover newly queried domains that may include your company's brand or intellectual property. You can use pattern search to find minor intentional misspellings – commonly used to confuse users in phishing emails – then identify campaigns targeted against your employees or customers. From those discoveries, pivot through the attacker's infrastructures to identify a related attacker infrastructure that shares that network space or other domains registered by the same email addresses.

About Pattern Search

Describes About Pattern Search in Cisco Secure Access. In the dashboard, an Investigate pattern search is limited to 500 results.

In the dashboard, an Investigate pattern search is limited to 500 results. The Secure Access Investigate API /search endpoint can return up to 1000 records. If the results of your query exceed these limits, we recommend that you refine the RegEx and perform multiple pattern searches. Alternatively, you can limit the period for the search.

The pattern search results only extend back thirty days. Only newly queried domains are discovered whether the domain was registered recently or not. The Investigate dashboard and the Investigate API pattern search include a date in which the domain was first seen – the first time Secure Access recorded a query for the domain. Domains seen before the query period are not found in the search result – including almost all common, well-known domains.

Pattern Search provides pre-configured time periods to constrain the search. The default and maximum time range to query Investigate is the last thirty days (Last 30 days). You can restrict the pattern search to include information about domains from the last seven days or the past 24 hours.

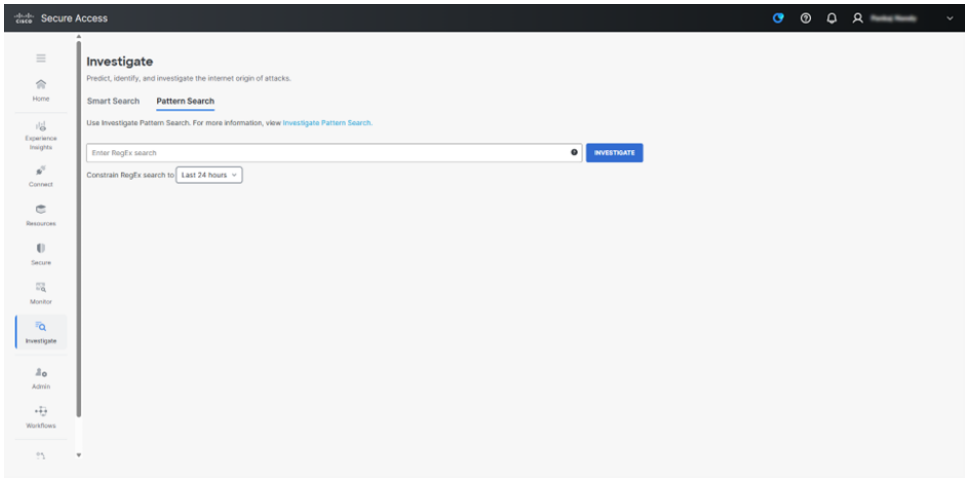
Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To execute a pattern search, perform the following steps:

Procedure

1. Navigate to **Investigate** > **Pattern Search** in Secure Access.
2. Choose a time range from the Constrain RegEx search to drop-down list.



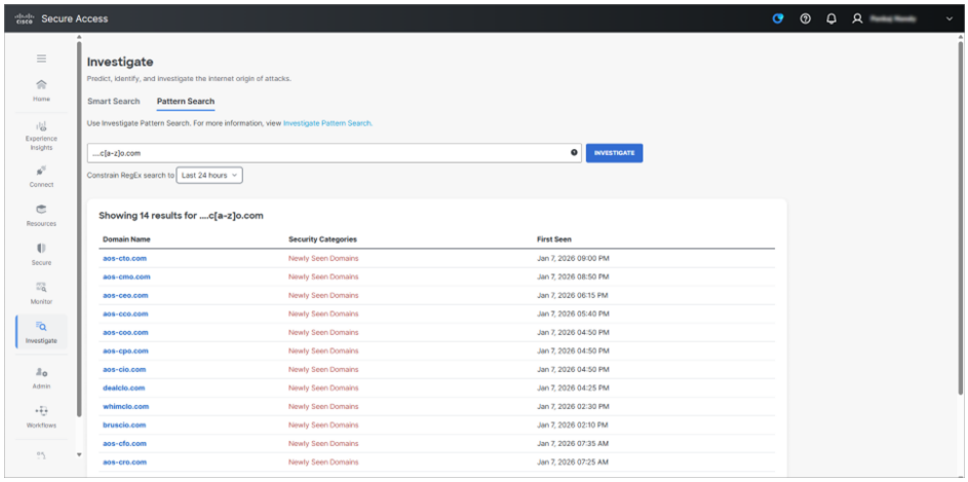
In the search bar, you can click the ? (help) icon to see a list of operators for a RegEx search.

Operators:

- ***** – An asterisk matches zero or more instances of the previous token.
- **.** – A period matches exactly one character.
- **[ ]** – Brackets match a class of characters. For example, use [0-9] to match single digits (0 to 9), or use [a-z] to match alphabetic characters (a to z).
- **( )** – Parentheses group tokens together for modifiers. For example, (ya)* matches ya, yaya, or yayaya.
- **?** – A question mark matches one or zero instances of the previous token. For example, hi(ya)? matches hi or hiya.

> **Note**
>
> The period (.) character has meaning as a wildcard and as a literal in hostnames. If you would like to use this character as part of your pattern, you must escape it using the backslash character (). For example, ..umbrella.com matches a.umbrella.com or b.umbrella.com.

3. Enter a RegEx expression into the search bar.
4. Click **INVESTIGATE**.

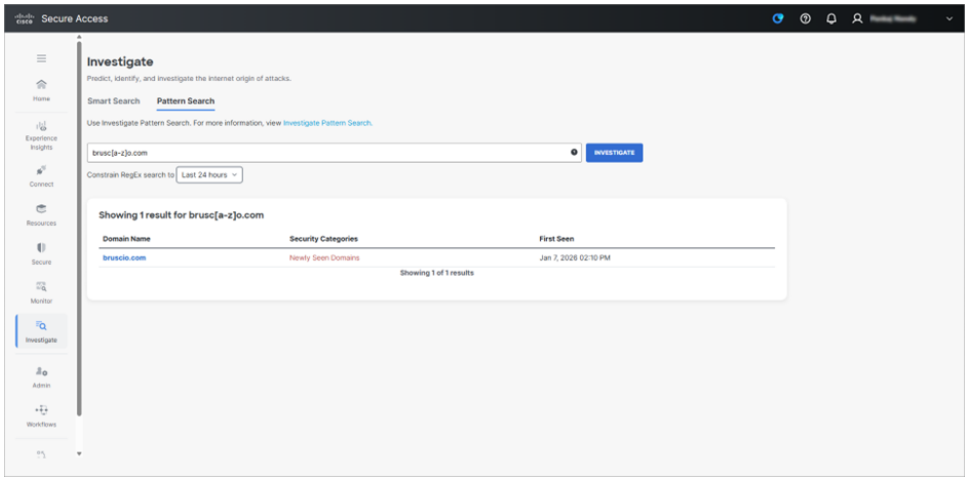


RegEx Examples

Describes RegEx Examples in Cisco Secure Access. To check for 'typosquatting' on a domain, enter a range of characters within a domain name.

To check for 'typosquatting' on a domain, enter a range of characters within a domain name. For example, ...yah[a-z]o.com, matches both the correct domain (www.yahoo.com) and the misspelled version, (www.yahro.com), and any other typos found in the fourth character of the string along with any other non-www prefixes.

To search for domains without specifying the www prefix, simplify the RegEx to brusc[a-z]o.com.



Pattern search returns the domain name and date when Secure Access recorded a DNS lookup against the hostname (First Seen).

> **Note**
>
> If the domains returned from your pattern search match any Secure Access security categories, Investigate lists the security categories with the domain.

About Passive DNS

Describes About Passive DNS in Cisco Secure Access. Secure Access Investigate monitors the DNS requests that are processed by the Secure Access DNS resolvers and records the Secure Access categorization changes in a passive DNS database.

Secure Access Investigate monitors the DNS requests that are processed by the Secure Access DNS resolvers and records the Secure Access categorization changes in a passive DNS database. Secure Access Investigate provides up to four years of DNS resolution history for you to work with.

Passive DNS represents a stored collection of historical DNS resolution data. Secure Access Investigate maintains a large repository of passive DNS history, providing a unique perspective of the internet. With passive DNS data, you can reference past DNS record values to uncover potential security incidents or discover malicious networks. For example, when a DNS record changes, the previous value is not saved. Without passive DNS, it is difficult to identify the prior DNS records for a malicious site.

Passive DNS helps you find patterns and use predictive analysis to uncover attacks. At a glance, you can discover useful information about a domain. For example, you can view the date that a domain's A record changed and uncover the changes to the A record. Unlike querying live records, searching for a passive DNS database does not alert bad actors to your investigation.

Secure Access Investigate stores security assessments and DNS query volumes so that you can view how security risks for domains change over time.

About Investigate View Types

Describes About Investigate View Types in Cisco Secure Access. Investigate displays graphical views of security scores and indicators to assist you in your research and analysis.

Investigate displays graphical views of security scores and indicators to assist you in your research and analysis. You can search Investigate using the following elements:

- **Domain or subdomain** – Specify a domain without the protocol or URL information. A domain may include subdomains. For instance, both www.example.com and example.com are valid and may return different results depending on the zone record configuration of the domain.
- **IP Address** – Specify a full IPv4 or IPv6 address, for example: `19.117.63.126` Only enter a single IP address. Investigate does not support searches for an IP range or a partial IP address.
- **ASN** – Specify the Autonomous System Number (ASN), for example: `36692`.
- **Email Address** – Specify an email address in the standard format, for example: name@domain.com. Secure Access Investigate does not support email addresses with wildcards. Use an email address to search for the domain registrant.

About the Investigate Domain Summary

Describes About the Investigate Domain Summary in Cisco Secure Access. The Investigate Domain Summary displays when you search for a domain name in the Smart Search or Pattern Search.

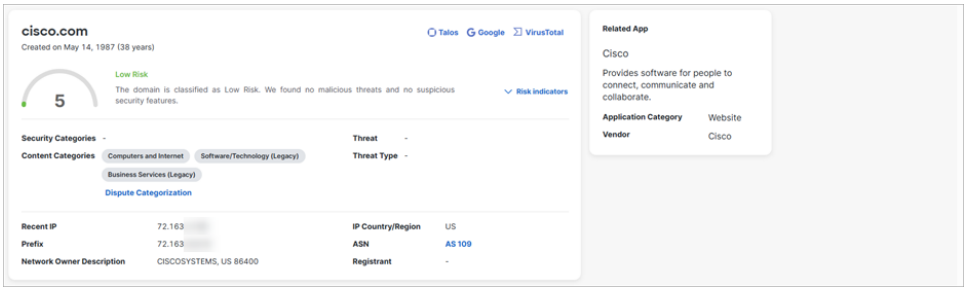
The Investigate Domain Summary displays when you search for a domain name in the Smart Search or Pattern Search. You can specify a fully qualified domain name (FQDN), for example: subdomain.subdomain.domain.com. Secure Access Investigate is protocol-agnostic.

> **Note**
>
> You must not include the protocol or any URL information in the search query.

Domain Summary Details

Describes Domain Summary Details in Cisco Secure Access. The Domain Summary lists the Investigate Domain Risk Score, sub-scores, security categorizations, content categorizations, and key domain notifications.

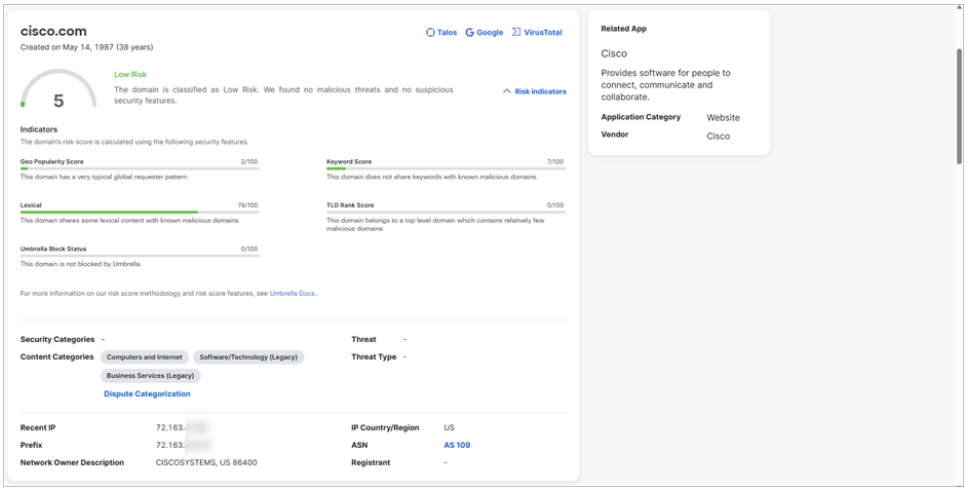
The Domain Summary lists the Investigate Domain Risk Score, sub-scores, security categorizations, content categorizations, and key domain notifications. When a domain is malicious, Investigate displays additional domain details associated with the security



Investigate Domain Risk Score

Describes Investigate Domain Risk Score in Cisco Secure Access. The Investigate Domain Risk Score is based on an analysis of the domain name, the DNS query behavior of the domain, and analyst reviews of the domain.

The Investigate Domain Risk Score is based on an analysis of the domain name, the DNS query behavior of the domain, and analyst reviews of the domain.



An Investigate Domain Risk Score falls into one of these ranges:

- High Risk – (90 to 100)
- Medium Risk – (40 to 90)
- Low Risk – (0 to 40)

An Investigate Domain Risk score emphasizes the lexical characteristics of domain names along with some key behavioral components. These risk scores are synthesized into one overall score—much like a credit score is made of account balances, lending history, debt ratios, and other components. The DNS behavioral components are:

- Lexical
  - Keyword Score
  - Lexical Score
- Behavioral
  - TLD Rank Score
  - Geo Popularity Score

Sub-Component Scores

The behavioral component scores are:

- Keyword Score
- Lexical Score
- TLD Score
- Geo Popularity

> **Note**
>
> The Secure Access Investigate overall risk score is created from many indicators.

Keyword Score

Describes Keyword Score in Cisco Secure Access. Many phishing attacks try to take advantage of the weakest link in the security chain: people.

Many phishing attacks try to take advantage of the weakest link in the security chain: people. If a domain name contains words related to legitimate companies and services, it is more likely to trick people into clicking. This style of social engineering continues to be a common technique for attackers.

Lexical Score

Describes Lexical Score in Cisco Secure Access. A mainstay of communication between infected machines and command and control servers are domains created using Domain Generation Algorithms (DGAs).

A mainstay of communication between infected machines and command and control servers are domains created using Domain Generation Algorithms (DGAs). A DGA circumvents any need to embed the location of control servers directly in the malware, and it enables attackers to regain control of their botnets even in the face of sink holing and takedowns. Using a generalization of the method behind the Cisco Secure Access DGA score, we can reliably predict when hostnames were generated without having to rely on developing models of what lexical patterns to look for.

TLD Score

Describes TLD Score in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Not all top-level domains (TLDs) are created equal. Over the years, the TLDs of choice for spammers have changed according to the following factors: cost, ease of batch registration, verification of registrant identity, and abuse complaint policies. Using our global reach, we can assess the risk indicated by the currently observed abuse levels, and combined with our other indicators, help security analysts make more informed decisions.

Geo Popularity

Describes Geo Popularity in Cisco Secure Access. Global complement of data centers of Secure Access gives us visibility into DNS requests made by clients around the world.

Global complement of data centers of Secure Access gives us visibility into DNS requests made by clients around the world. Is a domain getting requests from a country where it typically doesn't? Did the number of countries requesting a domain suddenly change? By analyzing requests to domains across all countries in the world, patterns emerge that allow us to detect anomalous behavior and identify increased risk.

About Investigate Passive DNS Timeline

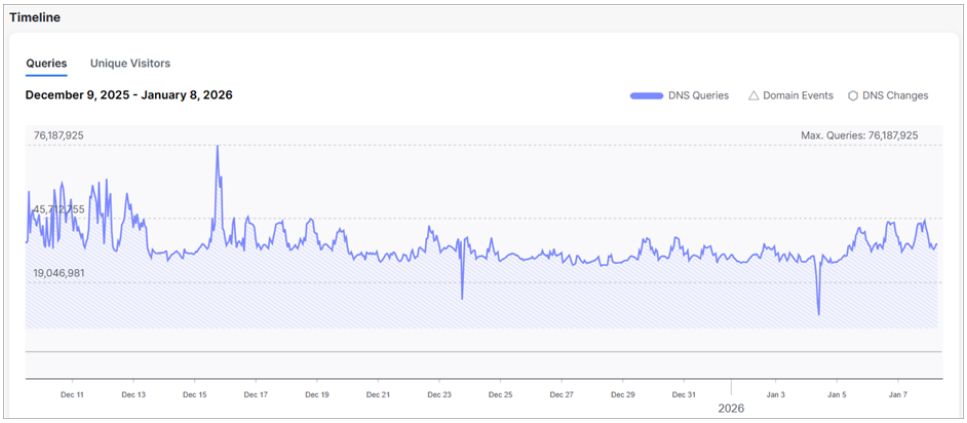
Describes About Investigate Passive DNS Timeline in Cisco Secure Access. The Passive DNS Timeline displays the DNS query volume, domain events, query history, and DNS changes.

The Passive DNS Timeline displays the DNS query volume, domain events, query history, and DNS changes. You can view the evolution of a domain over time, and view up to four years of DNS changes.

DNS Query Volume

The DNS Query Volume graph uses three icons:

- Blue Line – The volume of DNS queries over the last 30 days.
- Diamond – Domain events. The icon is colored red for malware, command and control, and phishing. It is colored yellow for other security events.
- Pentagon – DNS changes, such as A record changes. We store DNS changes for up to four years.



Event History

The Event History uses three lines, from top to bottom, to represent the following event types:

- DNS Changes–The top line uses dark grey to show DNS record events, such as A record changes.
- Security Categories–The middle line shows Secure Access security categorization events. Red represents malware, command and control, and phishing. Yellow represents other security events.
- Query History–The bottom line uses blue to show time periods with DNS query history available.



Click on the domain events or DNS changes icons to see details. A panel opens to show events, grouped by resource record type and date. If the view displays more than one event for the selected period, the icon shows the number of available events.

Event History uses the following icons:

Icon	Description
	Domain registration date.
	Date that the domain was first seen by our resolvers.
	Domain registration expiration date.

To view more details, hover the pointer over each icon.

Dispute Content Categorization

Describes Dispute Content Categorization in Cisco Secure Access. When a destination is classified in a category which you disagree with, you can dispute the categorization.

When a destination is classified in a category which you disagree with, you can dispute the categorization. Secure Access and Cisco Talos share a unified set of content categories. You can submit a category dispute request through Secure Access Investigate or Cisco Talos.

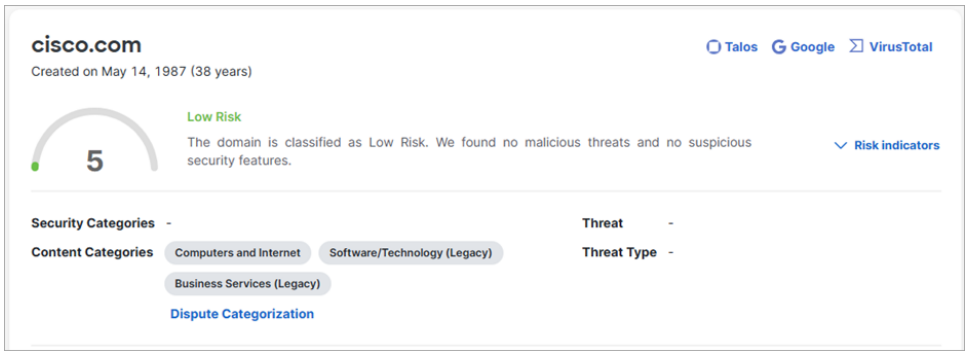
Submit categorization request through cisco Talos

You can submit a domain, an IP address, or a file hash to Cisco Talos, and request that Talos review the content category assigned to the destination. For more information, see Cisco Talos Reputation Center.

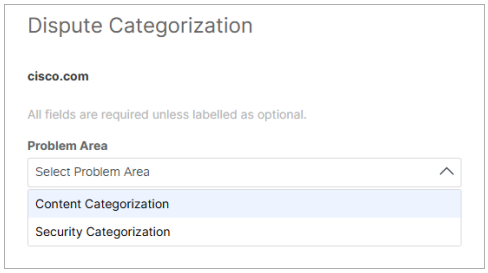
Submit categorization request through Investigate

To submit categorization request through Investigate, perform the following steps:

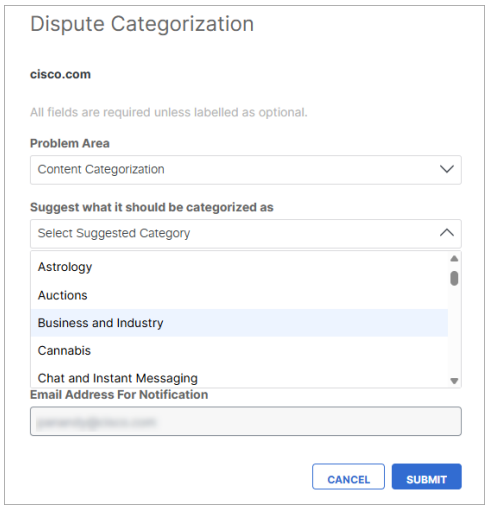
1. Log into Secure Access and enter a destination you want to query in the Pattern Search or Smart Search.
2. In the Domain Summary view, click **Dispute Categorization**.



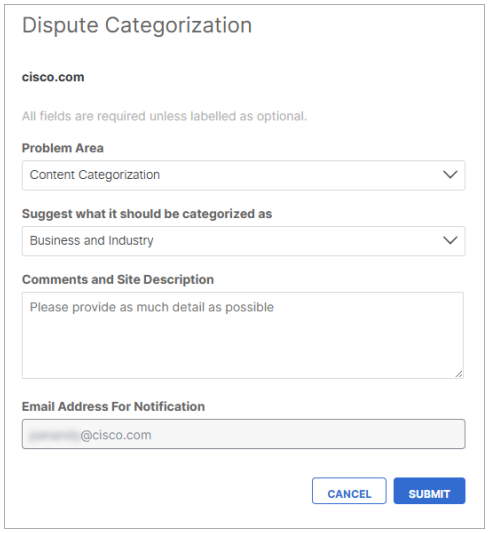
3. Under **Problem Area**, choose **Content Categorization**.



4. Choose a category to suggest a new categorization.



5. (Optional) Provide comments and a description of the destination for your suggestions.
6. Enter an email address for the notification. Investigate sends your suggestion directly to Talos for consideration. Talos replies to the email address that you provide with the resolution.



7. Click **SUBMIT**.

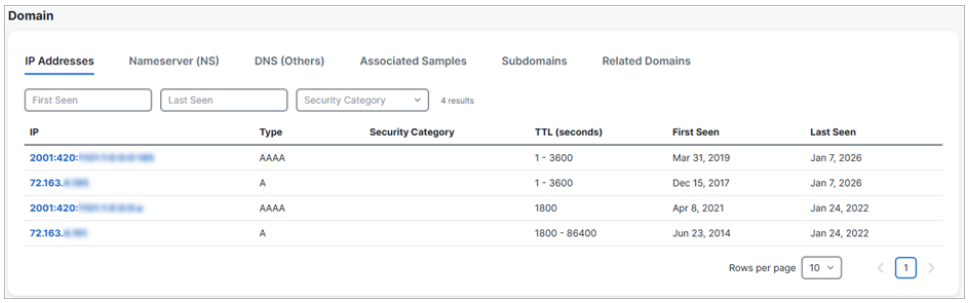
About DNS Resolution in Investigate

Describes About DNS Resolution in Investigate in Cisco Secure Access. The DNS Resolution includes IP addresses, Nameserver (NS), and other DNS record types, such as TXT records.

The DNS Resolution includes IP addresses, Nameserver (NS), and other DNS record types, such as TXT records. The DNS Resolution information represents the present and recent history of a domain's DNS settings. By default, the information is sorted from most recent to least recent.

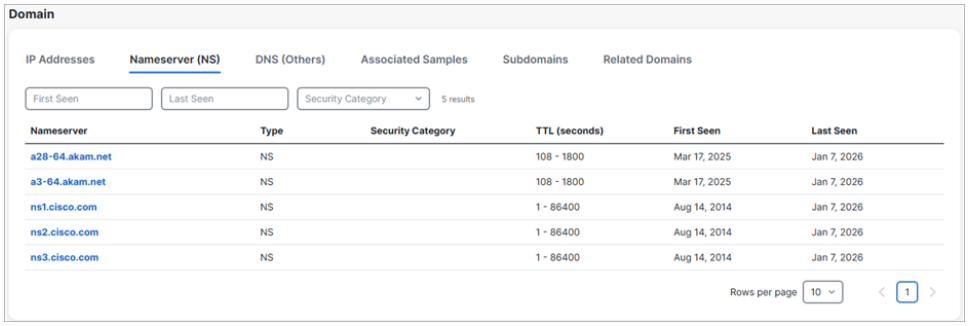
IP Addresses

The IP addresses tab contains information related to the domain. This information includes any security categories (if applicable), TTL(s) (shown as a range), first seen and last seen dates.



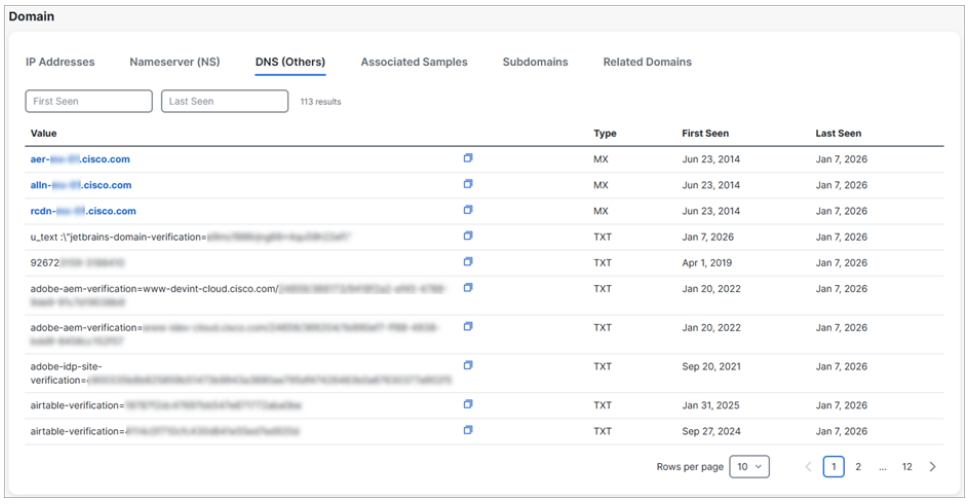
Nameserver (NS)

The Nameserver tab holds information about the nameserver related to the domain, including security categories, TTLs (shown as a range), and first seen and last seen dates.



DNS (Others)

The DNS (Others) tab holds other types of DNS records related to the domain – the value of the DNS record, type of the DNS record, and the first seen and last seen dates.



About Associated Samples in Investigate

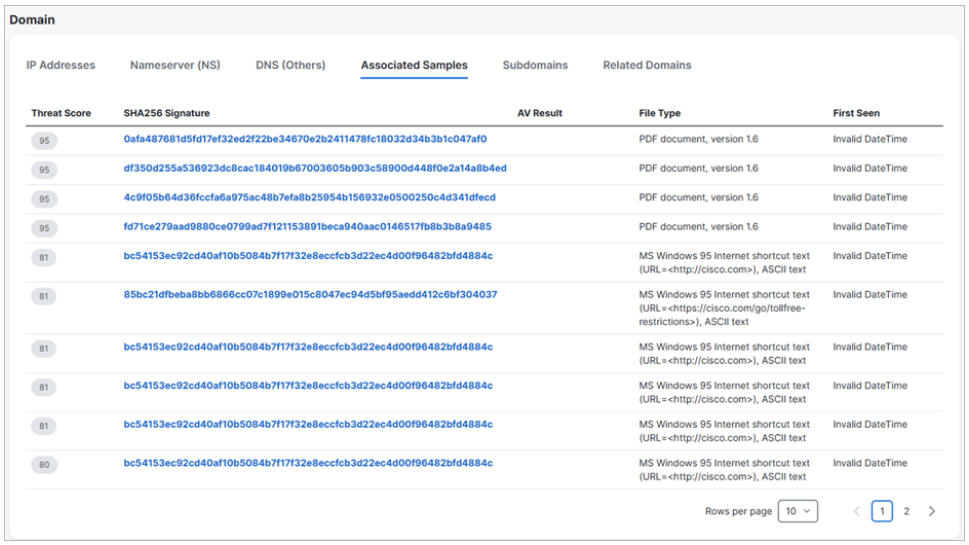
Describes About Associated Samples in Investigate in Cisco Secure Access. When you search for an IP, a domain, or URL, Secure Access Investigate lists any checksum samples associated with the destination.

When you search for an IP, a domain, or URL, Secure Access Investigate lists any checksum samples associated with the destination. A sample is a type of file, or file-like object created by a process running in memory. Cisco Secure Malware Analytics receives and analyzes submitted file samples and integrates the checksums with Secure Access Investigate. Associated samples are additional file samples known to be related to the main sample.

Cisco Secure Malware Analytics retains checksum samples for one year. You may find that Secure Access Investigate previously listed a sample related to a destination. If Cisco Secure Malware Analytics no longer contains a sample related to the destination, Investigate does not display the sample in the list of associated samples.

Note

Part of the functionality described for the Associated Samples feature of Investigate is only available with both Cisco Secure Malware Analytics and Secure Access Investigate subscriptions. For more information, contact Secure Access support. If you would like to add Cisco Secure Malware Analytics to your existing license, contact your account representative.



Click the link to the SHA-256 signature to display the Investigate Sample View. The Sample view shows information about the individual malware samples, including behavior of the sample on the network.

Note

Some normal, safe domains may have malicious samples associated with them. Malware may use a domain or IP to check internet connectivity or use a domain or IP as a source to determine more data about the host on which it resides–public IP of the infected host or network.

The Associated Sample tab lists up to 10 results per page and includes the following information:

- **Threat Score** – The score given to a particular sample based on the analysis performed by Cisco Secure Malware Analytics. A Threat Score is a measure of the amount of system weakening, obfuscation, persistence, modification, data exfiltration, and other behaviors which may be a threat to the host system's integrity. It is intended as an overall threat indicator that can be used as a guide to the likelihood that a submission is malicious. The Threat Score is not an authoritative classification of good and bad software.
- **SHA-256 Signature** – The SHA-256 checksum of the associated sample. Use the checksum to pivot to the information about the sample.

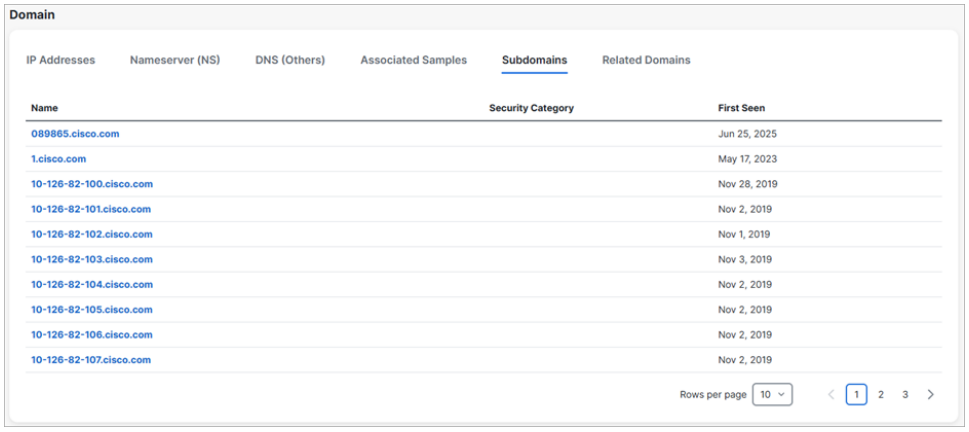
- **AV Result** – Antivirus results according to ClamAV. A sample can have more than one signature if it is detected under more than one family of malware. A sample may also have no signatures associated.
- **File Type** – The type of file associated with the checksum.
- **First Seen** – The date when the sample was first seen by Secure Access.

About the Subdomains Tab in Investigate

Describes About the Subdomains Tab in Investigate in Cisco Secure Access. The Subdomains tab lists all subdomains associated with the domain.

The Subdomains tab lists all subdomains associated with the domain.

- **Name** – The subdomain of the domain.
- **Security Category** – The type of security risk that this subdomain poses: for example, Malware. The security category is blank if the subdomain poses no risk.
- **First Seen** – The date when the subdomain was first detected. This date is determined from the NS records for this sub domain.



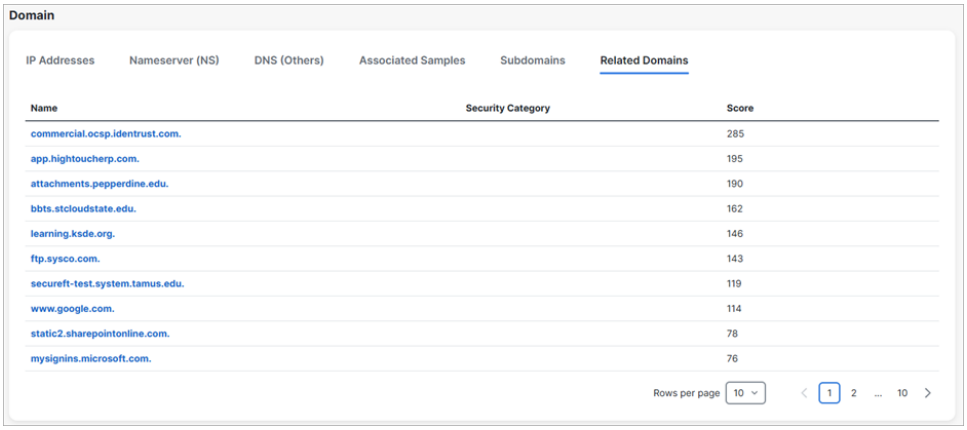
For information about the subdomain, click the link for the subdomain.

About Related Domains in Investigate

Describes About Related Domains in Investigate in Cisco Secure Access. The Related Domains tab lists the domain names that were frequently requested around the same time (up to 60 seconds before or after) as the domain name, but that are not frequently associated with other domain names.

The Related Domains tab lists the domain names that were frequently requested around the same time (up to 60 seconds before or after) as the domain name, but that are not frequently associated with other domain names.

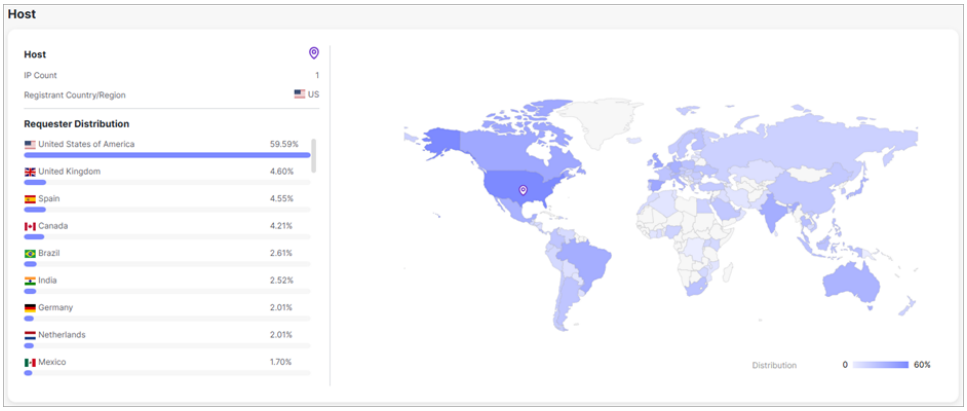
The **Score** reflects the number of client IP addresses that looked up related sites within 60 seconds of the original domain request.



About the Geographic Distribution View in Investigate

Describes About the Geographic Distribution View in Investigate in Cisco Secure Access. The Geographic Distribution displays a world map of the IP distribution for each searched domain.

The Geographic Distribution displays a world map of the IP distribution for each searched domain. The map shows the domain host countries (using pins), registrant information, and percentages of that distribution. The geographical representation shows our resolution data plotted across geolocations along with visual indicators to show distribution rates. You can use the Geographic Distribution map to define where a domain request originates.



- **Host** – Displays the physical location of the host IP addresses.
- **IP Count** – The number of IP addresses registered to the host.
- **Geo Distance (sum, mean)** – Lists both the sum and mean distances between hosts in kilometers. The distance between hosts is a mathematical algorithm scoring the relative distances between hosts serving the domain data. This algorithm reflects unusually high scores for the Mean Geo-distance and Sum Geo-distance in the domain features. An alert appears when the mean distance between hosts serving the site is over 3000 kilometers. In our research, we've found that hosts serving a non-malicious domain are geographically close, whereas a domain serving malware is served by hosts found around the globe. Our blog provides more information on how we use distance between domains to determine the maliciousness of certain domains.
- **Registrant Country** – Country of origin for the host.
- **Requester Distribution** – Hierarchical list in percentage of where in the world the domain requests occurred. Scroll your mouse over various countries on the map to see the percentage for each country.

About the Sample View in Investigate

Describes About the Sample View in Investigate in Cisco Secure Access. The Investigate Sample view displays the threat information obtained from a file hash or checksum.

The Investigate Sample view displays the threat information obtained from a file hash or checksum. You can search for a domain, IP, or URL related to security threats and obtain information about file checksums, threat scores, metadata, and antivirus results.

The Investigate Sample View may include data collected within the last two years by Cisco Secure Malware Analytics. In addition, you can use the Investigate Sample View to analyze a list of checksums gathered from a third-party data feed or in-house security information and event management (SIEM) system.

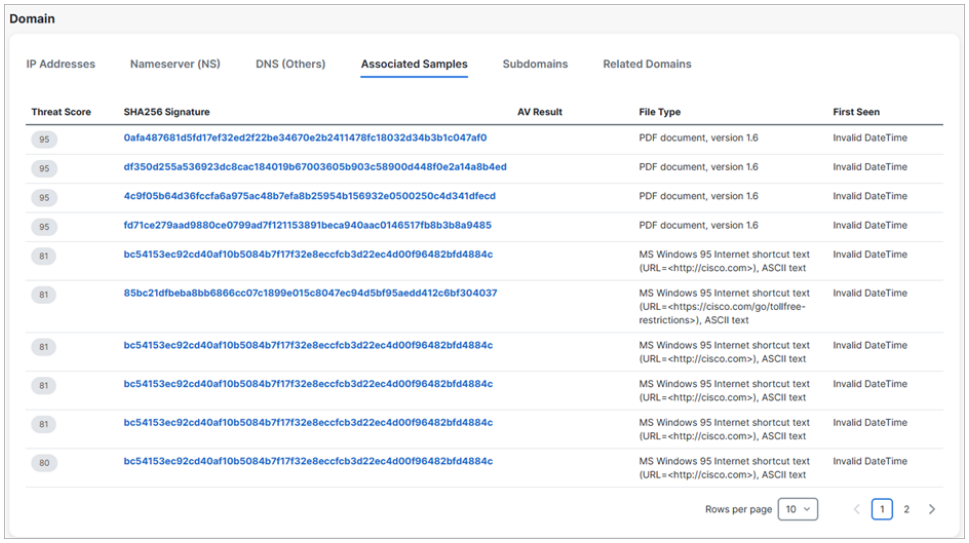
> **Note**
>
> Part of the Investigate Sample View functionality is only available with both Secure Access Investigate and Cisco Secure Malware Analytics subscriptions. For more information, contact Secure Access support. If you would like to add Cisco Secure Malware Analytics to your existing license, contact your account representative.

Get Started with Sample View

To get started, enter a checksum or file hash in the Investigate Smart Search, or pivot to the Sample view from the Domain or IP Address view.

> **Note**
>
> Investigate Sample View does not contain all data collected by Cisco Secure Malware Analytics. Some of the data collected does not match the criteria that Umbrella Investigate uses to detect security incidents.

If you begin with the Domain or IP Address view, navigate to the **Associated Samples** tab. Click the link to a sample to display the Sample view.



Sample View Details

The first part of the Sample View displays information about the checksum.



Components of a Threat Sample

- **SHA-256, SHA-1 and MD5 checksums of the sample** – The hash files or checksums which help to cross-reference samples against VirusTotal and similar databases.
- **Magic Type** – A file type based on established file format types that allow files to be associated by the operating system and executed or loaded into memory.
- **Threat Score** – The score given to a particular sample based on the analysis performed by Cisco Secure Malware Analytics. A threat score is a measure of the amount of system weakening, obfuscation, persistence, modification, data exfiltration, and other behaviors which may threaten the host system's integrity. The Threat Score is intended as an overall threat indicator or guide to a malicious system. The Threat Score is not an authoritative classification of good or bad software.
- **Size** – The size of the sample in bytes.
- **AV Results** – The Antivirus results according to ClamAV. A sample can have more than one signature if it is detected under more than one family of malware. A sample may also have no signatures associated with a virus.
- **First Seen** – The time stamp for when this sample was first seen by Cisco Secure Malware Analytics.

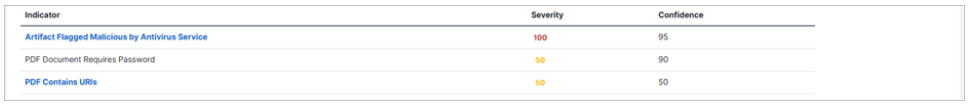
For more information, see Cisco Secure Malware Analytics.

Behavioral Indicators

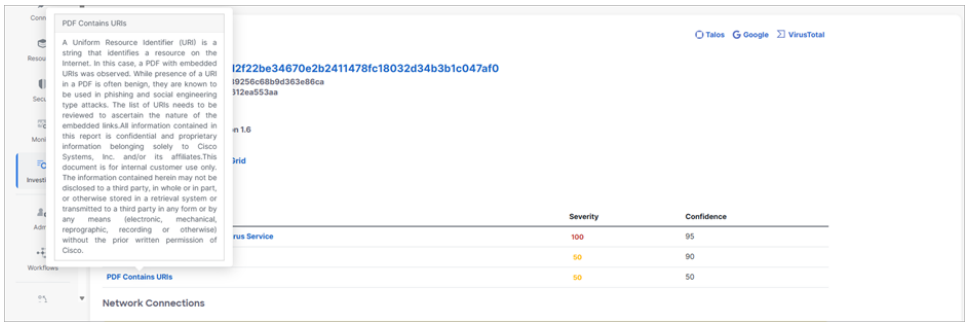
The Behavioral Indicators (BI) are key traits and behaviors which may indicate malicious activity. Behavioral indicators include threat severity levels, HTTP Traffic, DNS Traffic, TCP/IP network sessions, processes, artifacts, and registry activities.

Investigate provides two key indicator scores: **Severity** and **Confidence**.

- **Severity** – Indicates the likely security risk posed by a given behavior, ranging from 0 to 100.
- **Confidence** – Indicates the likelihood of the sample exhibiting the stated behavior, ranging from 0 to 100.



Click on the link to the behavioral indicator to view a description of the indicator.



Network Connections

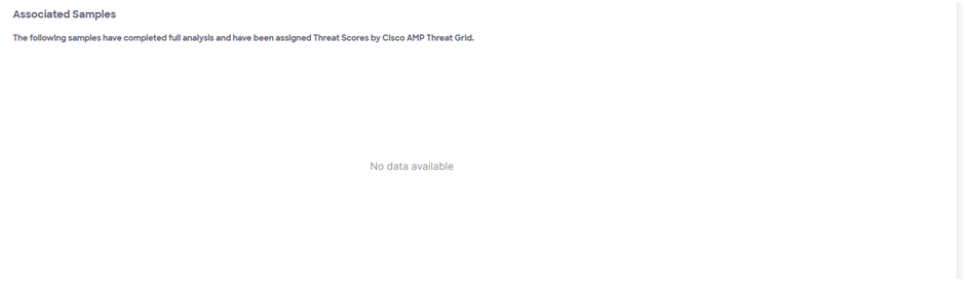
A network connection is made by a certain file sample to an IP or a domain. The Network Connections section lists the destination, URLs related to the domain or IP, and security categories for the connection.



Click on a destination to display the domain or IP Address view for the destination.

Associated Samples

A sample is a type of file, or file-like object, such as a process running in memory submitted and analyzed by Cisco Secure Malware Analytics. Associated samples are additional file samples known to be related to the main sample.

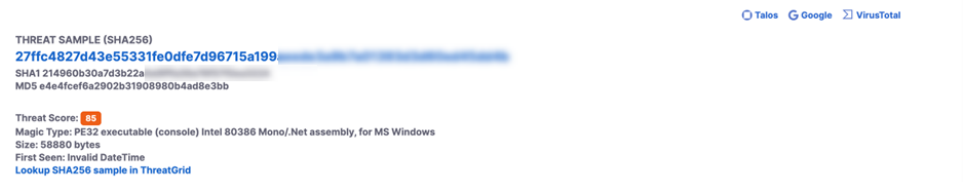


Associated Artifacts (Secure Malware Analytics Integration)

A threat artifact is a file that is created or modified during the analysis of a sample. Malware executables often download additional components and infect or modify system files, documents, and running processes. Artifacts are sometimes executables that you can analyze in Cisco Secure Malware Analytics.



Click on the link to a signature sample to display the details of the sample threat artifact.



About the IP Address View in Investigate

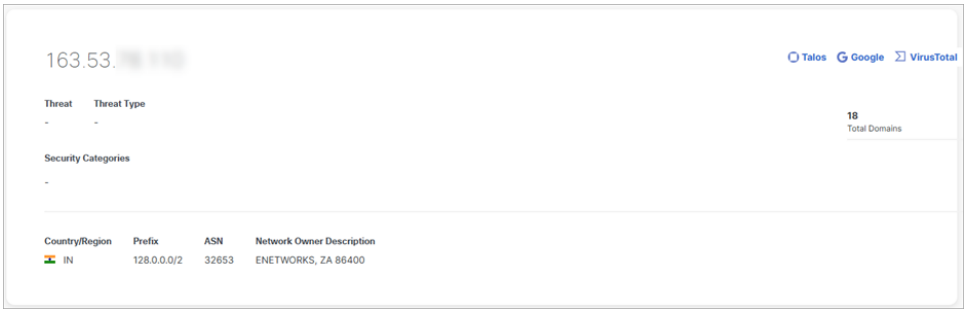
Describes About the IP Address View in Investigate in Cisco Secure Access. The Investigate IP address view includes a collection of data about an IP address: summary of key details, DNS resolution, Autonomous Systems (AS), associated samples, and recent detections.

The Investigate IP address view includes a collection of data about an IP address: summary of key details, DNS resolution, Autonomous Systems (AS), associated samples, and recent detections. Investigate displays the IP Address view when you use the Smart Search and provide an IP address, or when you link to an IP address from the Domain View. When you search for an IP address, specify the entire IP address. We currently do not support the option to search for a subnet, for example, a /24 network.

> **Note**
>
> The Investigate API /search endpoint accepts an IP subnet.

Summary

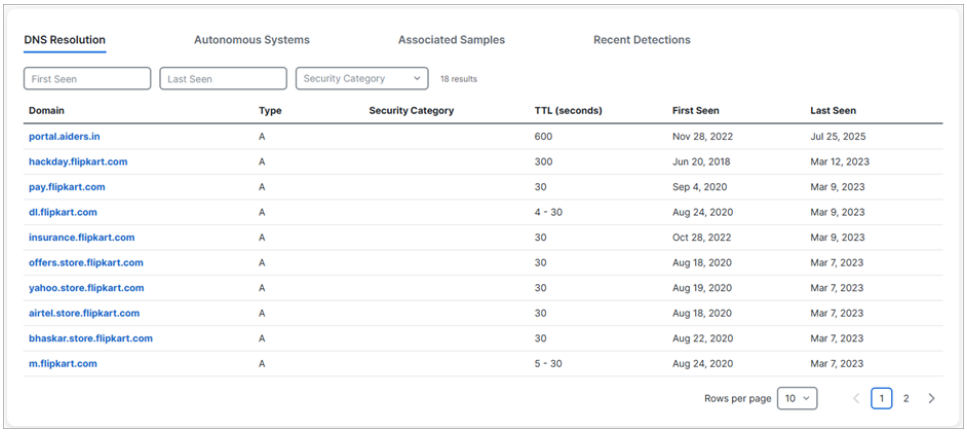
The IP Address summary provides the key details about an IP address: location, network, threats, security categories, links to integrated threat information, and an aggregate of malicious domains hosted on the IP grouped by security category.



> **Note**
>
> Watch for unexpected results when an IP address belongs to a content delivery network, or CDN. A malicious domain could potentially be hosted on any number of edge servers, depending on the requester's geographic location, load balancing at the CDN and the proxy cache time. As a result, searching for a single IP address belonging to a CDN may show that there are 0 malicious domains for that IP address because the content was being served on other, related IPs belonging to the CDN.

DNS Resolution

The DNS Resolution tab displays the list of domains associated with the IP address. The DNS Resolution view lists the domain name, type of record, and first seen and last seen dates.



Autonomous Systems

The Autonomous Systems (AS) tab lists the IP prefix, ASN of the IP address, and Network Owner Description. For more information about an ASN, click the link to the ASN.

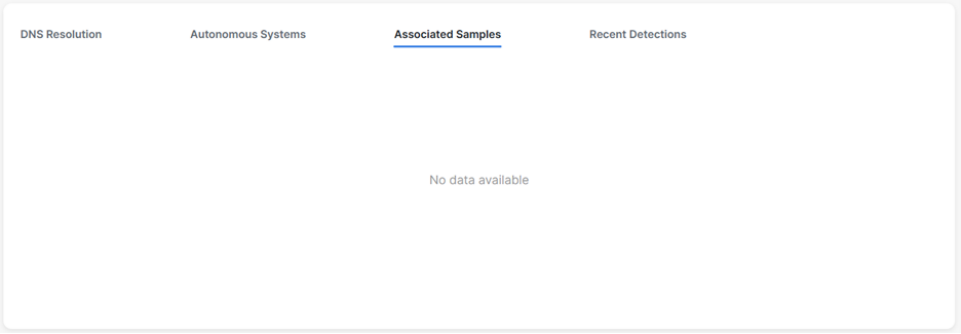


Associated Samples

When you search for an IP, a domain, or URL, Secure Access Investigate lists any checksum samples associated with the destination. A sample is a type of file, or file-like object created by a process running in memory. Cisco Secure Malware Analytics receives and analyzes submitted file samples and integrates the checksums with Secure Access Investigate. Associated samples are additional file samples known to be related to the main sample.

Cisco Secure Malware Analytics retains checksum samples for one year. You may find that Secure Access Investigate previously listed a sample related to a destination. If Cisco Secure Malware Analytics no longer contains the sample associated with the destination, Investigate does not display the sample in the list of associated samples.

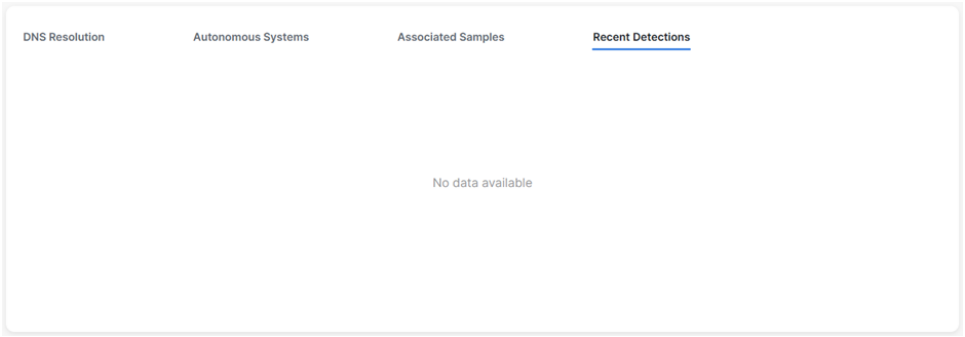
> **Note**
>
> Part of the functionality described for the Associated Samples feature of Investigate is only available for customers of both Cisco Secure Malware Analytics and Secure Access Investigate. For more information, contact Secure Access support.



The Associated Sample tab lists up to 10 results per page and includes the following information:

- **Threat Score** – The score given to a particular sample based on the analysis performed by Cisco Secure Malware Analytics. A Threat Score is a measure of the amount of system weakening, obfuscation, persistence, modification, data exfiltration, and other behaviors which may be a threat to the host system's integrity. It is intended as an overall threat indicator that can be used as a guide to the likelihood that a submission is malicious. The Threat Score is not an authoritative classification of good and bad software.
- **SHA-256 Signature** – The SHA-256 checksum of the associated sample. You can use the checksum to pivot to the specific information about the sample.
- **AV Result** – Antivirus results according to ClamAV. A sample can have more than one signature if it is possibly detected under more than one family of malware. A sample may also have no signatures associated.
- **File Type** – The type of file associated with the checksum.
- **First Seen** – The date when the sample was first seen by Secure Access.

Recent Detections



About WHOIS Record Information

Describes About WHOIS Record Information in Cisco Secure Access. The WHOIS record information is not gathered by performing a real time WHOIS lookup against another database.

The WHOIS record information is not gathered by performing a real time WHOIS lookup against another database. Instead, Secure Access Investigate maintains an extensive database of WHOIS record information. The WHOIS information shows the standard output of registered users or assignees for the domain queried, along with a full range of typical WHOIS data for a domain.

WHOIS data is generated from the domain registrars and, as a result, is not consistent in formatting, language or syntactical conventions. Investigate can return high-quality results when searching for gTLDs (for example, .com, .org and .net), but not from ccTLDs (for example, .ru, .cn, and co.uk). As a result of discrepancies, requests for information to our database can fail and there are times when historical or current records are not available.

WHOIS Record Is Unavailable

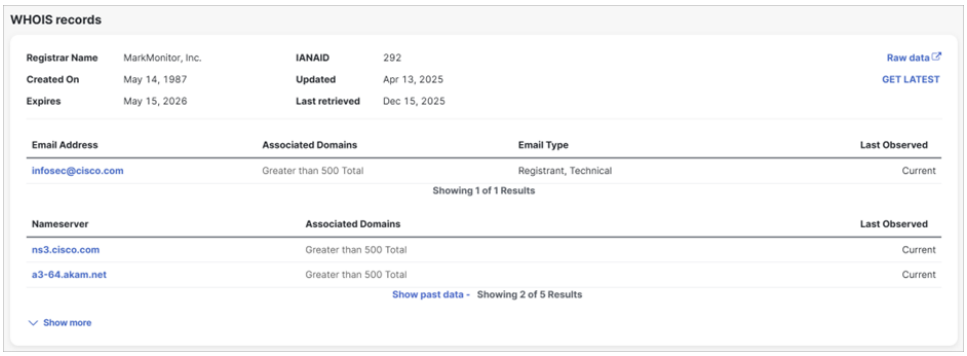
At times, WHOIS record information is not available. For example, the domain does not exist:

" Sorry, couldn't load WHOIS information for this domain”

> **Note**
>
> Data may also not be available if the WHOIS information is simply set to active with no details available.

WHOIS Record Contact Information

The first section of the WHOIS record information contains the Registrar Name and Internet Assigned Numbers Authority ID (IANAID) of the Registrar. For a full list of the IANAID, see Registrar IDs.



WHOIS Record Domain Availability

The next section of the WHOIS record includes fields related to when the domain was created, updated, or expires:

- **Created** – Date the domain was registered.
- **Updated** – Date the record was last updated.
- **Expires** – Date the record expires.

Click **Get latest** to refresh the record with the latest available data. This refresh can be helpful if the record seems outdated at first glance, or if you're reasonably confident that there is newer information available.

Click **Raw data** to open a new tab in your browser that displays the raw WHOIS record. If Investigate has no WHOIS record data, then the Raw data tab is blank.

WHOIS Record Email Addresses

Next, the WHOIS record lists the email addresses of the registrants for the domain.



Email Address	Associated Domains	Email Type	Last Observed
infosec@cisco.com	Greater than 500 Total	Registrant, Technical	Current

Showing 1 of 1 Results

The WHOIS Email Address section contains the following fields:

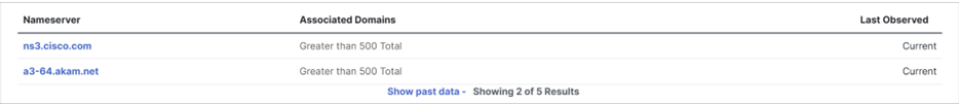
- **Email Address** – Address of the registrant associated with this domain.
- **Associated Domains** – The number of domains registered by this email address, including the number of malicious domains. The maximum number of Associated Domains is 500 and, where possible, the UI will show if any of the 500 gathered are malicious. The number of malicious domains only includes the ones in the first 500 results.
- **Email Type** – Owner, Administrator, Technical, Contact, Billing.
- **Last Observed** – Typically current, but changes to a date when the domain is no longer related to the email but was at some point in history. If Last Observed is dated, try clicking Get latest to refresh information.

If there is any historical information about the email address of the domain registrant, Investigate displays it under the “Show past data” button.

To pivot on the email and view information associated with the email address, click the email or the number associated domains to the email view of the WHOIS data.

WHOIS Record Nameservers

The WHOIS Record contains information about the name servers that provide zone records.



Nameserver	Associated Domains	Last Observed
ns3.cisco.com	Greater than 500 Total	Current
a3-64.akam.net	Greater than 500 Total	Current

Show past data - Showing 2 of 5 Results

The WHOIS nameservers section contains the following fields:

- **Nameserver** – Domain name of the nameserver.
- **Associated Domains** – The number of domains associated with the nameserver, including the number of malicious domains. The maximum number of Associated Domains is 500. Investigate displays the number of Associated Domains if any of the 500 domains are malicious.
- **Last Observed** – Current but may change to a date in the past when this domain is no longer associated with the nameserver but had been at some point in history. If Last Observed is dated, click Get Latest to refresh the information.

WHOIS Record Show More Data

For additional information about the WHOIS record connected to the personal details of the registrar–the Contact Name, Address, Phone number and Fax Number, click **Show more WHOIS Data**.

> **Note**
>
> In some cases, the information displayed may be falsified or obfuscated by malicious domain registrants and may not be of any particular value. You cannot pivot to other domains from this area of the WHOIS record.



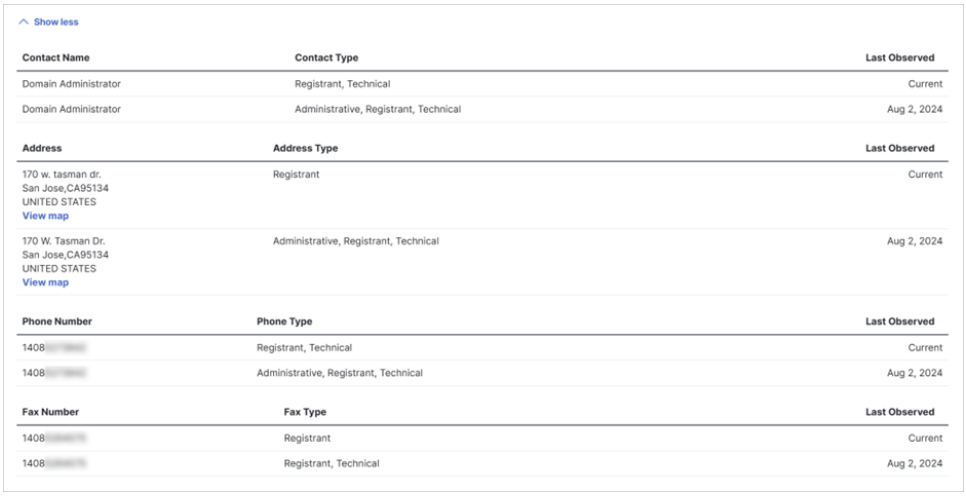
Nameserver	Associated Domains	Last Observed
ns3.cisco.com	Greater than 500 Total	Current
a3-64.akam.net	Greater than 500 Total	Current

Show past data - Showing 2 of 5 Results

Show more

The WHOIS record **Show more** section provides additional information which includes the Contact Name, Contact Type (Owner, Administrator, Technical, Contact, Billing), the date when the Contact Name Last Observed (Current, or a historical date), and the Registrant Address and Phone number (shown with their respective Type and Last Observed date). For each Address, there is a link to Google Maps.

> **Note**
>
> WHOIS data for addresses that do not follow any standard may fail to find the address location, and as a result fail to link to Google Maps.



Show less

Contact Name	Contact Type	Last Observed
Domain Administrator	Registrant, Technical	Current
Domain Administrator	Administrative, Registrant, Technical	Aug 2, 2024

Address	Address Type	Last Observed
170 w. tasman dr. San Jose,CA95134 UNITED STATES View map	Registrant	Current
170 W. Tasman Dr. San Jose,CA95134 UNITED STATES View map	Administrative, Registrant, Technical	Aug 2, 2024

Phone Number	Phone Type	Last Observed
1408	Registrant, Technical	Current
1408	Administrative, Registrant, Technical	Aug 2, 2024

Fax Number	Fax Type	Last Observed
1408	Registrant	Current
1408	Registrant, Technical	Aug 2, 2024

If the domain is a nameserver for other domains listed in the WHOIS database, the WHOIS records show these other domains. The information displays the domain-to-domain relationship (authoritative DNS) rather than an IP to domain relationship drawn from our DNS records.

About the WHOIS Nameserver View

Describes About the WHOIS Nameserver View in Cisco Secure Access. The Investigate WHOIS Nameserver view displays the WHOIS information for a nameserver.

The Investigate WHOIS Nameserver view displays the WHOIS information for a nameserver. A nameserver is a domain. A domain identifies as an authoritative nameserver when it provides responses to requests about names in a zone. However, any domain registrant can assign any domain as a nameserver, even if the domain is not serving records for their domain.

The WHOIS information for a domain enables you to find additional domains related to a certain domain. For instance, if you search for a domain that is flagged as malicious, you can locate other domains that are registered with the same nameserver.

To get started, enter the domain name of a nameserver in the Investigate Smart Search, or pivot to the Nameserver view from the Domain view. If you begin your search from a Domain view, follow the links to the nameserver information from the WHOIS data.

Prerequisites

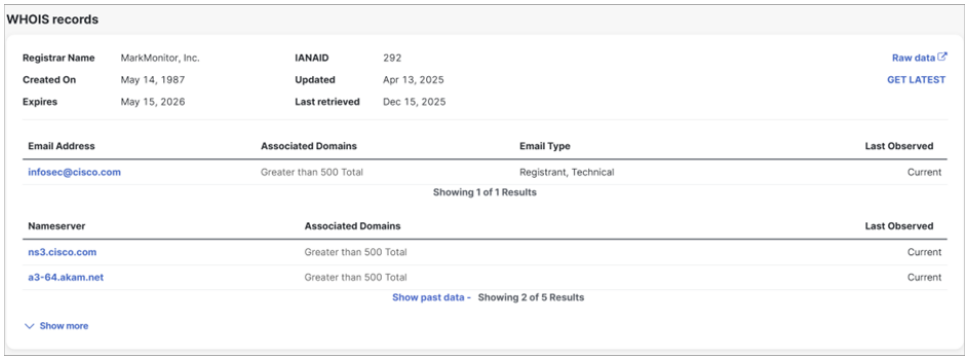
A minimum of Full Admin access to Secure Access.

Research WHOIS Nameserver From Domain View

The information described in the WHOIS record is retrieved from the Investigate WHOIS database and reflects an association between a domain that is a nameserver and another domain which is served by the nameserver.

Click on the link to the nameserver, or the number of the **Associated Domains** to view the domains associated with the nameserver.

> **Note**
>
> Secure Access Investigate lists no more than 500 domains associated with a nameserver.



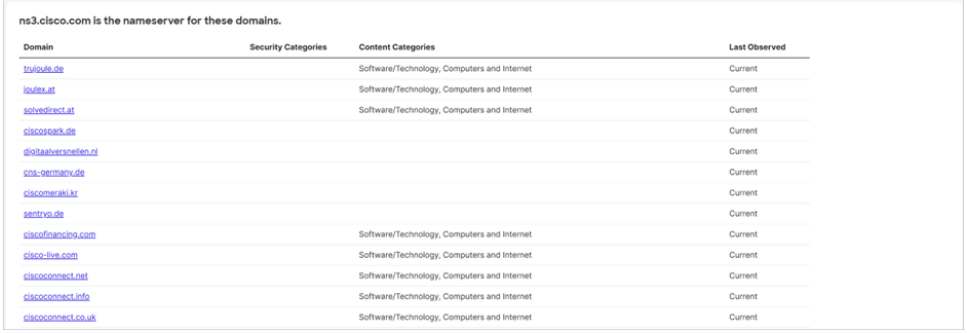
It is possible for a nameserver to have an A Record for its own domain. By recording its domain name, a nameserver can show its domain along with its stored domain records.

In the Domain and IP Address views, Investigate provides detailed information about the domain or IP address. The nameserver information in the Domain or IP address views are gathered from DNS data from our DNS resolvers and is an association between IP address and domain.

WHOIS Nameserver View

The WHOIS Nameserver view displays a list of the malicious domains, security categories, content categories, and indicator of when the domain was last observed. Investigate categorizes when a domain was last observed as: **Current** or **Past**. Investigate displays **Current** if the domain currently belongs to the name server and **Past** if the domain once belonged to this nameserver.

Click the link to the domain name to display the Domain view for the domain.



FAQs

Describes FAQs in Cisco Secure Access. The Investigate WHOIS data is compiled from information given by domain registrants to domain registrars.

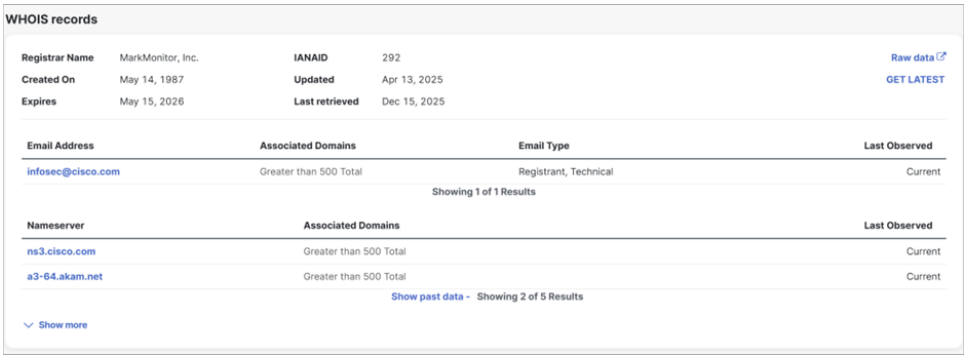
The Investigate WHOIS data is compiled from information given by domain registrants to domain registrars. Unfortunately, a fair amount of the data given to a registrant is falsified or forged or simply omitted. In general, the less complete or seemingly authentic the WHOIS data displayed is, the less trustworthy the website associated with that registrar is.

As a result, you may see WHOIS results that look strange, malformed or even corrupt – these results are expected and there are practical reasons for them. The volume of WHOIS data on the internet imposes practical limitations in what we can display in Investigate or return in an Investigate API response.

The FAQ answers general questions about how to use WHOIS data.

Q: Why doesn't this domain have an email or nameserver associated with it?

A: In the following example, the domain is missing email information from the WHOIS record. The WHOIS record is incomplete and is likely suspicious. Typically, the email is found between the Created and Updated dates and the Nameserver information. To view the raw WHOIS record, click **Raw data**.



Q: Why does information under "Show More WHOIS data" appear corrupt or not make any sense?

A: Similar to the previous question, expanding the **Show more WHOIS data** field shows strange information and as a result, the link to Google Maps may not work as expected. To view the raw WHOIS record, click **Raw data**. The standards for providing accurate data when registering a domain are quite loose and depend on the registrar's requirements.

If the data in the **Show More WHOIS data** appears incomplete or forged, the domain may be malicious. However, the WHOIS record may contain typos, created when at the time of domain registration.

Q: Why isn't the malicious domain I'm looking at not listed in the 500 email addresses or nameservers displayed?

A: Investigate only retrieves the first 500 results from the WHOIS database for performance reasons. Some email or nameservers have tens of thousands of domains associated with them. Gathering that data in a single query slows the performance of our systems down significantly, harming your user experience. In some instances, the first 500 domains retrieved for an email or nameserver won't include the domain you're actually looking at.

In general, if a nameserver or email address is associated with 500 or more domains and enough of them are considered non-malicious to not show up, you can assume that the email is forged by a malicious domain but is otherwise legitimate. Or, in case of a nameserver, it's a good assumption that the nameserver provides records for legitimate domains and is not a point of interest.

Q: The registration dates for this domain are strange, and data seems to be missing from history. What happened in these types of cases?

A: Some domains were registered, then the registration expired, then the domain was renewed at a later date. During the time when the domain was not registered, there was no WHOIS information and historically, there's a gap in the data. There simply is no WHOIS data when a domain isn't registered and that's reflected in our results.

About the ASN View

Describes About the ASN View in Cisco Secure Access. The Investigate Autonomous System Number (ASN) view includes the current information about an Autonomous System (AS) and the current routes that show the subnets assigned to an AS.

The Investigate Autonomous System Number (ASN) view includes the current information about an Autonomous System (AS) and the current routes that show the subnets assigned to an AS. Investigate displays the ASN view when you use the Smart Search and provide an AS number, or when you link to an ASN from the Domain or IP address view that shows the AS for the primary site. When you search for AS information, specify the AS number without the AS prefix, for example, search for `36692`, but not `AS36692`.

Prerequisites

A minimum of Full Admin access to Secure Access.

Current Information

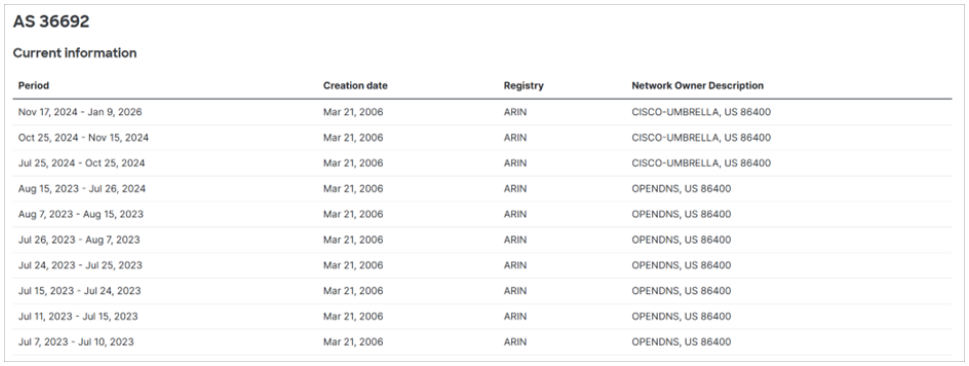
Describes Current Information in Cisco Secure Access. The AS Current Information view includes the time period when the AS was published, the creation date when the AS routes were published, the Regional Internet Registry (RIR) for the ASN, and the description of the network owner.

The AS Current Information view includes the time period when the AS was published, the creation date when the AS routes were published, the Regional Internet Registry (RIR) for the ASN, and the description of the network owner.

Investigate lists the registry information with the appropriate regional registry. The registries and associated regions are:

- **AfriNIC** – Africa
- **APNIC** – Asia, Australia, New Zealand, and neighboring countries
- **ARIN** – United States, Canada, several parts of the Caribbean region, and Antarctica
- **LACNIC** – Latin America and parts of the Caribbean region
- **RIPE NCC** – Europe, Russia, the Middle East, and Central Asia

> **Note**
>
> If no registry is available, Investigate displays Unknown / Not Available.



AS 36692

Current information

Period	Creation date	Registry	Network Owner Description
Nov 17, 2024 - Jan 9, 2026	Mar 21, 2006	ARIN	CISCO-UMBRELLA, US 86400
Oct 25, 2024 - Nov 15, 2024	Mar 21, 2006	ARIN	CISCO-UMBRELLA, US 86400
Jul 25, 2024 - Oct 25, 2024	Mar 21, 2006	ARIN	CISCO-UMBRELLA, US 86400
Aug 15, 2023 - Jul 26, 2024	Mar 21, 2006	ARIN	OPENDNS, US 86400
Aug 7, 2023 - Aug 15, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400
Jul 26, 2023 - Aug 7, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400
Jul 24, 2023 - Jul 25, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400
Jul 15, 2023 - Jul 24, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400
Jul 11, 2023 - Jul 15, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400
Jul 7, 2023 - Jul 10, 2023	Mar 21, 2006	ARIN	OPENDNS, US 86400

Current Routes

Describes Current Routes in Cisco Secure Access. The AS Current routes view displays the subnets assigned to each AS, including any suspicious sites associated with the subnets within the last seven days.

The AS Current routes view displays the subnets assigned to each AS, including any suspicious sites associated with the subnets within the last seven days. Note that the domains listed as suspicious have the IP for the route as part of their DNS records, but that does not indicate that you should add the subnet or the ASN to a block list.

The number of suspicious domains as a percentage of benign domains varies based on the AS and the subnet, but it is unlikely that any one AS or subnet is entirely malicious. The ASN view can help to investigate suspicious activity originating toward subnets associated with other malicious traffic. Looking at the associated domains and the geographic location of the AS and associated subnets is a way to build a framework for investigation.



Current routes for AS

Prefix	Country/Region	Suspicious activity in the past week
67.215.64.0/24	United States of America	
67.215.65.0/24	United States of America	
67.215.66.0/24	United States of America	
67.215.69.0/24	United States of America	
67.215.70.0/24	United States of America	
67.215.73.0/24	United States of America	
67.215.76.0/24	United States of America	
67.215.78.0/24	United States of America	
67.215.79.0/24	United States of America	
67.215.80.0/24	Singapore	
67.215.81.0/24	United States of America	
67.215.82.0/24	Hong Kong	

Research AS From IP Address View

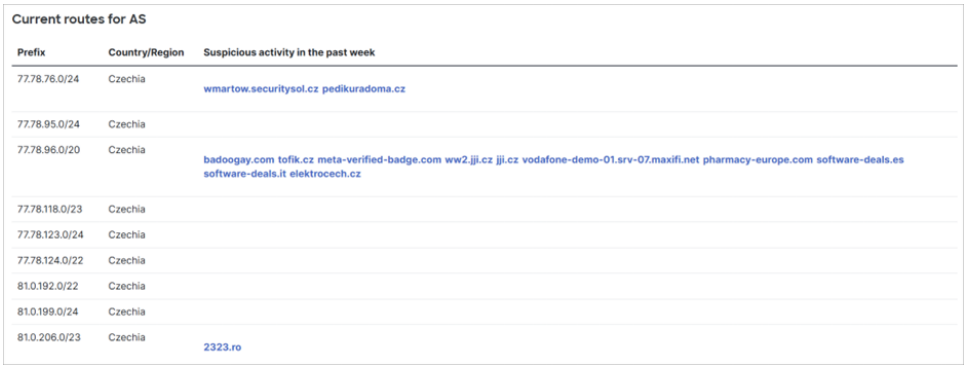
Describes Research AS From IP Address View in Cisco Secure Access. You can research an AS number by providing an IP address to the Investigate Smart Search, for example: 82.208.40.8.

You can research an AS number by providing an IP address to the Investigate Smart Search, for example: 82.208.40.8. Investigate returns a list of 66 malicious domains hosted by this IP address for the past week.



The ASN for the IP address, 82.208.40.8, is AS15685, and the network owner is **CASABLANCA-AS**. AS15685 is part of **RIPE-NIC**, which includes Europe. The description of the network owner provides geolocation details about the AS.

From the **IP address view > Autonomous Systems** tab, click the number of the AS to display the **Investigate ASN view > Current routes for AS**. The Current routes for AS lists the suspicious domains associated with a route for the last seven days.



Part V

Mobile Device Management

Topics:

- Client-based Zero Trust Access from Mobile Devices
- Cisco Secure Client on Windows, macOS, and Linux Devices
- Zero Trust Access using Cisco Secure Client
- Endpoint Data Loss Prevention using Cisco Secure Client
- Virtual Private Networks on Cisco Secure Client
- Internet Security on Cisco Secure Client
- Endpoint Diagnostic Tool
- Managed iOS
- Managed Android
- Unmanaged Mobile Devices

Cisco offers a fully featured secure client for Windows, macOS, and Linux devices as well as platform-native Zero Trust Access client apps for iOS devices and Samsung devices running Android.

57 Client-based Zero Trust Access from Mobile Devices

Topics:

- Get Started and Manage Client-based Zero Trust Access from Mobile Devices
- Set up the Zero Trust Access App for iOS Devices
- Set up the Zero Trust Access App for Android Devices
- Set up the Zero Trust Access App for Android on Samsung Devices
- Monitor and Troubleshoot the Zero Trust Access App from Mobile Devices

Provides an overview of Client-based Zero Trust Access from Mobile Devices in Cisco Secure Access, including Get Started and Manage Client-based Zero Trust Access from Mobile Devices. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started and Manage Client-based Zero Trust Access from Mobile Devices

Describes Get Started and Manage Client-based Zero Trust Access from Mobile Devices in Cisco Secure Access. Secure Access offers client-based Zero Trust Access to private resources using a platform-native app on certain mobile devices.

Secure Access offers client-based Zero Trust Access to private resources using a platform-native app on certain mobile devices.

- Set up the Zero Trust Access App for iOS Devices
- Set up the Zero Trust Access App for Android Devices
- Set up the Zero Trust Access App for Android on Samsung Devices Devices
- Monitor and Troubleshoot Zero Trust Access from Mobile Devices

Set up the Zero Trust Access App for iOS Devices

Describes Set up the Zero Trust Access App for iOS Devices in Cisco Secure Access. End users can access private resources from their Apple iOS mobile devices (iPhone or iPad) using the Zero Trust Access app.

End users can access private resources from their Apple iOS mobile devices (iPhone or iPad) using the Zero Trust Access app. This Cisco Secure Client app uses Apple's platform-native zero trust network access technology.

Zero Trust Access app for iOS:



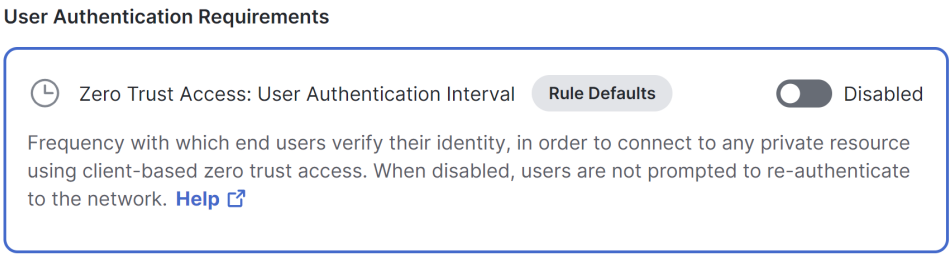
System Requirements

Apple iPhone or iPad running iOS 17.2 or later

Guidelines and Limitations

Describes Guidelines and Limitations in Cisco Secure Access. iOS does not currently support step-up authentication, so users will not be able to use the Zero Trust Access app to access a private resource if step up authentication is enabled for that resource.

- iOS does not currently support step-up authentication, so users will not be able to use the Zero Trust Access app to access a private resource if step up authentication is enabled for that resource. You can disable this functionality by default on the Rule Defaults page, or disable it in private access rules that include access for iOS devices:

  For information, see Network Authentication for Zero Trust Access.

- Traffic originating from the iOS client has an implicit subdomain wildcard on every rule. So, for example, if a resource is configured with the address `foo.com`, iOS traffic to that resource will also match `bar.foo.com`. Configure your private resources and rules accordingly.

Configure iOS Settings

Describes Configure iOS Settings in Cisco Secure Access and explains Configure iOS Settings in Secure Access and Configure iOS Settings in MDM. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Configure iOS Settings in Secure Access

We strongly recommend making the following configuration changes in the Secure Access dashboard:

1. Configure a client-based posture profile that includes iOS devices and supported iOS versions: Navigate to **Secure** > **Endpoint Posture Profiles**. For information, see Add a Client-Based Zero Trust Access Posture Profile.
2. Ensure that each applicable private resource is configured to allow client-based Zero Trust Access connections. For information, see Add a Private Resource.
3. Ensure that a network tunnel group or resource connector group is configured to send ZTA traffic to this resource. Navigate to **Connect** > **End User Connectivity**. For information, see Manage Network Connections.
4. Configure a private access rule that allows traffic to the applicable private resources using the posture profile you configured in Step 1.
5. Ensure that the end user is configured for single sign-on authentication (SSO).

Configure iOS Settings in Mobile Device Manager (MDM)

At this time, Apple iOS 5.1.19 supports certificate-based zero touch enrollment through the ManagedApp tool. Administrators can use a compatible EMM solution with Declarative Device Management (DDM) support for managed applications to provision the enrollment choice configuration and enrollment certificate identity to ZTA. For more information specifically on Apple managed apps, search for "Apple's guidance for configuring managed apps".

Use the following configurations for certificate-based zero touch enrollment:

- The device runs iOS 18.4 or later, which supports the ManagedApp configuration and credential delivery used by this feature.
- ZTA 5.1.19 or later is deployed as a managed app.
- The EMM solution supports Apple's DDM managed application configuration and credential provisioning. General DDM support alone does not establish support for these capabilities.
- A valid ZTA enrollment choice file is configured for certificate-based enrollment, and a certificate identity matching its certificate selection requirements is available.
- `"enrollment_choice": <enrollment choice file content>`. This allows you to deploy a different enrollment choice file instead of the default file.
- `"DeviceUniqueIdentifier": <device UDID>`. This allows the admin to set a unique device ID to the enrolled device into each connection request to the private resource to assist in identify the user's device.

Using the EMM solution, provision the certificate identity and enrollment choice configuration to the managed ZTA app. A certificate identity includes the certificate and its associated private key.

Install the App

Describes Install the App in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

There are two ways to distribute the app to IOS devices:

- You or end users can obtain the app from the App Store

- You can use your EMM/MDM vendor ecosystem

Have End Users Enroll in Zero Trust Access

Describes Have End Users Enroll in Zero Trust Access in Cisco Secure Access. The Zero Trust Access client app will walk end users through the enrollment process, which they should find reasonably straightforward.

The Zero Trust Access client app will walk end users through the enrollment process, which they should find reasonably straightforward.

You can give your end users the following instructions for (if applicable) installing the app and enrolling in Zero Trust Access:

1. If your administrator has not yet installed the Zero Trust Access app on your device: Install the app from the App Store.
2. In order to enroll your device for Zero Trust Access, you will need your work email address and your single sign-on credentials.
3. Launch the app and follow the instructions.

   Important

   In order to avoid unpredictable disruptions when accessing your organization's resources, you should allow notifications.

   a. You will be prompted to sign in using Single sign-on credentials.
   b. When you see an **Approve** prompt, verify that the information on the screen is correct, then tap **Approve**.
   c. You may need to sign in again the first time you access an application on your network.
4. You may be required to sign in again periodically in order to access applications on your network. This is expected.

Notes for administrators

Describes Notes for administrators in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- The enrollment process recommends that users allow notifications. Notifications keep users up-to-date on Zero Trust Access and allows the Zero Trust Access application to communicate with the backend relay configuration.
- To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

Set up the Zero Trust Access App for Android Devices

Describes Set up the Zero Trust Access App for Android Devices in Cisco Secure Access. End users can access private resources from their mobile devices running the Android operating system using the Zero Trust Access app.

End users can access private resources from their mobile devices running the Android operating system using the Zero Trust Access app. For information on client limitations and a comparison between generic Android and Samsung Android, see Release Notes for Cisco Secure Client.

Requirements and Prerequisites

- A device running Android version 14+.

- A Google Play store account.

Configure Cisco Secure Access

Provides instructions for completing the Configure Cisco Secure Access workflow in Cisco Secure Access. Configure a posture profile for client-based Zero Trust Connections that includes Android devices: Navigate to Secure Endpoint Posture Profiles .

Procedure

1. Configure a posture profile for client-based Zero Trust Connections that includes Android devices: Navigate to **Secure** > **Endpoint Posture Profiles**.
2. Configure a private resource that allows client-based ZTA connections: Navigate to **Resources** > **Private Resources**.
3. Ensure that a network tunnel or resource connector is configured to send ZTA traffic to this resource. Navigate to **Connect** > **End User Connectivity**.
4. Configure a private access rule that allows the user ID associated with the Samsung Android device to access the private resource you configured above. Select a posture profile that includes Android devices. Navigate to **Secure** > **Access Rules**.

Install the App

Describes Install the App in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

There are two ways to distribute the app to Android Samsung devices:

- You or end users can obtain the app from the Google Play store: https://play.google.com/store/apps/details?id=com.cisco.secureclient.zta
- You can use your EMM/MDM vendor ecosystem

Notes for administrators

Describes Notes for administrators in Cisco Secure Access. To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

- To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

Set up the Zero Trust Access App for Android on Samsung Devices

Describes Set up the Zero Trust Access App for Android on Samsung Devices in Cisco Secure Access. End users can access private resources from their Samsung mobile devices running the Android operating system using the Zero Trust Access app.

End users can access private resources from their Samsung mobile devices running the Android operating system using the Zero Trust Access app. This Cisco Secure Client app uses platform-native zero trust network access technology.

Cisco Zero Trust Access app:



Requirements and Prerequisites

- Samsung device running Android version 14+ and Samsung Knox 3.10 or higher. Example: Samsung S23.
- A Mobile Device Management (MDM) System where Samsung Knox Service Plugin (KSP) can be configured. Cisco has tested Ivanti Neurons, formerly known as MobileIron cloud version.
- A Google Play store account.

Configure Android Settings in Secure Access

Describes Configure Android Settings in Secure Access and explains Configure Android Settings in Sucre Access and Configure Android Settings in MDM. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Configure Android Settings in Sucre Access

We strongly recommend making the following configuration changes in the Secure Access dashboard:

1. Configure a posture profile for client-based Zero Trust Connections that includes Android devices: Navigate to **Secure** > **Endpoint Posture Profiles**.
2. Configure a private resource that allows client-based ZTA connections: Navigate to **Resources** > **Private Resources**.
3. Ensure that a network tunnel or resource connector is configured to send ZTA traffic to this resource. Navigate to **Connect** > **End User Connectivity**.
4. Configure a private access rule that allows the user ID associated with the Samsung Android device to access the private resource you configured above. Select a posture profile that includes Android devices. Navigate to **Secure** > **Access Rules**.

Configure Android Settings in MDM

We strongly recommend configuring the following settings in your Mobile Device Manager (MDM) to support the full range of functionality and features that Secure Access has to offer.

- (Optional) **Administrator Email Address** - Set a default administrator email address for sending logs
- (Optional) **Device ID** - Set a custom device ID
- (Optional) **Enrollment Choice** - Set the enrollment choice file content
- (Optional) **Allowed Certificate Aliases** - Comma-separated list of certificate aliases the app is allowed to use.

Install the App

Describes Install the App in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

There are two ways to distribute the app to Android Samsung devices:

- You or end users can obtain the app from the Google Play store: https://play.google.com/store/apps/details?id=com.cisco.secureclient.zta
- You can use your EMM/MDM vendor ecosystem

(Optional) Set up the Android device for Zero Trust Access using MDM

Describes (Optional) Set up the Android device for Zero Trust Access using MDM in Cisco Secure Access. If your organization uses a Mobile Device Management (MDM) solution, you can streamline and automate the deployment and configuration of the Zero Trust Access (ZTA) app on Android devices.

If your organization uses a Mobile Device Management (MDM) solution, you can streamline and automate the deployment and configuration of the Zero Trust Access (ZTA) app on Android devices. Using MDM allows you to enforce consistent security policies across all devices and makes the setup process easier for end users.

The following procedures describe how to:

1. **Add the app to MDM**
2. **Set up the App on the Samsung device**

Add the app to MDM

Provides instructions for completing the Add the app to MDM workflow in Cisco Secure Access. Follow these steps to deploy the Knox Service Plugin (KSP) and configure the Cisco Secure Client (Zero Trust Access) app for Samsung devices using Ivanti.

Follow these steps to deploy the Knox Service Plugin (KSP) and configure the Cisco Secure Client (Zero Trust Access) app for Samsung devices using Ivanti.

Procedure

1. Sign in to your Ivanti dashboard with administrator credentials.
2. Add Knox Service Plugin to App Catalog.
   a) Navigate to **Apps** > **App** Catalog and click **+Add**.
   b) From the **Source** drop-down, choose **Google Play store**.
   c) In the **Search** field, enter **Knox Service Plugin**. The app should appear. If it does not, check your spelling, network, or permissions.
   d) Click **Knox Service Plugin** and then click **Approve** if prompted.
   e) Click **Select** and change the category for the app if needed. Then click **Next**.
3. Assign the App to Users or Devices.
   a) By default, **Delegate this app to all spaces** is selected. Click **Next**.
   b) Choose which people or devices will get the Knox Service Plugin (KSP) app. By default, **Everyone** is selected. Click **Next**.
4. Configure Managed Settings.
   a) If **Managed Configurations for Android** does not appear, add it and give it a name.
   b) Enable **Auto-launch on install**.
   c) In the **Managed Configurations** section, click **Expand All** to display all settings.
5. Enter Knox and ZTNA Details.
   a) If you need to obtain a free Knox License key for the next steps, see Manage Knox Licenses.
   b) In the **Profile name(version)** field, enter your Samsung Knox profile name and make sure the slider is set to **On**.
   c) In the **Knox License key(Knox Suite, DualDAR, etc)** field, enter your Samsung Knox license key and set the slider **On**.
   d) Enable **Debug Mode**.
6. Select Device Enrollment Type.
   a) In the **Device-wide policies** section, choose the device enrollment type as:

Fully Manage Device (DO)

or

Work Profile-on company owned devices (WP-C), also known as PO (Profile Owner)

> **Note**
>
> PO enrollment is more common. These instructions assume PO enrollment.

Important

If you are doing a PO-type enrollment, ensure your device is not part of any other configuration, as it could conflict with the PO config.

7. Configure ZTNA Policy.
   a) Scroll down to the **ZTNA Policy** section.
   b) Enable the **Enable ZTNA controls** setting.
   a) In the **Package Name** field, enter `com.cisco.secureclient.zta` (if needed, click the **Refresh** button to the right of the field to allow typing).
   b) You can leave **Package Signature** blank.
8. Click **Next** to finish Managed App configuration.
9. Set Device Installation Requirements.
   a) For **Install on device**, add a config or edit the config if one is listed.
   b) Enable **Device Installation Configurations** and **Require installation on device**.
   c) Click **Update** or **Save** to retain your changes.
10. Assign and Distribute the Configuration.
    a) From the left menu, navigate to **Configurations**.
    b) Find the configuration called **Android enterprise: Work Profile (Android for Work)** or similar and click it.
    c) Click the pencil to edit the configuration.
    d) Click **Next** on the first screen.
    e) On the **Distribute** screen, make sure your user/device/group is selected.
    f) Click **Done**.

Set up the App on the Samsung Device

Provides instructions for completing the Set up the App on the Samsung Device workflow in Cisco Secure Access. Follow these steps to enroll your Samsung device and install the Cisco Zero Trust Access app using Ivanti MDM.

Follow these steps to enroll your Samsung device and install the Cisco Zero Trust Access app using Ivanti MDM.

Procedure

---

1. Enroll the Device in Ivanti MDM.
   a) On the Samsung device, sign into your Google Play store account.

b) Install the **Ivanti Go** app from the Google Play store.
c) Open the **Ivanti Go** app and enter your work email address to begin MDM enrollment.
d) Enter your Ivanti password.
e) Follow the remaining steps to complete MDM enrollment.

2. Verify Work Profile Creation.
   a) Once enrollment is complete, your device will have a Work profile managed by your MDM.
      This is a separate partition on the device for "work apps," which appear with a small briefcase icon to distinguish them from personal apps.
   b) To view your work apps:
      1. Swipe up from the bottom of the phone to show all installed apps.
      2. At the bottom, select **Work** to display apps installed in the work profile.
      3. **Personal** will show your regular apps.
3. Confirm App Installation in Ivanti.
   a) In the Ivanti dashboard, navigate to **Devices** > **Devices**.
   b) Locate your device by name or model number.
   c) Click on your device, then select the **Installed Apps** tab.
   d) Wait a few minutes for the **Knox Service Plugin (KSP)** app to appear in the list of installed apps.
      The KSP app and any other configured apps should be installed automatically.
4. Activate and Update KSP.
   a) On the device, open the **Knox Service Plugin** app from the Work profile.
   b) The work profile should display a configuration and indicate a successful setup.
   c) If the configuration is not successful, tap the **APPLY LATEST POLICIES** button to update it.
5. Add Google Play Account to Work Profile.
   a) On your Samsung device, add your Google Play store account to the Work profile. (Navigate to **Android Settings** > **Manage Accounts** > **Work** > **Add Account**.)
6. Install the Cisco Zero Trust Access app.
   a) In the work profile, open the **Play Store** app and ensure the correct Google Play account is selected.
   b) In the search field, enter **Cisco Zero Trust Access** or the app ID **com.cisco.secureclient.zta**.
   c) Tap and install the **Cisco Zero Trust Access** app or use this direct link.

Enroll the Device in Zero Trust Access

Provides instructions for completing the Enroll the Device in Zero Trust Access workflow in Cisco Secure Access. If you do not use an EMM/MDM tool to install the app, either you or the end user can install the app from the Google Play store.

If you do not use an EMM/MDM tool to install the app, either you or the end user can install the app from the Google Play store. After the app is installed, either you or the user can enroll the app in Zero Trust Access.

If applicable, you can give these instructions to the end user:

Procedure

1. If your administrator has not yet installed the Zero Trust Access app on your device:

   Install the app from the Google Play store.

2. The first time you start the Zero Trust Access app, if your administrator has not yet enrolled your device, the app will prompt you to enroll in Zero Trust Access.
3. In order to enroll your device for Zero Trust Access, you will need your work email address and your single sign-on credentials.
4. Start the Zero Trust app.
5. Follow the instructions on the screens.

   Important

   You must allow notifications or the app will not work!

   a. You will be prompted to sign in using Single sign-on credentials.

   b. When you see an **Approve** prompt, verify that the information on the screen is correct, then tap **Approve**.

   c. You may need to sign in again the first time you access an application on your network.

6. You may be required to sign in again periodically in order to access applications on your network. This is expected.

Notes for administrators

Describes Notes for administrators in Cisco Secure Access. To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

- To monitor and troubleshoot client-based zero trust access connections from mobile devices, see Monitor and Troubleshoot Zero Trust Access from Mobile Devices.

Monitor and Troubleshoot the Zero Trust Access App from Mobile Devices

Describes Monitor and Troubleshoot the Zero Trust Access App from Mobile Devices in Cisco Secure Access. This topic applies to client-based zero trust access connections from iOS devices and Samsung devices running Android operating systems.

This topic applies to client-based zero trust access connections from iOS devices and Samsung devices running Android operating systems.

Monitor Activity

After a mobile device begins to access private resources, you can monitor that activity:

- To view details about the enrolled device including, app version, client version and sync / enrollment dates:

  Navigate to **Connect** > **Users and Groups** page and click the user enrolled in the mobile app.

- To view access logs:

  Navigate to **Monitor** > **Activity** Search. To filter the view, click on **ZTNA client-based** on the top right side of the table and select an appropriate time window.

  - iOS access logs will have `apple-ios` in the OS column.
  - Android access logs will have `samsung-android` in the OS column.

General Troubleshooting

Make sure the device is running a supported and permitted operating system, as configured in the endpoint posture profile configured in the applicable access rule.

The Zero Trust Access: User Authentication Interval setting in access rules does not apply to mobile devices.

Troubleshoot iOS Devices

Describes Troubleshoot iOS Devices in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To troubleshoot enrolled iOS devices:

- Confirm that the Zero Trust Access relay configuration was added:
  - On the device, go to **Settings** > **VPN & Relays**.
  - In the Per-App Relays section, **Zero Trust** displays.
  - To view information about the Zero Trust relay configuration, click the **(i)** icon.
- Confirm that Zero Trust Access logs are available:
  - In the Zero Trust Access application, go to **Settings**.
  - Choose **Troubleshooting**.
- Confirm that the sync configurations and user unenrollment page displays:
  - In the Zero Trust Access application, click the status frame.

Troubleshoot Samsung Devices Running Android OS

Describes Troubleshoot Samsung Devices Running Android OS in Cisco Secure Access. To send logs from the Android device: From the home screen, tap Settings Send Logs .

- To send logs from the Android device: From the home screen, tap **Settings** > **Send Logs**.
- To enable verbose logging: From the home screen, tap **Settings**, enable verbose logging, and restart the device.
- To sync configurations: From the home screen, tap **You're enrolled** > **Sync now**.
- To unenroll the user: From the home screen, tap **You're enrolled** > **Unenroll**.
- To view ZTA statistics: From the home screen, tap **You're enrolled** and scroll to the **General** section.
- If a Cisco support representative requests certificate information: From the home screen, tap **You're enrolled** and scroll to **Certificate** section

Troubleshoot access issues

Describes Troubleshoot access issues in Cisco Secure Access. If users are unexpectedly blocked or allowed access to resources, see Troubleshoot Private Access Rules.

If users are unexpectedly blocked or allowed access to resources, see Troubleshoot Private Access Rules.

58 Cisco Secure Client on Windows, macOS, and Linux Devices

Topics:

- Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices
- Windows, macOS, and Linux Device Prerequisites
- Download and Install Cisco Secure Client
- Download the OrgInfo.json File
- Manual Installation of Cisco Secure Client (Windows and macOS)
- Mass Deployment Overview
- Mass Deployment (Windows)
- Customize Windows Installation of Cisco Secure Client
- Mass Deployment (macOS)
- Customize macOS Installation of Cisco Secure Client
- Optional OrgInfo.json Parameter Configurations
- VPN Headend Deployment
- Secure Firewall Management Center and Secure Firewall Threat Defense
- Meraki Systems Manager (SM) Deployment
- Migration from Secure Access Roaming Client
- Install the Root Certificate for All Browsers
- Cloud Management
- Additional References
- Manage Device Deployment

Provides an overview of Cisco Secure Client on Windows, macOS, and Linux Devices in Cisco Secure Access, including Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices, Prerequisites, and Download Cisco Secure Client. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices

Describes Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices in Cisco Secure Access. Cisco Secure Client provides security to user devices on any network from any location.

Cisco Secure Client provides security to user devices on any network from any location. User devices can connect to private resources through Zero Trust Access or VPNs, or access internet resources protected by the Cisco Secure Access DNS-layer security and web security. Secure Client manages the endpoint security on user devices in your organization and ensures that Windows, macOS, and Linux devices have a uniform, continuous security experience.

Secure Client manages the endpoint security on user devices in your organization. Secure Client ensures that Windows, macOS, and Linux devices have a uniform, continuous security experience. For more information about Secure Client, see Cisco Secure Client At-a-Glance.

> **Note**
>
> If you are using Cisco Secure Client with Secure Web Gateway (SWG), Cisco recommends disabling the QUIC protocol in your browser settings (for example, Google Chrome, Microsoft Edge, or Firefox) to prevent issues with browser services like search, Gmail, or YouTube. For more information, see Disable QUIC Protocol to Ensure Compatibility with AnyConnect SWG.

Secure Client features include:

- Endpoint compliance
- User identity verification and device communications managed by Zero Trust Access, VPNs, and internet security, including roaming protection
- Threat protection
- Network and identity visibility
- Inspection service

Windows, macOS, and Linux Device Prerequisites

Describes Windows, macOS, and Linux Device Prerequisites in Cisco Secure Access and explains Secure Access Requirements, System Requirements, and Download the Cisco Secure Client Pre-Deployment Package. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Secure Client provides security to user devices on any network, whether the device connects to private resources using Zero Trust Access or VPN, or is securely connected to the internet using DNS-layer security and the secure web gateway (SWG). Deploy Secure Client on your organization's user devices that meet the client's minimum operating system requirements.

Secure Access Requirements

- Full Admin user role. For more information, see Manage Accounts.
- Administrative privileges on the user device.

System Requirements

The Cisco Secure Client supports all vendor-maintained, generally available releases of an operating system unless otherwise noted. For more information on the Cisco Secure Client and supported operating systems, see Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1.

Download the Cisco Secure Client Pre-Deployment Package

Install Cisco Secure Client version 5.1.17 or newer packages for Windows, macOS, and Linux. For more information, see Download the Cisco Secure Client.

Download and Install Cisco Secure Client

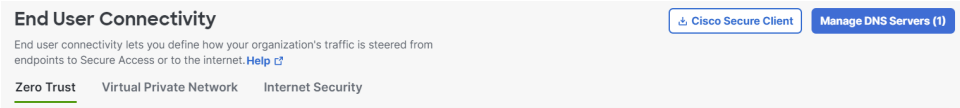
Explains how to obtain the installer and the specific configuration files required to activate the VPN, Zero Trust Access, Internet Security, and ThousandEyes modules in your Secure Access organization.

This section describes how to download and install the Cisco Secure Client on endpoint devices. It also covers downloading the configuration files required to connect the Secure Client VPN module, Zero Trust Access, Internet Security, and ThousandEyes modules to your Secure Access organization.

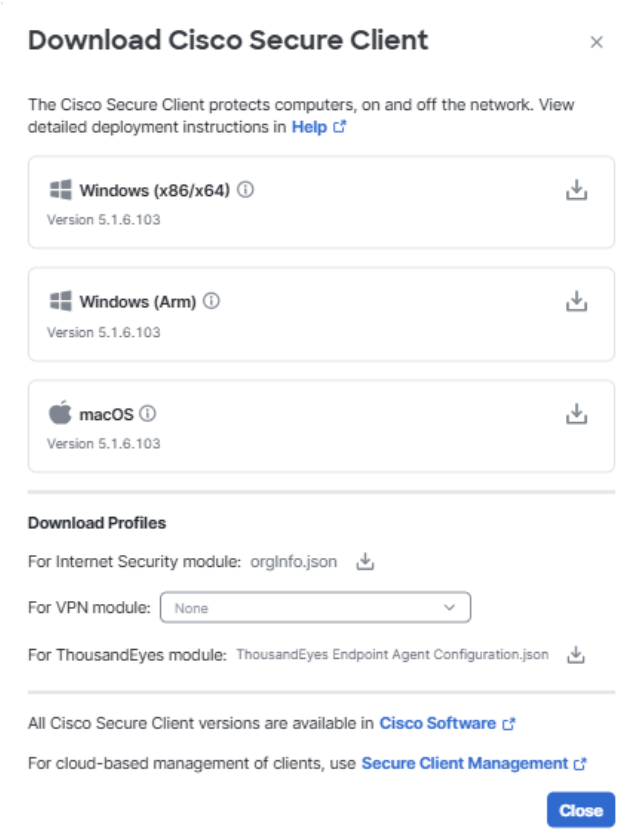
For more information on Cisco Secure Client deployment, see Deploy Cisco Secure Client in the Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. On the End User Connectivity page, click **Cisco Secure Client**.



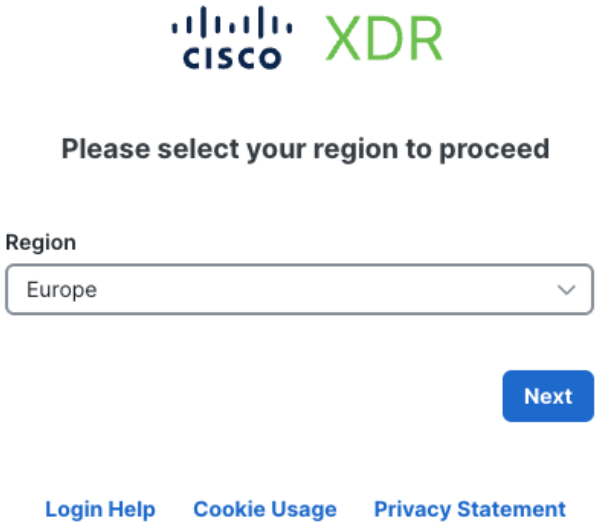
The **Download Cisco Secure Client** window appears.



3. In the **Download Cisco Secure Client** window, choose one of the following options to obtain the installer:
   - Download the latest version of Secure Client from Secure Access: Click the **Download** icon next to your specific operating system. To see version details, hover over the **Information (i)** icon beside the client name.
   - Download the cloud-managed version of Secure Client:To manage your deployment through the cloud, click **Secure Client Management** at the bottom of the Download Cisco Secure Client menu and choose one of the following options:

     Option 1: For Cisco XDR Customers

     - Select your XDR region to obtain the client and manage your clients in the cloud. For more information, see XDR: Client Management.



- If you are not automatically directed to Cisco XDR, launch XDR and click the link below for your region:
  - US: https://registration.us.security.cisco.com/auth-ui.html
  - EU: https://registration.eu.security.cisco.com/auth-ui.html
  - Asia: https://registration.apjc.security.cisco.com/auth-ui.html
- For more information, see the Cisco XDR product page.

Option 2: For Non-XDR Customers

Use **Secure Client Management** to download and manage your clients. This is a free cloud-based application available upon registration. For more information, see About Cisco Secure Client Cloud Management.

- **Existing SecureX Users:** If you used SecureX before the End of Life (EoL) date of July 31, 2024, you should already have access. The **Secure Client Management** link will take you there directly. For more information, see Accessing Secure Client Cloud Management after the SecureX EoL.
- **New Users:** If you did not use SecureX before July 31, 2024, follow the Instructions for Requesting a New Secure Client Cloud Management Tenant.
- **Alternative Access**You can also access the Secure Client Management application through your personalized Cisco Application portal.
  a. In the Cisco Application Portal, click the **Expand** icon for your region.
  b. Navigate to **Secure Client Management**, then click **Launch**.
  c. Once subscribed, you will receive an email with a link to sign in through Security Cloud Sign On. For more information, see the Cisco Security Cloud Sign On Quick Start Guide.

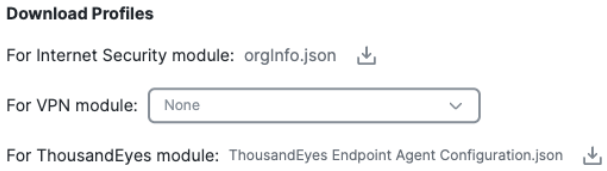
- Download a previous version of Secure Client from Cisco Secure Central: Click the **Cisco Software** link.

> **Note**
>
> You must have a valid service contract associated with your Cisco.com profile to access these files.

In Cisco Secure Central, download the desired Secure Client pre-deployment package and the version for the OS on the end-user device.

- Examples:
  - macOS – `cisco-secure-client-macos-5.1.8.105-predeploy-k9.pkg`
  - Windows – `cisco-secure-client-win-5.1.8.105-predeploy-k9.msi`

4. In the **Download configuration files** section, download the configuration files (also known as profiles) for your deployment:



   a. **VPN Module:** Choose the applicable VPN profiles. The VPN profile tells Secure Access which VPN profiles to enforce. For more information, see Manage VPN Profiles.

   b. **Zero Trust Access:** Expand the drop-down menu and select one of the following enrollment authentication methods you want for your ZTA environment. For in-depth descriptions on what these options see the "Pre and Post Login authentication" section here Pre-login and Post-login Authentication to your Cisco Secure Client on page 1214.
      - **SAML:** Post-login.
      - **Certificate:** Post-login.
      - **SAML:** Pre- login & Post-login (single-user device).
      - **Certificate:** Pre-login & Post-login (single-user device).

   c. **Internet Security module:** Download the `orginfo.json` file. This file configures policies in the Internet Security module (also known as the Umbrella roaming module).

   d. **ThousandEyes module:** Download the `ThousandEyes Endpoint Agent Configuration.json` file.

> **Note**
>
> To register the ThousandEyes module, you must first onboard Experience Insights in Cisco Secure Access. For more information, see Onboard Experience Insights.

5. Install the Cisco Secure Client by running the installer (for example, Setup.exe for Windows) and following the prompts in the installation wizard. For more information, see Deploy Cisco Secure Client in the Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.

ThousandEyes Endpoint Agent Module

Describes ThousandEyes Endpoint Agent Module in Cisco Secure Access. ThousandEyes Endpoint Agent is included as part of Cisco Secure Client.

ThousandEyes Endpoint Agent is included as part of Cisco Secure Client. To learn how to download and manage your endpoint agents with your other Cisco Secure Client Modules, see Cisco Secure Client ThousandEyes Endpoint Agent Module.

Automatic Registration

After completing the Secure Client installation, the ThousandEyes endpoint agent will register the endpoint with your Secure Access organization automatically once the endpoint establishes a connection to VPN, ZTA, or the roaming module. For more information, see Automatic Registration of ThousandEyes Endpoint Agents.

Manual Registration

If an endpoint will not connect via VPN, ZTA, or the roaming module, you can manually register it with Secure Access by running the registration script on the endpoint command line. For more information, see Manual Registration of ThousandEyes Endpoint Agent.

MDM Registration

For an example of how to use an MDM to install Secure Client and register the ThousandEyes endpoint agent, see Deploy Cisco ThousandEyes Module via Microsoft Intune.

Download the OrgInfo.json File

Provides instructions for completing the Download the OrgInfo.json File workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can deploy various modules with the Cisco Secure Client. The Cisco Secure Client may require a certain profile present to install a module successfully.

The Cisco Secure Client Umbrella Roaming Security module (DNS-layer and Web security) requires the Secure Access **OrgInfo.json** file. The Secure Access **OrgInfo.json** file associates a Cisco Secure Client deployment with the Umbrella Roaming Security module to a Secure Access user and organization. Once the module is deployed on the Cisco Secure Client, Secure Access applies the organization's configured policy rules to the device. The device's traffic events are visible in the Activity Search report.

If you use another **OrgInfo.json** file from a different organization in Secure Access to install the Cisco Secure Client Umbrella module, the roaming device is managed by that instance of Secure Access instead.

To deploy the Cisco Secure Client with the Umbrella Roaming Security module on a user device, download the **OrgInfo.json** file from Secure Access to the device.

Download the Cisco Secure Client internet security profile (**OrgInfo.json**).

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Download the OrgInfo.json File:
   a) Navigate to **Connect** > **End User Connectivity** > **Internet Security**.
   b) For Cisco Secure Client, click **Download Profile** to save the **OrgInfo.json** file to the local system.
2. Copy your **OrgInfo.json** file to either the location of the Cisco Secure Client install directory or the `Profiles\\umbrella` directory on the local system.

   When you deploy the **OrgInfo.json** file for the first time, the Cisco Secure Client copies the **OrgInfo.json** file to the data subdirectory (`/umbrella/data`), which also contains several registration files. If you need to deploy a new **OrgInfo.json** file, you must delete the data subdirectory. Alternatively, you can uninstall the Cisco Secure Client Secure Access Roaming Security module, which deletes the data subdirectory, and then reinstall the new **OrgInfo.json** file.

> **Note**
>
> If you deploy the **OrgInfo.json** file on the device after installing the Cisco Secure Client, the Cisco Secure Client Secure Access Roaming Security module directories already exist. If you deploy the **OrgInfo.json** file on the device before installing the Cisco Secure Client, you have to create the required directories for the Secure Access Roaming Security module on the device.

OS	Location	Description	File
Windows	`%ProgramData%\\Cisco\\Cisco Secure Client\\Umbrella`	You must copy the **OrgInfo.json** file that you downloaded from Secure Access to the target directory. Do not rename the file. Alternatively, before installing the Cisco Secure Client, copy the **OrgInfo.json** file to `\\Profiles\\Umbrella`. The Secure Access module installer is located in `\\Profiles\\Umbrella`.	Secure Access module
macOS	/opt/cisco/secureclient/umbrella/		Secure Access module

Manual Installation of Cisco Secure Client (Windows and macOS)

Describes Manual Installation of Cisco Secure Client (Windows and macOS) in Cisco Secure Access. To install Cisco Secure Client, run the Cisco Secure Client installer (.exe or .dmg file) and choose Secure Access from the list of modules.

Install Cisco Secure Client

To install Cisco Secure Client, run the Cisco Secure Client installer (.exe or .dmg file) and choose **Secure Access** from the list of modules.

> **Note**
>
> - If you choose only the **Secure Access** option, the VPN functionality in Cisco Secure Client will be disabled. However, the core VPN service will still be installed, as Secure Access shares some underlying functionality with this service.
> - Unchecking the **Core & AnyConnect VPN** option will hide the VPN from the graphical user interface (GUI). The VPN service (csc_vpnagent) will continue to run in the background, but it will not be visible in the GUI.
> - We highly recommend that you select **Diagnostics and Reporting Tool** for troubleshooting capabilities.

Install Secure Access Profile

After installing Cisco Secure Client, install the Secure Access profile (OrgInfo.json), downloaded from your dashboard. Copy the profile to the correct folder to register and activate Secure Access:

Windows	`ProgramData\\Cisco\\Cisco Secure Client\\Secure Access\\OrgInfo.json`
macOS	`/opt/cisco/secureclient/secureaccess/OrgInfo.json`

> **Note**
>
> If the profile is not installed in the correct location, the Cisco Secure Client will display a `"Profile is missing"` error message.

Mass Deployment Overview

Describes Mass Deployment Overview in Cisco Secure Access. Cisco Secure Client can be deployed with endpoint management software designed to remotely install applications.

Remote Installation

Cisco Secure Client can be deployed with endpoint management software designed to remotely install applications. This includes tools such as Unified Endpoint Management (UEM) and Remote Management and Monitoring (RMM).

The remote installation options outlined below includes installing both the Cisco Secure Client software and the Umbrella profile (OrgInfo.json), similar to the steps followed in the manual deployment process.

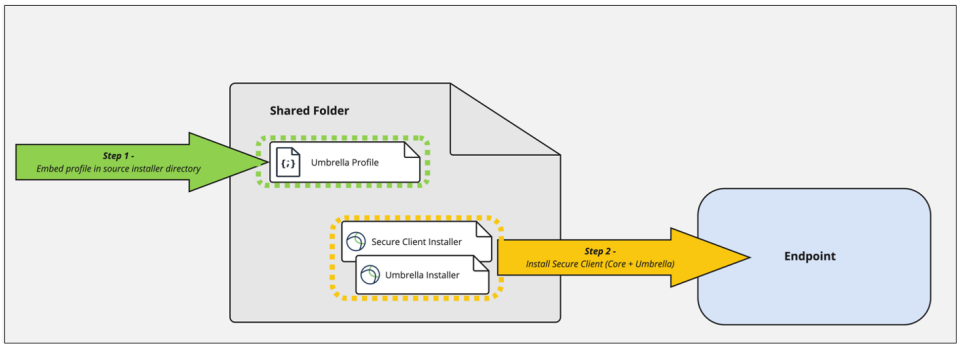
Scripted Installation	• Cisco Secure Client is installed by endpoint management software. • The Umbrella profile information is copied to the endpoint by a `post install` script or task.
Mass Deployment Package	• The installation package or source is modified, and the Umbrella configuration profile is bundled with this package or source prior to installation. • The customized package can be installed by endpoint management software with the profile that is already included.

VPN Headend Deployment	(This option is suitable for customers using Secure Client for VPN.) • The software and profile are uploaded to the VPN headend. • Umbrella is automatically downloaded and installed when the corresponding user connects to the VPN.
RMM Deployment	(This option is suitable for managed service providers.) Cisco Secure Client can be deployed to multiple end customers using RMM tools.

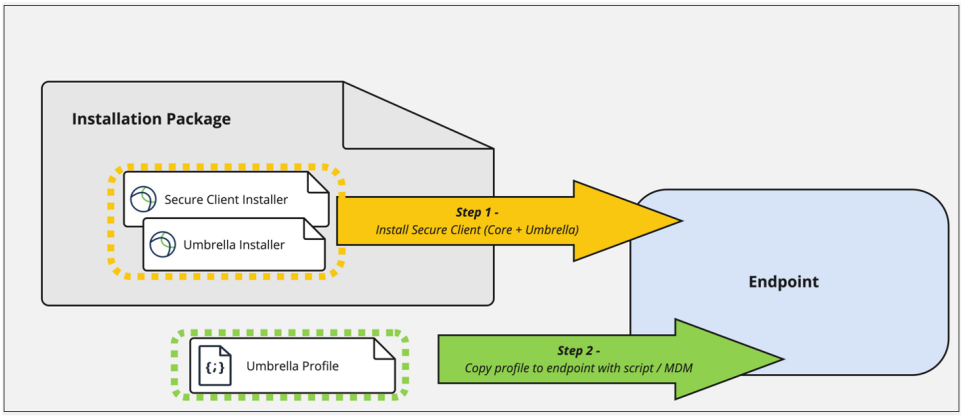
Profile Installation

Installing your Umbrella organization profile (OrgInfo.json) is a mandatory step in the deployment process because this file uniquely identifies your Umbrella organization and is required for the Cisco Secure Client to register with Umbrella. The following diagrams show the two main ways in which the Umbrella organization profile can be distributed.

- **Bundle Profile**:The profile (OrgInfo.json) is bundled with the installation package prior to installation.



- **Copy Profile** : The profile (OrgInfo.json) is copied to a location in the endpoint (programmatically) after installation. (MDM - Managed Device Manager).



Customization Options

Describes Customization Options in Cisco Secure Access. Before performing a mass deployment of Cisco Secure Client, you may consider the following common installation customizations.

Before performing a mass deployment of Cisco Secure Client, you may consider the following common installation customizations.

1. **Select Cisco Secure Client Modules**

Choose which Cisco Secure Client modules you want to install. For a minimum installation (Umbrella protection only) you must install two modules:

- Core & AnyConnect VPN module
- Umbrella module

Choose the modules using the following methods.

Windows	Using a 'Pre-Deployment' package, the modules are provided as individual Microsoft Software Installer (MSIs). Only install the desired .msi files. A minimum of two .msi files must be installed (Core VPN + Umbrella module)
macOS	Using a 'Pre-Deployment' package Cisco Secure Client (and its modules) are installed using a single .dmg image. An 'install_choices.xml' file can be provided to the macOS installer to disable unwanted modules. Alternatively, use a 'Web Deployment' package, install each Cisco Secure Client module using a separate .dmg image. A minimum of two .dmg image files must be installed (Core VPN + Umbrella module)

2. **Disable VPN Functionality**

   The Core Secure Client VPN module must be installed for the Umbrella module to function. However, the VPN functionality itself is not required and can be disabled (for macOS and Windows) such that it is not available to users. Each of the installation methods on this page provide options for disabling Cisco Secure Client VPN.

   You can disable the VPN functionality using one of these methods:

   - During manual installation uncheck the Core & AnyConnect VPN (for Windows and macOS).
   - Disable the VPN functionality within a customized .dmg package (macOS).
   - Disable the VPN functionality by deploying a special VPN profile (Windows and macOS).

   For more information, see Disable the VPN Module in Secure Client.

3. **Lockdown Services (Windows)**

   On Windows, you can customize the installation to prevent users from tampering with Cisco Secure Client. To do this, modify any of the **msiexec** commands and provide these additional MSI parameters:

   - **LOCKDOWN=1** : Prevents the service from being stopped.
   - **ARPSYSTEMCOMPONENT=1** : Hides the program from **Programs and Features** in Windows.

   For more information, see Understand Command Line Installation and RMM Reference for Umbrella Module.

Mass Deployment (Windows)

Describes Mass Deployment (Windows) in Cisco Secure Access. You have the option to bundle the Umbrella profile within the installation source directory before running the Cisco Secure Client installer.

(Optional) Package Customization

You have the option to bundle the Umbrella profile within the installation source directory before running the Cisco Secure Client installer. The profile will then be automatically imported during installation.

This method creates a preconfigured deployment package, which can be executed without any additional script or configuration. However, note that for this method to work, one of the following is required:

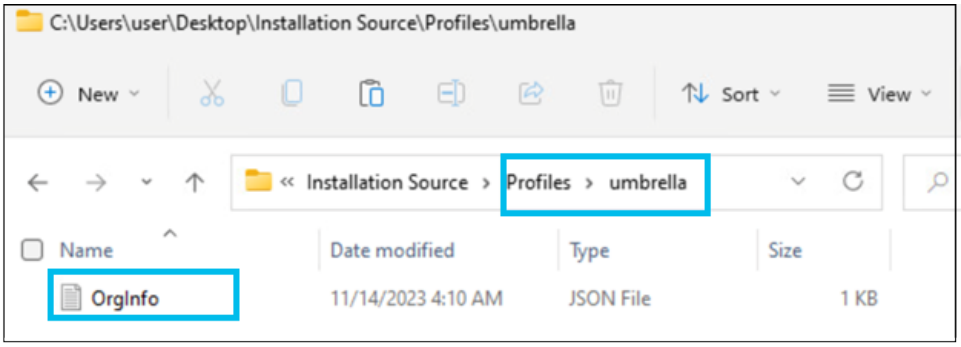
- A shared network folder to act as the installation source.
- Endpoint management software that can create and distribute multifile installation packages.

> **Note**
>
> See the following examples of software that can distribute multifile installation packages using the Windows Content Prep Tool or Jamf Composer:
>
> - Secure Client Umbrella Roaming Security Module Provisioning via MS Intune (Windows)
> - How to deploy Cisco Secure Client via JAMF (MacOS)
>
> For more information, see Customize Windows Installations of Secure Client.

Add Umbrella Profile

Add the `OrgInfo.json` file to a `\\Profiles\\umbrella` subdirectory within the installation package. The source installation folder must have the following contents:

```
cisco-secure-client-win-X.X.XXXXX-core-vpn-predeploy-k9.msi
cisco-secure-client-win-X.X.XXXXX-umbrella-predeploy-k9.msi
\\Profiles\\umbrella\\OrgInfo.json
```



For more information, see Automated deployment tutorial with bundled Umbrella profile.

Automated Installation (Windows)

Cisco Secure Client can be installed using an unattended process that uses a script and follows the same workflow as the manual installation process.

Install Cisco Secure Client

Use the following `msiexec` commands to install the required modules (Core + Umbrella):

```
msiexec /i "cisco-secure-client-win-5.X.XXXX-core-vpn-predeploy-k9.msi" /passive
 PRE_DEPLOY_DISABLE_VPN=1 /lvx_ vpninstall.log
msiexec /i "cisco-secure-client-win-5.X.XXXX-umbrella-predeploy-k9.msi" /passive
 PRE_DEPLOY_DISABLE_VPN=1 /lvx_ umbrellainstall.log
```

For more information, see Understand Command Line Installation and RMM Reference for Umbrella Module .

> **Note**
>
> The PRE_DEPLOY_DISABLE_VPN=1 parameter disables the VPN functionality for customers not using Cisco Secure Client for VPN access. Note, however, that the Core VPN module must be installed.

Install the Umbrella Profile

This step is necessary unless the profile is already bundled within the installation package (see Package Customization). After installation, copy the Umbrella profile (downloaded from your Umbrella dashboard) to the correct folder in the local device to register and activate Umbrella. This can be done with a task or `post install` script.

Copy the Umbrella profile to the following location:

`%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`

Instead of copying the Umbrella profile, you can create it with a script if your management software supports `post-installation` scripts.

The following example shows how to create an Umbrella profile using PowerShell. Replace ORG_ID, FINGERPRINT, and USER_ID values with the ones from your profile (OrgInfo.json) file:

```
$org_file = "%PROGRAMDATA%\\Cisco\\Cisco Secure Client\\Umbrella\\OrgInfo.json"

$data=@"
{
    "organizationId" : "ORG_ID",
    "fingerprint" : "FINGERPRINT",
    "userId" : "USER_ID"
}
"@

if(-not(Test-Path -Path $org_file))
{
 $data > $org_file
}
```

(Optional) Disable VPN Functionality (Post installation)

If the VPN functionality was not disabled during installation, it can optionally be disabled with a post-installation task or script. You can disable the Secure Client VPN functionality after installation by creating a special profile, `VPNDisable_ServiceProfile.xml`.

`%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile\`**`VPNDisable_ServiceProfile.xml`**

Instead of copying the VPN profile, it can also be created with a script. This is useful if your endpoint management software supports `post install` scripts. The following example shows how to create the `VPNDisable_ServiceProfile.xml` using bash script.

```
$profile_file = "%PROGRAMDATA%\\Cisco\\Cisco Secure Client\\VPN\\Profile\\
VPNDisable_ServiceProfile.xml "
$data=@"
{
?\<xml version="1.0" encoding="utf-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">

  <ClientInitialization>
```

```
    <ServiceDisable>true</ServiceDisable>
  </ClientInitialization>
</AnyConnectProfile>
}
"@

if(-not(Test-Path -Path $profile_file))
{
 $data > $profile_file
}
```

For more information, see Disable the VPN Module in Secure Client.

Customize Windows Installation of Cisco Secure Client

Describes Customize Windows Installation of Cisco Secure Client in Cisco Secure Access. You can customize the installation of the Cisco Secure Client with various modules and features on Windows.

You can customize the installation of the Cisco Secure Client with various modules and features on Windows. The Cisco Secure Client deployment packages support several MSI properties that you can change during installation, including lockdown and disabling the display of the VPN module in the client's GUI.

You can deploy the Cisco Secure Client for Windows using several options including:

- Hide the VPN module in the Cisco Secure Client GUI.
- Hide the Secure Client installation from the Add/Remove Windows programs list.
- Enable Lockdown mode to prevent users from stopping or disabling Secure Client services, for more information , see Configure AnyConnect Lockdown For Windows.

Deploy the Cisco Secure Client VPN Module

Run the Windows installer to deploy the Cisco Secure Client VPN package with the `PRE_DEPLOY_DISABLE_VPN=1` option. This option hides the VPN module Secure Client 's GUI, but is not disabled. Set the MSI property to `PRE_DEPLOY_DISABLE_VPN=1`.

> **Note**
>
> If the VPN module is hidden in the client's GUI, you can manage the VPN module through the Cisco Secure Client's CLI.

The following command disables the VPN functionality by copying the `VPNDisable_ServiceProfile.xml` file embedded in the MSI to the directory specified to the endpoints VPN profiles directory.

Example:

```
msiexec /package cisco-secure-client-win-<version>-core-vpn-predeploy-k9.msi
/norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* c:\\output.log
```

Deploy the Cisco Secure Client Umbrella Roaming Security Module

1. Run the Windows installer to deploy the Cisco Secure Client Umbrella Roaming Security package.

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
 /norestart /passive /lvx* c:\\output.log
```

2. To enable lockdown, add `LOCKDOWN=1` in the CLI.

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
 /passive LOCKDOWN=1 /lvx* c:\\output.log
```

(Optional) Deploy Cisco Secure Client DART

Run the Windows installer to deploy the Secure Client DART package.

```
msiexec /package cisco-secure-client-win-<version>-dart-predeploy-k9.msi
/norestart /passive /lvx* c:\\dart.log
```

Hide Cisco Secure Client Modules from Add/Remove Programs List

You can hide the installed Cisco Secure Client modules from users who have permission to view the Windows Add/Remove Programs list.

Run the Windows installer for the Cisco Secure Client package using `ARPSYSTEMCOMPONENT=1`. You can apply this option to all the modules at the time of deployment.

Example:

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi
/passive ARPSYSTEMCOMPONENT=1 /lvx* c:\\output.log
```

(Optional) OrgInfo.json Parameter Configurations

Describes (Optional) OrgInfo.json Parameter Configurations in Cisco Secure Access. When deploying the Umbrella Roaming Security module in Cisco Secure Client on Windows, you have the flexibility to add and configure various parameters directly within the Umbrella OrgInfo.json file.

When deploying the Umbrella Roaming Security module in Cisco Secure Client on Windows, you have the flexibility to add and configure various parameters directly within the Umbrella OrgInfo.json file. Unlike the LOCKDOWN parameter, these settings are applied directly to the OrgInfo.json profile rather than during the installation process using an **msiexec** parameter. The following information is not applicable if executed at the time of installation.

Starting with Cisco Secure Client version 5.1.13.177 (MR13) or later versions, a new parameter, `deviceKeyType`, can be added to the orginfo.json file to enable device registration using the serial number instead of the hostname. This enhancement provides IT administrators with more accurate and reliable data, benefiting asset management, CMDB integration, and compliance reporting.

To enable registration with the serial number, the orginfo.json file must be modified by adding a key/value pair for deviceKeyType prior to the registration of a roaming security module.

Parameter	Values	Description
noAutoSuffix	`0` - Adds the domains (default) `1` - Does not add domains	Does not add the domains present in the DNS suffix settings in network adapters and networking properties to the Internal Domains list. This exists to enable the Umbrella roaming module to recognize local resources and domains on foreign networks.
customUSResolvers	`\["208.67.221.76", "208.67.223.76"\]` - Sets primary and secondary US-based AnyCast addresses	Enables special DNS resolver AnyCast addresses that limit DNS queries to only U.S.-based Umbrella servers. Does not affect block pages or proxy.

Parameter	Values	Description
noNXDOMAIN	`0` - Performs requery (default) `1` - Does not perform requery	Automatically requerie public NXDOMAINS at the local resolvers. This parameter allows roaming users to resolve internal domains in networks beyond their own without interruption or internal domains list management. **Note** DNS search suffixes are automatically sent to local resolvers, unless this parameter is disabled.
deviceKeyType	`"serialnumber"`	Enables device registration via serial number instead of hostname. If the serial number is not found on the device, the hostname is used as a fallback. This parameter should only be used with new device registrations. Using this parameter for existing devices could cause registration conflicts or disrupt their current configuration. **Note** This parameter applies to Cisco Secure Client version 5.1.13.177 (MR13) or later versions.

Note

Modify the correct Orginfo.json file with the following `%ProgramData%\\Cisco\\CiscoSecureClient\\Umbrella` path.

Mass Deployment (macOS)

Describes Mass Deployment (macOS) in Cisco Secure Access. We recommend that on macOS platform, you customize the installation package before performing a mass deployment.

(Optional) Package Customization

We recommend that on macOS platform, you customize the installation package before performing a mass deployment. For detailed instructions see Customize the macOS installation of Cisco Secure Client.

You can customize the macOS installer image (.dmg file) to embed the Umbrella profile (OrgInfo.json) within it before deployment. The profile will then be automatically imported during installation. The package can also include customizations to (optionally) disable the Secure Client VPN functionality.

You can use this customization to create a preconfigured deployment package that can be executed without additional scripts. For detailed instructions see Customize the macOS installation of Cisco Secure Client.

Add Umbrella Profile

Use the macOS `hdiutil` command to create and mount a writable version of the .dmg image.

```
hdiutil convert cisco-secure-client-macos-<version>-predeploy-k9.dmg -format
UDRW -o csc-writeable.dmg
hdiutil attach csc-writeable.dmg
```

You can then add the Umbrella profile (OrgInfo.json) to the package in the following location:

```
/Volumes/Cisco\ Secure\ Client\ <version>/Profiles/Umbrella/OrgInfo.json
```

(Optional) Disable VPN Functionality

You can edit the following file (within the mounted DMG image) to disable the VPN functionality. `/Volumes/Cisco\ Secure\ Client\ <version>/Profiles/ACTransforms.xml`

Add the following configuration to ACTransforms.xml:

```
<Transforms>
<DisableVPN>true</DisableVPN>
<DisableCustomerExperienceFeedback>true</DisableCustomerExperienceFeedback>
</Transforms>
```

Save the .dmg image

Eject the mounted disk image and convert it back to a read-only format.

```
diskutil eject /Volumes/Cisco\\ Secure\\ Client\\ <version>
hdiutil convert csc-writeable.dmg -format UDRO -o csc-readable.dmg
```

The resulting file (csc-readable.dmg) can be distributed to users for manual installation or used as part of the Automated Installation process.

Automated Installation (macOS)

You can install Cisco Secure Client using a scripted, unattended process that follows the same workflow as the standard manual installation.

Installation (Pre-Deployment Package)

Cisco Secure Client (and its modules) are provided as a single 'pre-deployment' .dmg package. You must provide the attached `install_choices.xml` file to customize the installation so that only the necessary modules are installed. The attached `install_choices.xml` is preconfigured to install the minimum modules (Core VPN + Umbrella).

This installation method is possible only if you are performing a scripted installation or if your endpoint management tool supports the **-applyChoiceChangesXML** parameter.

Example:

```
hdiutil attach
~/Downloads/cisco-secure-client-macos-X.X.XXXX-core-vpn-predeploy-k9.dmg
```

```
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\<version>/Cisco\\ Secure\\
 Client.pkg -applyChoiceChangesXML ~/Downloads/install_choices.xml -target /
```

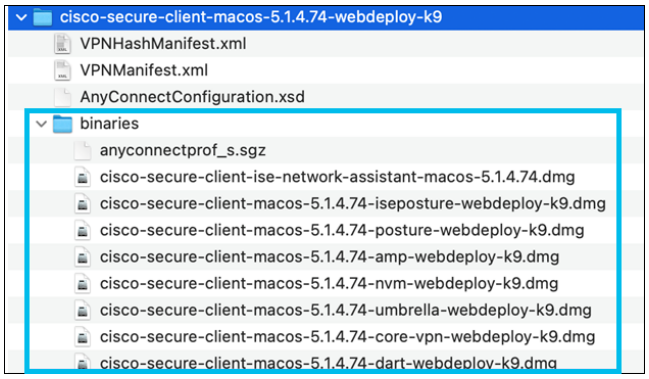
Note

The 'install_choices.xml' file is used to install the Core Secure Client and Umbrella modules. Additionally, it can be edited to include the installation of other Secure Client modules as well.

Installation (Web Deployment Package)

Cisco also provides a web deployment package that contains each Cisco Secure Client module as individual .dmg files. This alternative is only recommended if your endpoint management tool can't supply the required **-applyChoiceChangesXML** parameter to select the corresponding modules.

Download the alternative headend (webdeploy) package (.pkg) and extract it with the macOS archive utility. Locate the relevant .dmg files in the binaries/ directory of the extracted package.



Both the Core VPN module and the Umbrella module must be installed separately as shown in the following examples:

```
hdiutil attach cisco-secure-client-macos-X.X.XXXX-core-vpn-webdeploy-k9.dmg
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\\ -\\ AnyConnect\\ VPN\\
 X.X.X.XX/ -target /

hdiutil attach cisco-secure-client-macos-X.X.XXXX-umbrella-webdeploy-k9.dmg
sudo installer -pkg /Volumes/Cisco\\ Secure\\ Client\\ -\\ Umbrella\\ X.X.X.XX/
 -target /
```

Install Umbrella Profile

This is necessary unless the profile is already bundled with the installation package, see Package Customization.

After installation, copy the Umbrella profile to the correct folder on the local machine to register and activate the Umbrella module. This method is useful for endpoint management software that can push the files to the endpoint. The profile must be placed in the following location:

`/opt/cisco/secureclient/umbrella/OrgInfo.json`

Instead of copying the umbrella profile, you can create it with a script. This is useful if your endpoint management tools support `post-install` scripts.

The following example shows how to create the OrgInfo.json file using a bash script. Replace ORG_ID, FINGERPRINT, and USER_ID values with the ones from your profile.

```
# !/bin/bash

orginfo_file="/opt/cisco/secureclient/umbrella/OrgInfo.json"
data="{\\n
    "organizationId" : "ORG_ID",\\n
    "fingerprint" : "FINGERPRINT",\\n
    "userId" : "USER_ID"\\n
}"
if ! test -f $orginfo_file; then
 echo -e $data > $orginfo_file
fi
```

Note

The Meraki Systems Manager (SM) Deployment guide explains how to deploy the Umbrella profile using scripts.

(Optional) Disable VPN Functionality (Post-Installation)

If the VPN functionality is not disabled during installation, it can be (optionally) disabled with a post-installation task or script. The Secure Client VPN functionality can be disabled after installation by creating a special profile, `VPNDisable_ServiceProfile.xml`. Place the profile in the following directory:

`/opt/cisco/secureclient/vpn/profile/VPNDisable_ServiceProfile.xml`

Instead of copying the umbrella profile, you can create it with a script. This is useful for management software that supports `post-install` script. The following example shows how to create the `VPNDisable_ServiceProfile.xml` using a bash script.

```
# !/bin/bash

profile_file="/opt/cisco/secureclient/vpn/profile/VPNDisable_ServiceProfile.xml"

data="<?xml version="1.0" encoding="utf-8"?>\\n
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">\\n
  <ClientInitialization>\\n
    <ServiceDisable>true</ServiceDisable>\\n
  </ClientInitialization>\\n
</AnyConnectProfile>\\n"

if ! test -f $profile_file; then
 echo -e $data > $profile_file
fi
```

For more information, see Disable the VPN Module in Secure Client.

Allow Secure Client System Extensions

By default, macOS requires users to accept the activation of a new system extension. As a result, users are presented with a dialog box when they first install Cisco Secure Client. Users must follow the prompts to allow the Cisco Secure Client - Socket Filter' extension.

Alternatively, the system extension can be approved centrally by the administrator using endpoint management, or device management suites if the device is managed by UEM tools. For more information, see the advice in Approving the Cisco Secure Client System Extension.

Customize macOS Installation of Cisco Secure Client

Describes Customize macOS Installation of Cisco Secure Client in Cisco Secure Access. Managed Device Manager systems can customize the installation of the Cisco Secure Client with various modules on macOS.

Managed Device Manager systems can customize the installation of the Cisco Secure Client with various modules on macOS. Cisco Secure Client offers the flexibility to install with preconfigured Umbrella profiles and to hide modules if needed. To select the modules for installation, modify the Cisco Secure Client .dmg file accordingly.

By default, the Cisco Secure Client is deployed with the VPN module. To deploy the Cisco Secure Client with the Umbrella Roaming Security module via CLI or MDM, an XML configuration is required. Use a transform file **(ACTransforms.xml)** to deploy the Cisco Secure Client without VPN capabilities.

Procedure

Choose the modules to install with the Cisco Secure Client on a macOS device.

Step 1 – Make the .dmg Package Writeable

Provides instructions for completing the Step 1 – Make the .dmg Package Writeable workflow in Cisco Secure Access. Open a Terminal and set the .dmg file to Read/Write.

Use disk utility or **hdiutil** to change the permissions in the .dmg package from Read Only to Read/Write.

Procedure

Open a **Terminal** and set the .dmg file to Read/Write. Make sure you are in the Downloads folder when running the following command:

```
hdiutil convert cisco-secure-client-macos-<version>-predeploy-k9.dmg -format
UDRW -o csc-writeable.dmg
hdiutil attach csc-writeable.dmg
```

Here, *<version>* refers to the current version number of Cisco Secure Client.

Step 2 – Generate the Module Installation Configuration File

Provides instructions for completing the Step 2 – Generate the Module Installation Configuration File workflow in Cisco Secure Access. Open a terminal and launch the .dmg file from /Volumes.

Generate the Cisco Secure Client module configuration file. The configuration file defines the modules to be included with the installation of Secure Client.

Procedure

1. Open a **terminal** and launch the .dmg file from `/Volumes`.

   ```
   open /Volumes/Cisco\ Secure\ Client\ <version>
   ```

   Here, *<version>* refers to the current version number of Cisco Secure Client.

2. Run **installer** which provides `pkg` option with the name of the Cisco Secure Client package and the `showChoiceChangesXML` option. Redirect the output to `install_choices.xml` to generate the installation configuration file.

```
installer -pkg /volumes/Cisco\ Secure\ Client\ <version>/Cisco\ Secure\
Client.pkg -showChoiceChangesXML > ~/Downloads/install_choices.xml
```

   Here, *<version>* refers to the current version number of Cisco Secure Client.

Step 3 – Copy OrgInfo.json to Cisco Secure Client Installation Directory

Provides instructions for completing the Step 3 - Copy OrgInfo.json to Cisco Secure Client Installation Directory workflow in Cisco Secure Access. Open a terminal and launch the .dmg from /Volumes/Profiles.

Procedure

1. Open a **terminal** and launch the .dmg from `/Volumes/Profiles`.

```
cd /Volumes/Cisco\ Secure\ Client\ <version>/Profiles/Umbrella/
```

   Here, *<version>* refers to the current version number of Cisco Secure Client.

2. Drag and drop the `OrgInfo.json` file that you downloaded from Secure Access to `Volumes/Profiles`.

Step 4 – (Optional) Hide the VPN Module

Provides instructions for completing the Step 4 - (Optional) Hide the VPN Module workflow in Cisco Secure Access. Open a terminal and launch the ACTransforms.xml file from /Volumes.

To hide the Secure Client VPN module in the client GUI, modify **ACTransforms.xml**.

Procedure

1. Open a **terminal** and launch the `ACTransforms.xml` file from `/Volumes`.

```
open -e /Volumes/Cisco\ Secure\ Client\ <version>/Profiles/ACTransforms.xml
```

2. Remove the XML comments around the `Transforms` element, and then save `ACTransforms.xml`.

```
<Transforms>
<DisableVPN>true</DisableVPN>
<DisableCustomerExperienceFeedback>true</DisableCustomerExperienceFeedback>
</Transforms>
```

Step 5 – Customize the Cisco Secure Client Installation Modules

Provides instructions for completing the Step 5 - Customize the Cisco Secure Client Installation Modules workflow in Cisco Secure Access. To skip a module, define the module with 0.

Edit `install_choices.xml` created in Step 2 - Generate the Module Installation Configuration File. You can either skip or install the Secure Client modules defined in the configuration file.

Procedure

1. To skip a module, define the module with `0`.
2. To install a module, define the module with `1`.

What to do next

Note: Modifying `choice_vpn` does not supersede the changes that you made to **`ACTransforms.xml`**. The VPN module is required, even if the module is not displayed in the client GUI.

1. Open a **terminal** and launch `install_choices.xml`.
2. Define an integer XML element for each module and assign to `0` or `1`, and then save `install_choices.xml`.

```
cd /Volumes
open -e ~/Downloads/install_choices.xml
```

Sample Customization

Describes Sample Customization in Cisco Secure Access. In the following example, the Core VPN, Umbrella, and DART modules are set to 1 and are included in the Secure Client installation.

In the following example, the Core VPN, Umbrella, and DART modules are set to `1` and are included in the Secure Client installation.

> **Note**
>
> The modules listed are subject to change. Follow Step 1 and Step 5 to extract your XML file from the target version .pkg and modify it to install the crossponding modules, such as Core VPN, Umbrella, and DART.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
 <dict>
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>visible</string>
  <key>choiceIdentifier</key>
  <string>choice_anyconnect_vpn</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <false/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_anyconnect_vpn</string>
```

```
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>1</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_anyconnect_vpn</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_fireamp</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_fireamp</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_fireamp</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>1</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_dart</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
```

```
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_firewall_posture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_iseposture</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
```

```
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_nvm</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>1</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_secure_umbrella</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <true/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_thousandeyes</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>enabled</string>
 <key>choiceIdentifier</key>
 <string>choice_thousandeyes</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <integer>0</integer>
 <key>choiceAttribute</key>
 <string>selected</string>
 <key>choiceIdentifier</key>
 <string>choice_thousandeyes</string>
</dict>
<dict>
 <key>attributeSetting</key>
 <false/>
 <key>choiceAttribute</key>
 <string>visible</string>
 <key>choiceIdentifier</key>
 <string>choice_duo</string>
</dict>
<dict>
```

```
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_duo</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <integer>0</integer>
  <key>choiceAttribute</key>
  <string>selected</string>
  <key>choiceIdentifier</key>
  <string>choice_duo</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <true/>
  <key>choiceAttribute</key>
  <string>visible</string>
  <key>choiceIdentifier</key>
  <string>choice_zta</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <false/>
  <key>choiceAttribute</key>
  <string>enabled</string>
  <key>choiceIdentifier</key>
  <string>choice_zta</string>
 </dict>
 <dict>
  <key>attributeSetting</key>
  <integer>0</integer>
  <key>choiceAttribute</key>
  <string>selected</string>
  <key>choiceIdentifier</key>
  <string>choice_zta</string>
 </dict>
</array>
</plist>
```

Step 6 – Set Up the Correct Extension Permission Settings

Provides instructions for completing the Step 6 - Set Up the Correct Extension Permission Settings workflow in Cisco Secure Access. By default, macOS requires users to accept the activation of a new system extension.

Procedure

1. By default, macOS requires users to accept the activation of a new system extension. As a result, users are presented with a dialog box. The Managed Device Manager is required to approve the Cisco Secure Client system extension and disable the dialog box using a management profile's system extensions paylo ad. For more information about this, see System Extensions.
2. Follow the payload guidance provided in Extension Approval using MDM to deploy the system extension settings.

Step 7 – Install Secure Client with Selected Modules

Provides instructions for completing the Step 7 - Install Secure Client with Selected Modules workflow in Cisco Secure Access. Open a terminal and mount the .dmg from /Volumes.

Install Secure Client with the configured modules.

Procedure

1. Open a **terminal** and mount the .dmg from `/Volumes`.

```
cd ~/Downloads
diskutil eject Cisco\ Secure\ Client\ <version>
hdiutil convert csc-writeable.dmg -format UDRO -o csc-readable.dmg
```

   Here, *<version>* refers to the current version number of Cisco Secure Client.

2. Run the **installer** which provides the `pkg` option along with the name of the Cisco Secure Client package and the`applyChoiceChangesXML` option with `install_choices.xml`. Make sure you are still in the `/Volumes` directory when running this command.

```
hdiutil attach ~/Downloads/csc-readable.dmg
sudo installer -pkg Cisco\ Secure\ Client\ <version>/Cisco\ Secure\ Client.pkg
 -applyChoiceChangesXML ~/Downloads/install_choices.xml -target /
```

   Here, *<version>* refers to the current version number of Cisco Secure Client.

Optional OrgInfo.json Parameter Configurations

Describes Optional OrgInfo.json Parameter Configurations in Cisco Secure Access. When deploying the Umbrella Roaming Security module in Cisco Secure Client, on macOS you have the flexibility to add and configure various parameters directly within the Umbrella OrgInfo.json file.

When deploying the Umbrella Roaming Security module in Cisco Secure Client, on macOS you have the flexibility to add and configure various parameters directly within the Umbrella OrgInfo.json file. Unlike the LOCKDOWN parameter, these settings are applied directly to the OrgInfo.json profile rather than during the installation process using an **msiexec** parameter. The following information is not applicable if executed at the time of installation.

Starting with Cisco Secure Client version 5.1.13.177 (MR13) or later versions, a new parameter, `deviceKeyType`, can be added to the orginfo.json file to enable device registration using the serial number instead of the hostname. This enhancement provides IT administrators with more accurate and reliable data, benefiting asset management, CMDB integration, and compliance reporting.

To enable registration with the serial number, the orginfo.json file must be modified by adding a key/value pair for deviceKeyType prior to the registration of a roaming security module.

Parameter	Values	Description
noAutoSuffix	`0` - Adds the domains (default) `1` - Does not add domains	Does not add the domains present in the DNS suffix settings in network adapters and networking properties to the Internal Domains list. This exists to enable the Umbrella roaming module to recognize local resources and domains on foreign networks.

Parameter	Values	Description
customUSResolvers	`\["208.67.221.76", "208.67.223.76"\]` - Sets primary and secondary US-based AnyCast addresses	Enables special DNS resolver AnyCast addresses that limit DNS queries to only U.S.-based Umbrella servers. Does not affect block pages or proxy.
noNXDOMAIN	`0` - Performs requery (default) `1` - Does not perform requery	Automatically requerie public NXDOMAINS at the local resolvers. This parameter allows roaming users to resolve internal domains in networks beyond their own without interruption or internal domains list management. **Note** DNS search suffixes are automatically sent to local resolvers, unless this parameter is disabled.
deviceKeyType	`"serialnumber"`	Enables device registration via serial number instead of hostname. If the serial number is not found on the device, the hostname is used as a fallback. This parameter should only be used with new device registrations. Using this parameter for existing devices could cause registration conflicts or disrupt their current configuration. **Note** This parameter applies to Cisco Secure Client version 5.1.13.177 (MR13) or later versions.

Note

Modify the correct Orginfo.json file with the following `/Library/Application Support/Cisco/Cisco Secure Client/Umbrella/datapath/`path on macOS.

VPN Headend Deployment

Describes VPN Headend Deployment in Cisco Secure Access. Customers utilizing the Secure Client VPN functionality can deploy the Umbrella module directly from their VPN headend, a method known as web deployment.

Customers utilizing the Secure Client VPN functionality can deploy the Umbrella module directly from their VPN headend, a method known as web deployment. This configuration is performed on the VPN server.

- Clients with existing AnyConnect Secure Client deployments can automatically download the Umbrella module and profile when they initiate a connection to the VPN.
- Cisco Secure Client can also be installed through a self-service workflow, where each user visits the HTTP web portal hosted on the VPN headend.
- This web deployment method allow you to update Cisco Secure Client and the Umbrella module software versions by centrally uploading new versions to the VPN server.

For more information, seeWeb Deployment of Cisco Secure Client.

Secure Firewall Management Center and Secure Firewall Threat Defense

Describes Secure Firewall Management Center and Secure Firewall Threat Defense in Cisco Secure Access. This configuration guide covers the steps to provision the Umbrella Module in the Secure Firewall Management Center for version 6.5 or later.

This configuration guide covers the steps to provision the Umbrella Module in the Secure Firewall Management Center for version 6.5 or later. The provisioned module is applied to Secure Firewall Threat Defense managed by the management center.

Prerequisites to provision the Umbrella Module

- Access to the Cisco Umbrella Dashboard.
- Access to management center or threat defense, as this version adds support for additional AnyConnect modules. For versions earlier than 6.7, FlexConfig can be used to deploy the module, you can refer to the Cisco documentation for details.
- Umbrella Module Profile (orginfo.json).
- AnyConnect VPN module configuration is already complete and functional on the management center or threat defense.

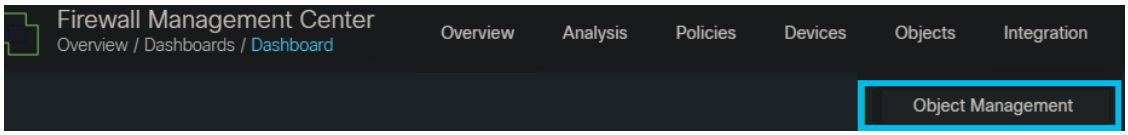
Procedure to enable Secure Client Secure Access Module in Management Center and Threat Defense

Provides instructions for completing the Procedure to enable Secure Client Secure Access Module in Management Center and Threat Defense workflow in Cisco Secure Access. In the management center dashboard, go to Object Objects Management .

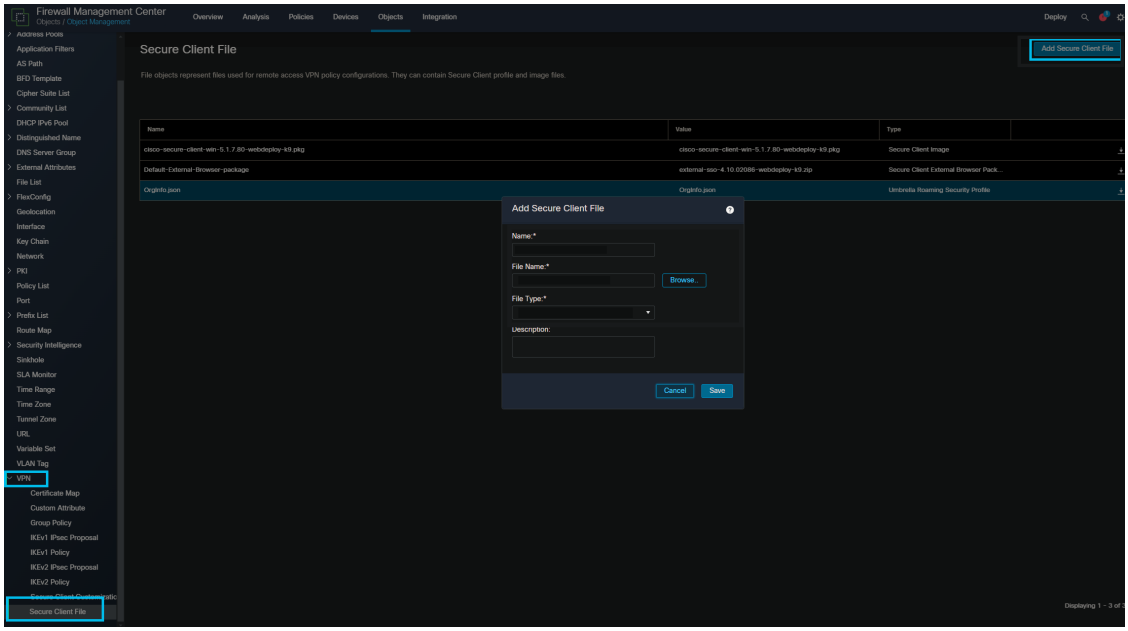
Follow these steps to enable Secure Client Secure Access Module in the management center:

Procedure

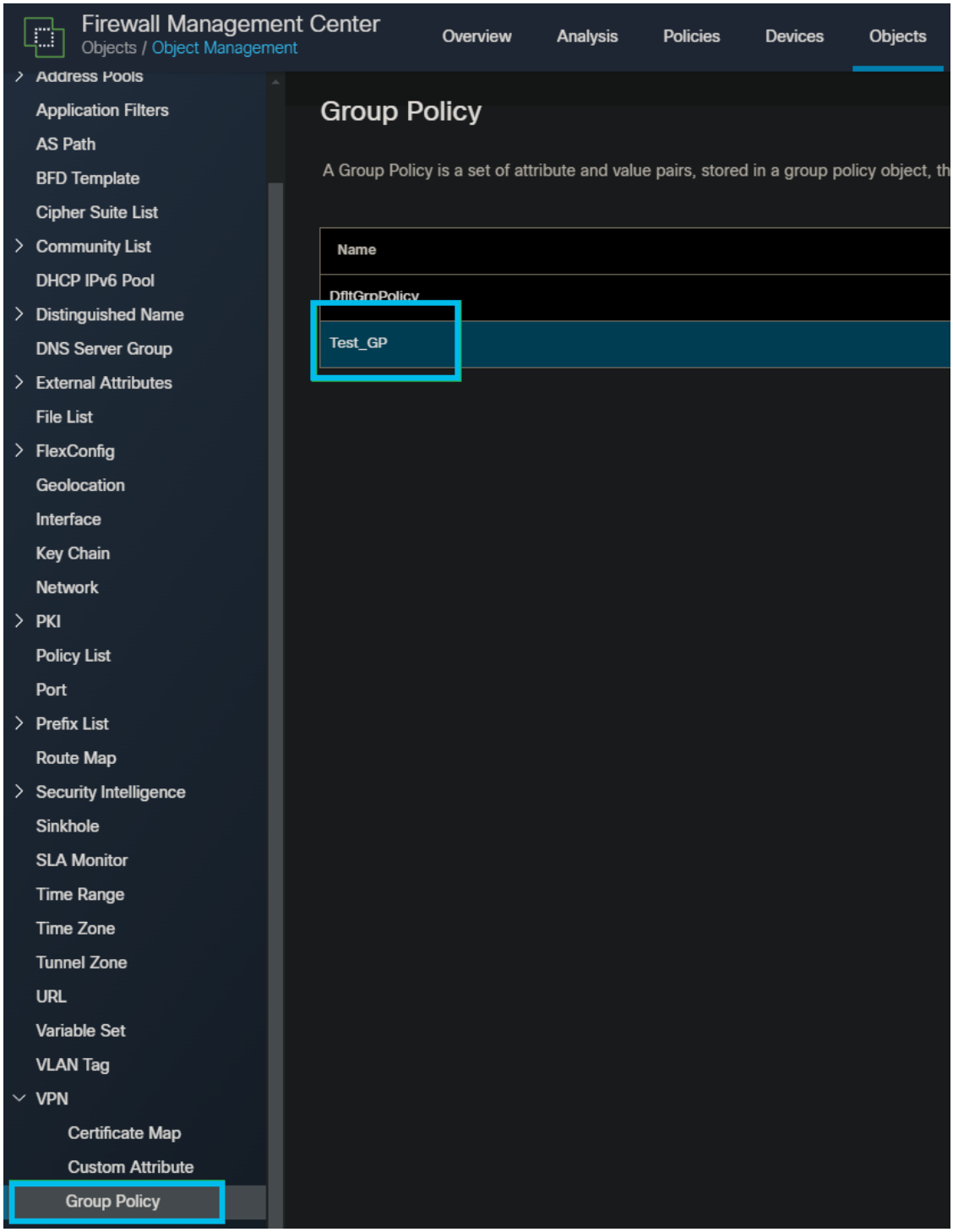
1. In the management center dashboard, go to **Object** > **Objects Management**.



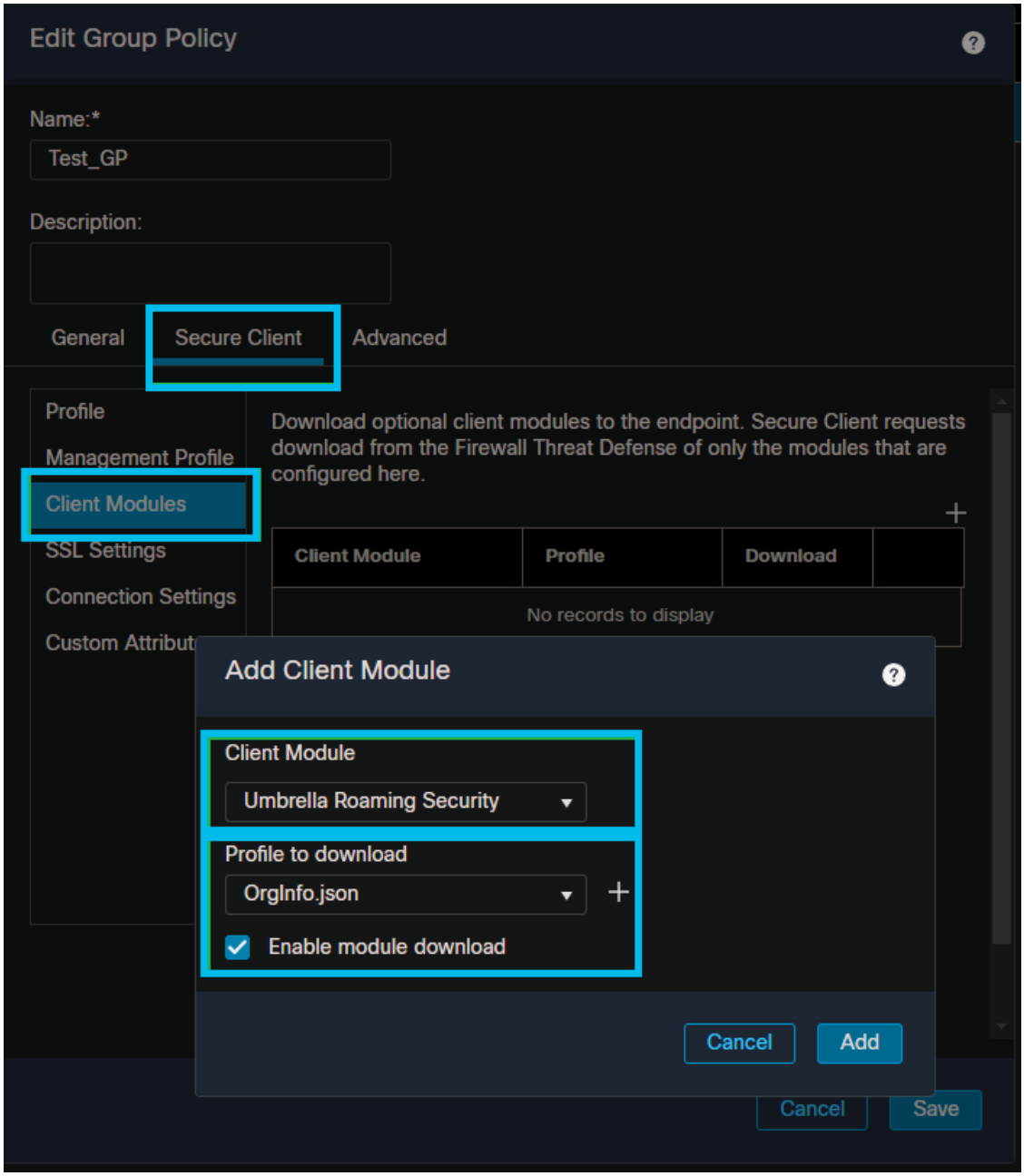
2. Navigate to **VPN** > **Secure Client File**.
3. On the **Secure Client File** page, click the **Add Secure Client File**.



4. In the **Add Secure Client File** window, complete the fields, including the following:
   a. Set a name for the profile (locally significant). From the **File Name**, click **Browse** to choose the JSON file that you just downloaded.
   b. From the **File Type** drop-down list, choose **Secure Access Roaming Security Profile**, and click **Save**.
5. On the Group Policy window, click **Group Policy**, and then select the group policy that you're using to deploy Secure Access ("Test_GP" in this case).



6. Click the **Secure Client** tab, and then click **Client Modules**. Click **+** button to add a client module.
   a. In **Add Client Module**, from the **Client Module** drop-down list, choose **Secure Access Roaming Security**, and from **Profile to download** drop-down list, choose the profile that was added under step 4.
   b. Check **Enable module download** checkbox so that users connecting through Secure Client will automatically download the JSON profile.



(OPTIONAL) VPN Local Authentication (Management Center 7.0 or later required)

Provides instructions for completing the (OPTIONAL) VPN Local Authentication (Management Center 7.0 or later required) workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

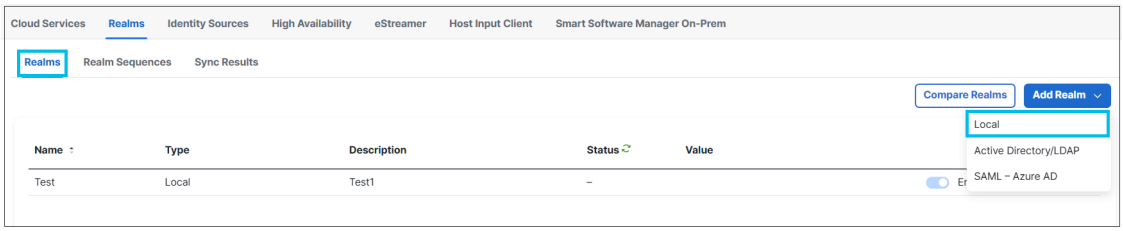
If you want to test a separate profile with local authentication on the management center or threat defense, follow these steps:

Procedure

1. Create a local realm.
   a. Local usernames and passwords are stored in local realms.

b. When you create a realm (**Integration** > **Other Integrations** > **Realms**) and select or create a new **LOCAL realm** type, you are prompted to add one or more local users.

c. Click **Add Realm** > **Local** to create a local realm.



2. Manage a local realm.

a. Click **Integration** > **Other Integrations** > **Realms**.

b. To delete a realm, click **Delete**.

c. To edit a realm, click **Edit** next to the realm.

d. To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.

e. To download users and user groups, click **Download**.

f. To copy a realm, click **Copy**.

Meraki Systems Manager (SM) Deployment

Describes Meraki Systems Manager (SM) Deployment in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Deploying Cisco Meraki Systems Manager (SM) consists of the following steps:

1. Consult our command line parameters reference and confirm if any additional MSI arguments are desired. Examples include hiding from Add/Remove programs and installing without the VPN core.
2. Add a new application to the Meraki SM portal for deployment for the Cisco Secure Client core module MSI.
3. Repeat the process for the Umbrella Module MSI as a second application. For the Umbrella module, add the following command line execution, replacing <OrgInfo.json> with the contents of your organization's Umbrella profile OrgInfo.json file:

```
echo <OrgInfo.json> > "C:\ProgramData\Cisco\Cisco Secure
Client\Umbrella\OrgInfo.json"
```

An example command line execution is below:

```
echo {    "organizationId" : "12345",    "fingerprint" : "12345123451234512345",
    "userId" : "12345"} > "C:\ProgramData\Cisco\Secure
Client\Umbrella\OrgInfo.json"
```

Migration from Secure Access Roaming Client

Describes Migration from Secure Access Roaming Client. The standalone Secure Access Roaming module is approaching end of support and is directly replaced by the Secure Access module in Cisco Secure Client.

The standalone Secure Access Roaming module is approaching end of support and is directly replaced by the Secure Access module in Cisco Secure Client.

The Secure Access Roaming module in Cisco Secure Client provides a more robust handling of DNS and web traffic using the Cisco Secure Client's underlying driver technologies. Cisco Secure Client provides a greater level of compatibility and reliability than the legacy Roaming Client.

To upgrade an existing Roaming Client computer to the Secure Access Roaming module in Cisco Secure Client, install Cisco Secure Client using any of the previous guides of Roaming Security DNS Requirements.

- The existing Umbrella profile information (OrgInfo.json) from Roaming Client will be retained.
- The standalone Secure Access Roaming Client will be automatically removed during installation.
- Under no circumstances should both the Secure Access Roaming Client and Umbrella module be running. Ensure you have disabled any deployment tasks for the Secure Access Roaming Client to prevent re-installation.

Install the Root Certificate for All Browsers

Describes Install the Root Certificate for All Browsers in Cisco Secure Access and explains Inspect and Decrypt HTTPS Traffic and Render Block and Warn Pages. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To inspect web traffic, perform SSL decryption, or render a block page correctly when a browser on a user device attempts to visit a blocked HTTPS web site, install the Cisco Secure Access root certificate for each browser on the organization's user devices. User devices must have the Cisco Secure Client deployed with the Umbrella module.

Steps to perform the installation of certificates vary based on the operating system and browser type. For more information, see Install the Cisco Secure Access Root Certificate.

Inspect and Decrypt HTTPS Traffic

In order to apply most security features to encrypted internet traffic -- and most internet traffic is encrypted -- that traffic must be decrypted. In order to decrypt internet traffic, you must install a Secure Access root certificate for each browser on user devices. See Install the Cisco Secure Access Root Certificate.

Render Block and Warn Pages

Render Block and Warn pages correctly.

1. When a browser on user device visits a blocked HTTPS website, even without HTTPS inspection or SSL decryption enabled, Secure Access does not downgrade the HTTPS protocol to HTTP when serving a block page. Thus, if a root certificate is not installed, the web browser displays a certificate warning to the user. For more information, see Manage Notification Pages.

Cloud Management

Describes Cloud Management in Cisco Secure Access. Cisco Secure Client can now be deployed from Cisco cloud utilizing Cisco XDR or Cisco Secure Client Cloud Management.

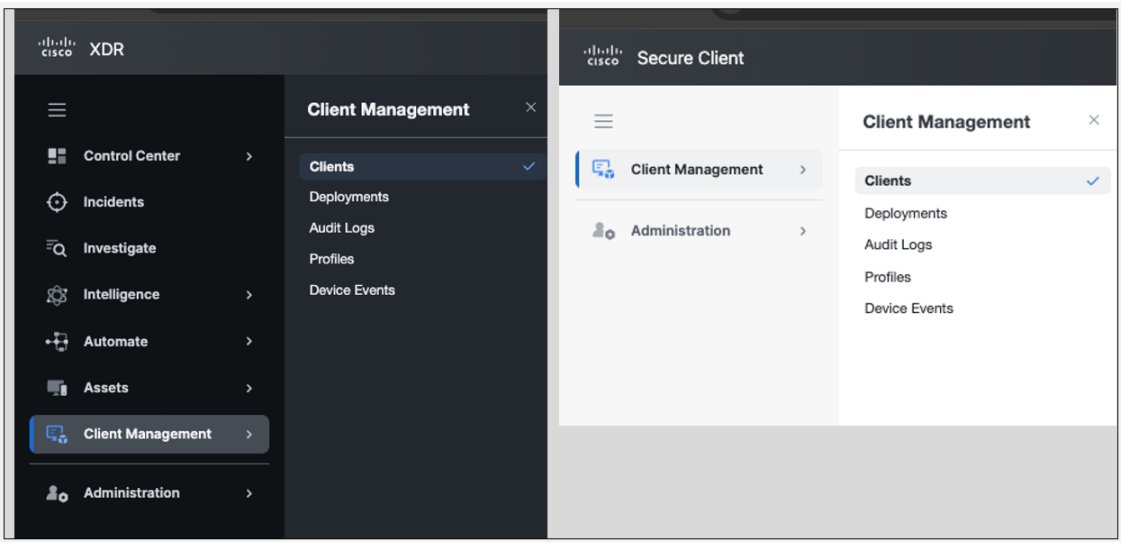
Cisco Secure Client can now be deployed from Cisco cloud utilizing Cisco XDR or Cisco Secure Client Cloud Management.

Cisco XDR is a cloud-based security solution that simplifies operations by helping security teams detect, prioritize, and respond to threats. It integrates Cisco and third-party tools into a single platform for comprehensive threat management. Cisco Secure Client with Client Management is the next-generation Secure Mobility Client that combines the existing features of both AnyConnect and Secure Endpoint with a Cloud Management solution in a single, unified end-user interface.

For customers who are not using Cisco XDR, Cisco offers Cisco Secure Client Cloud Management at no additional cost. This service is available to those with an active Cisco Secure Client or Umbrella license.

Both solutions support the creation and uploading of Cisco Secure Client profiles, including the Umbrella Orginfo.json file. Deployments can then be configured to specify Cisco Secure Client modules using these profiles. The Cloud Management module is essential, enabling the client to check in with the cloud every 2, 4, 6, or 8 hours. This ensures that clients remain up to date, as any changes to their deployment are pushed during these check-ins. Additionally, administrators receive a client inventory that displays installed versions, modules, and the last check-in time.

The following image shows the XDR Client Management and Cisco Secure cloud management:



Deploying Cisco Secure Client

Describes Deploying Cisco Secure Client in Cisco Secure Access. In this instance, XDR will be utilized; However, the procedure remains the same when using Cisco Secure Client Cloud Management too.

In this instance, XDR will be utilized; However, the procedure remains the same when using Cisco Secure Client Cloud Management too.

Profiles

The Profiles page provides a list of all the Cisco Secure Client profiles in your Cisco XDR organization and allows you to create profiles that control the Cisco Secure Client endpoint software.

Note

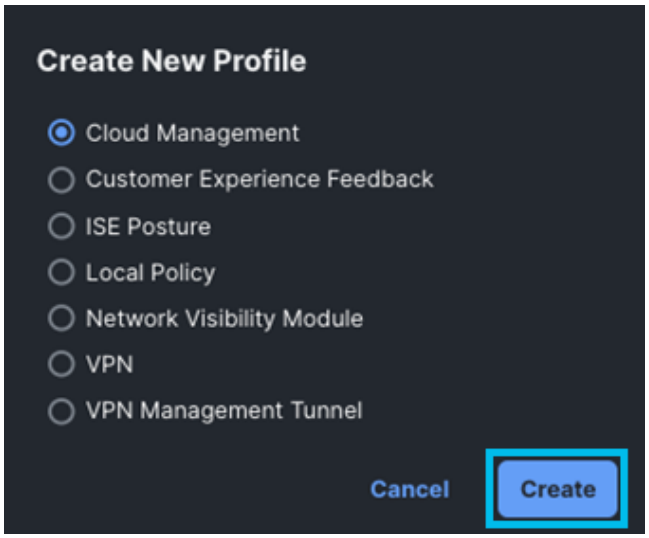
We recommend that you start by gathering existing profiles or using the profile editor in Client Management to create new ones. The online profile editor can create profiles for the modules listed here. For the Network Access Manager (802.1x supplicant) and the Umbrella Orginfo.json, these profiles must be uploaded.

There are only two default profiles, and this is directly from the XDR Client Management Help. The NVM Cloud Default Profile is mandatory but the Cloud Management default profile is optional.

Cisco XDR includes the following default profiles to help you get started with Cisco Secure Client deployments:

- Cloud Management Default Profile
- NVM Cloud Default Profile

The default profiles are associated with the XDR default deployment, which can be installed on your endpoints to improve detections and enrich incidents in Cisco XDR. These profiles can also be applied to any user created deployments. For more information, see XDR Profiles



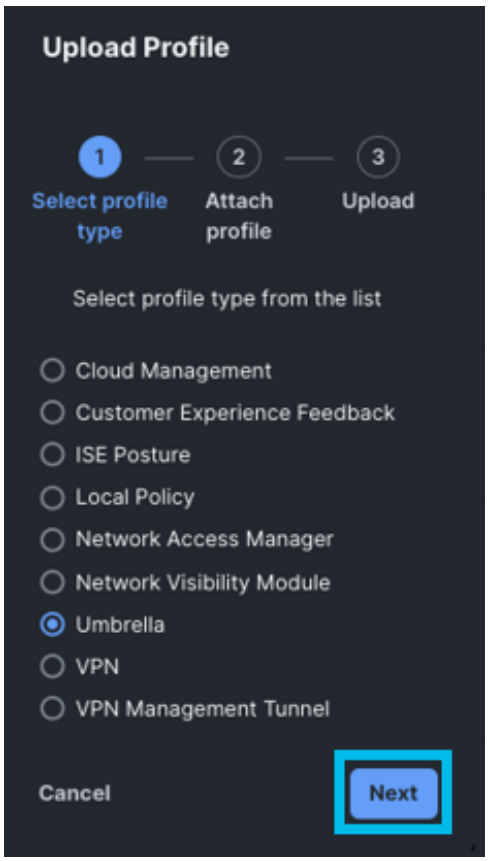
Uploading the Orginfo.json profile

Provides instructions for completing the Uploading the Orginfo.json profile workflow in Cisco Secure Access. Navigate to Client Management Profiles Upload , select Umbrella from the list and click Next.

Upload the Orginfo.json file that you previously downloaded from the Umbrella dashboard.

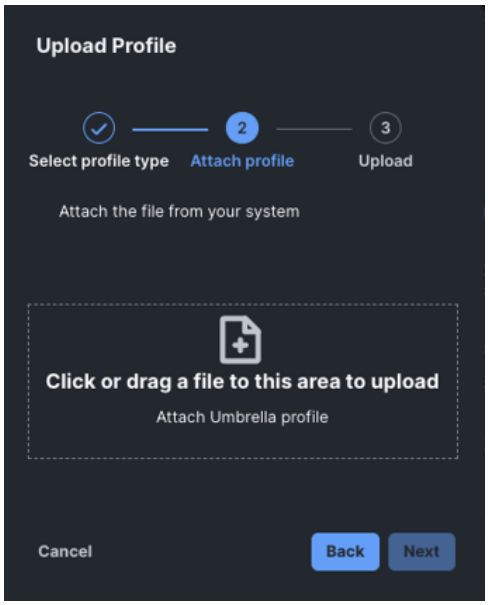
Procedure

1. Navigate to **Client Management** > **Profiles** > **Upload**, select **Umbrella** from the list and click **Next.**

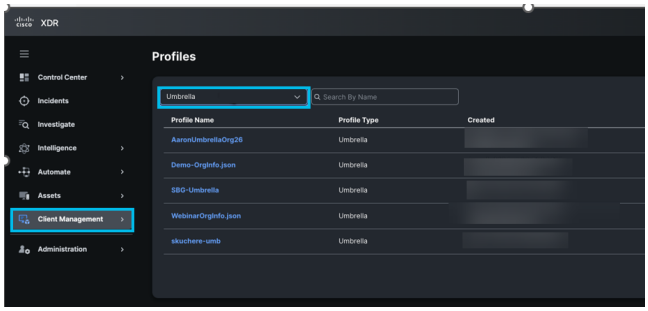


A pop-up is displayed.

2. You can either drag and drop the `Orginfo.json` file or navigate to its location to add this profile and make it available for deployments.



3. After the file is uploaded, go to **Client Management** > **Profiles** and, if required, apply a filter for Umbrella to display only the available Umbrella profiles. Typically, this step has to be performed only once. The profiles can be used in multiple deployments.



Create a Deployment

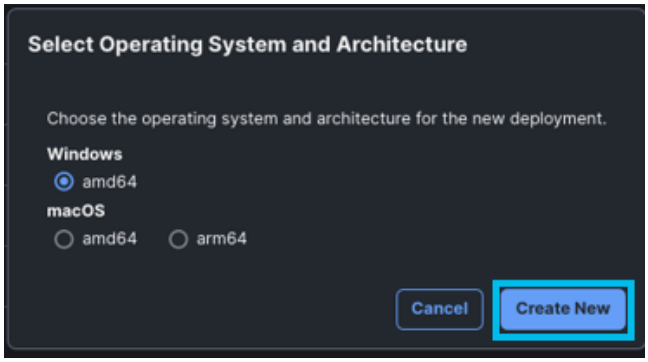
Provides instructions for completing the Create a Deployment workflow in Cisco Secure Access. To create a new deployment, navigate to Client Management Deployments and click on New.

The Deployments page provides a list of all the Cisco Secure Client deployments in your Cisco XDR organization and allows users to define a list of all the packages and related profiles that must be installed on all the computers in a specific deployment within an organization (for example, QA department).

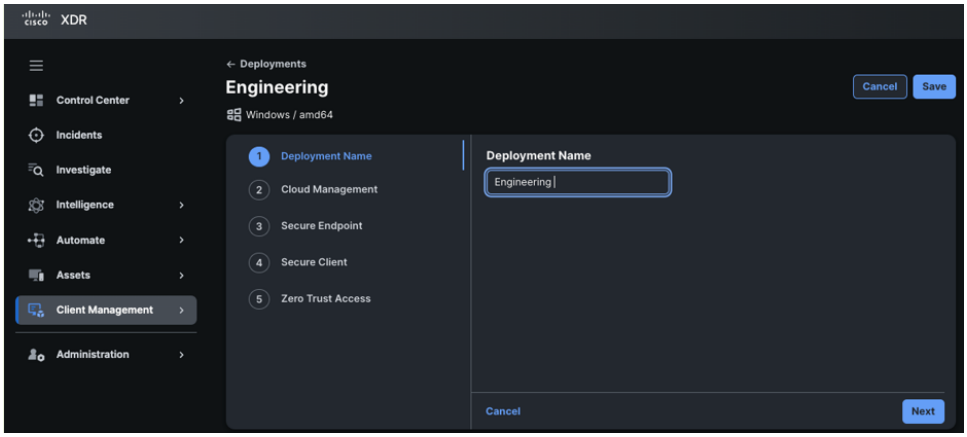
Procedure

1. To create a new deployment, navigate to **Client Management** > **Deployments** and click on **New**. You can also edit existing deployments from the list displayed.
2. When prompted, select the operating system for the deployment, that is, either **Windows** or **macOS**.

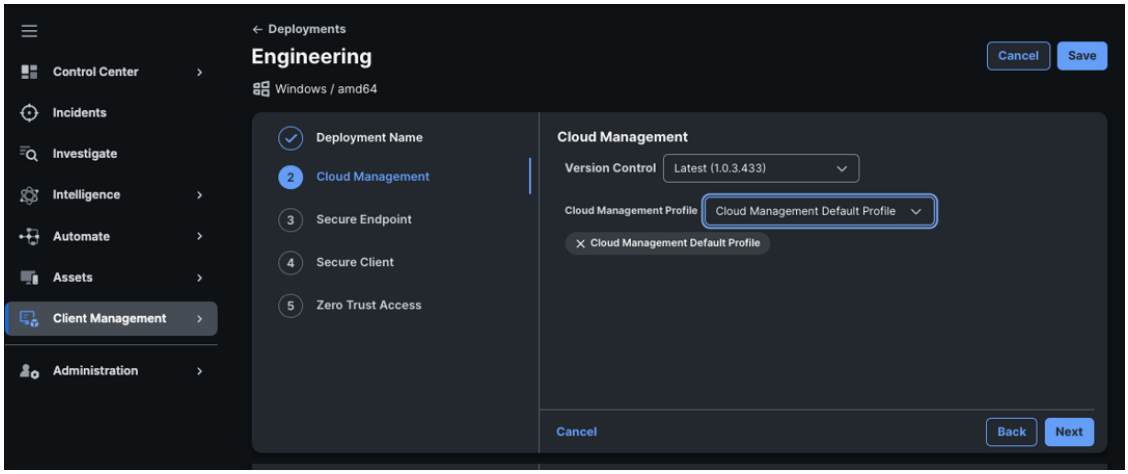
   In this example, **Windows** is selected.
3. Click **Create New**.



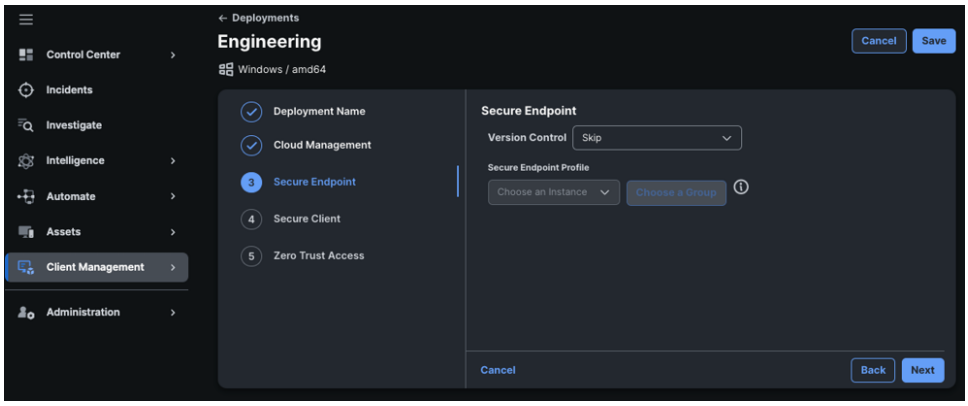
4. **Specify** a name for the deployment: This name will be included in the file name of the final package after the deployment configuration is complete.



Every deployment includes the Cloud Management module and profile. Choose a version for both the Cloud Management module and the Cloud Management profile. While the default Cloud Management profile typically works well, administrators have the option to create a custom profile, if needed. For example, you might want different check-in intervals or update Windows for certain user groups.



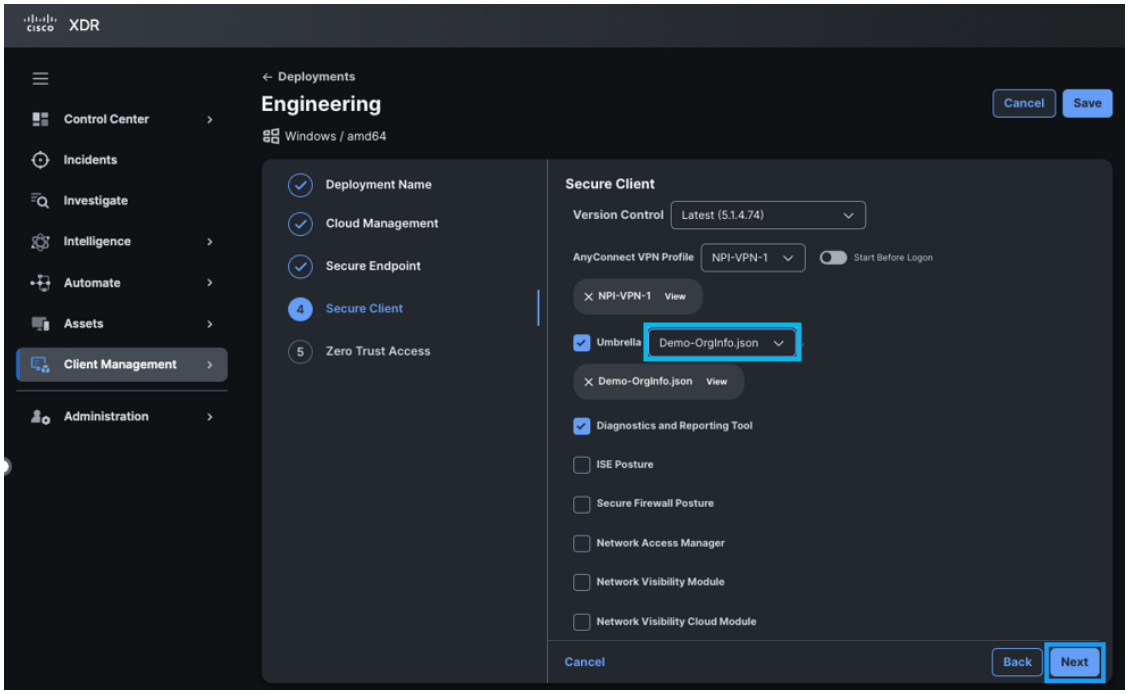
5. From the **Version Control** drop-down list, choose the Secure Endpoint connector version that you want to deploy. If you prefer to not include the Secure Endpoint module, choose **Skip** and proceed. In this example, **Skip** is chosen.



Next, configure the Cisco Secure Client section to include AnyConnect VPN, Umbrella, and DART in the deployment.

> **Note**
>
> If you don't plan to use AnyConnect VPN, you can skip adding a VPN profile. After completing the cloud deployment, push the `VPNDisable_ServiceProfile.xm` file to the VPN profile directory (as described earlier in Customize Windows Installation of Cisco Secure Client guide). This hides the AnyConnect VPN tile in the GUI.

To complete the Cisco Secure Client section of the deployment, we selected an existing VPN profile that was either uploaded or created in Client Management using the profile editor. Along with the VPN profile, we enabled the DART and the Umbrella module, specifying the previously uploaded Umbrella OrgInfo.json profile. This configuration generates a deployment package that includes the specified modules and profiles upon installation.

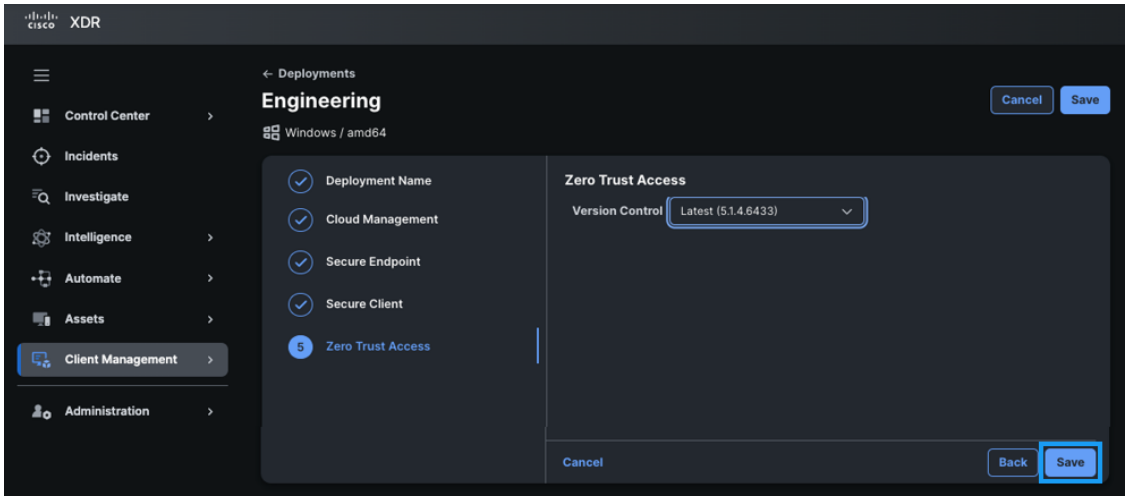


6. After completing the deployment configuration, click **Next**.

   For Windows deployments, the administrator will have the option to add the Zero Trust Access (ZTA) module for Cisco Secure Client. While the ZTA module is supported on macOS through other deployment methods, it is not yet supported for cloud deployments using XDR or Cisco Secure Cloud Client Management. The ZTA module is designed to work seamlessly with the Cisco Secure Access solution.

   ZTA focuses on knowing, understanding, and controlling who and what is on your network:

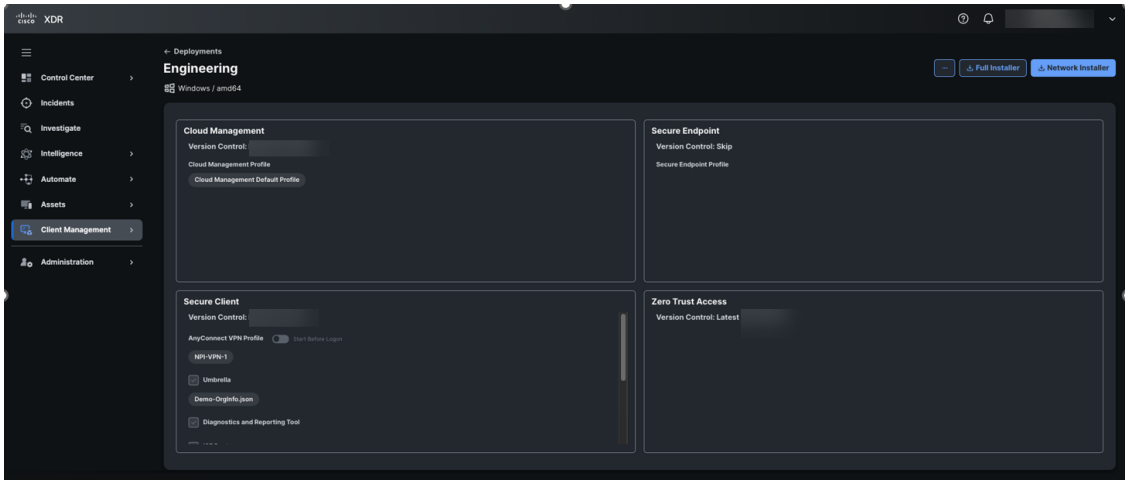
   - It grants appropriate access based on role or function.
   - It controls application access at the network layer.
   - By assuming that the network layer is untrustworthy, it helps prevent unauthorized access and breaches.



7. When you click **Save** it finalizes the deployment configuration and presents the Administrator with two installation package options – Network Installer or Full Installer.

   - **Network Installer**: A streamlined installer that includes only the Cloud Management client. When using the Network Installer, it will download the remaining components specified in the deployment in the background.
   - **Full Installer**: A comprehensive package that includes all the installers and profiles configured for the deployment. It is larger than the Network Installer, and when used, it installs the Cloud Management client along with all associated packages from the deployment.

   Both the Full and Network installers will link the device to the deployment from which the installer was created. Whenever the device connects to the cloud, it checks the installed packages against the deployment requirements. The device then updates the packages and profiles to match the deployment, but does not downgrade any packages that are newer than those specified in the deployment.



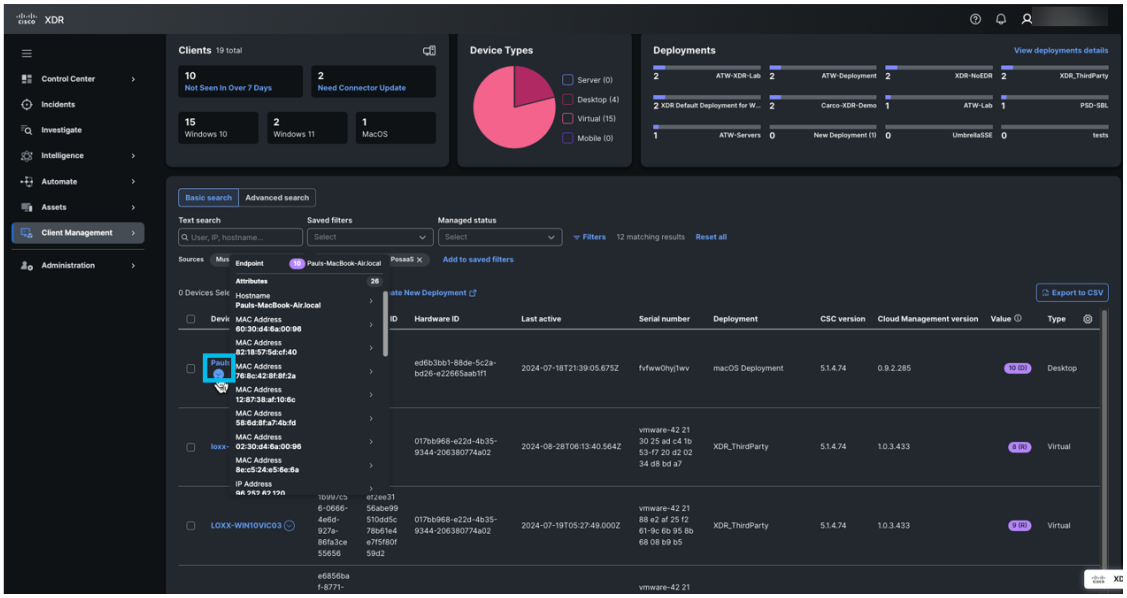
Post Deployment

Describes Post Deployment in Cisco Secure Access. After deploying Cisco Secure Client with Cloud Management, both Cisco XDR and Cisco Secure Client Cloud Management offer valuable insights into the clients deployed to the cloud.

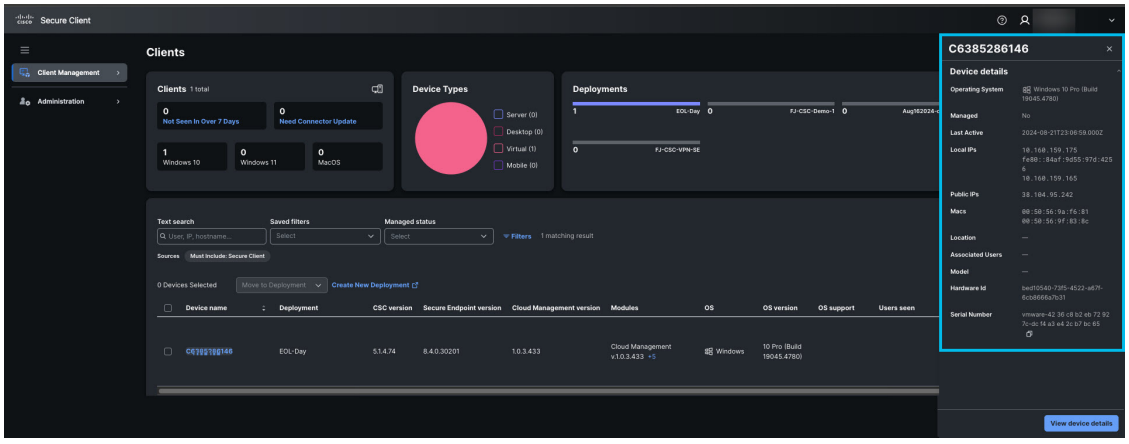
After deploying Cisco Secure Client with Cloud Management, both Cisco XDR and Cisco Secure Client Cloud Management offer valuable insights into the clients deployed to the cloud. The administrator can access a comprehensive inventory of these clients by navigating to **Client Management** > **Clients**. A table lists all the Cisco Secure Client devices in your organization along with their data. The following information is also displayed:

- The total number of devices found.
- The number of devices selected.
- **Move to Deployment:** Click to move selected devices to a specific deployment.
- **Create New Deployment:** Click to open the Deployments page. From this page, Admin users can define a list of all the packages and related profiles that must be installed on all the computers in a specific deployment within an organization.
- **Export to CSV:** Click to download the table contents to a spreadsheet. Note that only the contents of the table will be downloaded.

Each device includes a pivot menu icon that enables you to take action on it. You can perform some actions directly using pivot menu or pivot to the integrated product to perform additional actions.



The behavior varies slightly when performed in Cisco Secure Client Cloud Management. However, the Administrator can switch to a detailed view for more information.



Additional Reference

For more information about Cisco Secure Client Cloud Management, please refer to the FAQ.

Additional References

Describes Additional References in Cisco Secure Access. The following guides provide in-depth information for customers deploying Cisco Secure Client with endpoint management, systems management, or device management tools.

The following guides provide in-depth information for customers deploying Cisco Secure Client with endpoint management, systems management, or device management tools.

Command Line and RMM Reference (Windows)	Provides information about installing Cisco Secure Client using the CLI (Windows)
Customize Windows Installations of Cisco Secure Client (Windows)	Provides command-line reference for installing Cisco Secure Client. Includes customizations for disabling the VPN functionality and locking down Cisco Secure Client services
Customize MacOS installations of Cisco Secure Client	Provides detailed instructions for creating a mass deployment package for macOS. Includes customizations for disabling VPN functionality and approving Cisco Secure Client extensions.
VPN Headend Installation (Windows)]	Provides customers who are using Secure Client VPN functionality to deploy Umbrella from their VPN headend. This will automatically download the software and profile when connecting to VPN.
Meraki Systems Manager (SM) (Windows)	Provides information about how to deploy the Umbrella profile (OrgInfo.json) on Windows computers using post-install scripts.
Microsoft InTune (Windows)	Provides a tutorial for Intune (Windows clients). The software and Umbrella profile are packaged together using the Content Prep tool and delivered to Windows endpoints.
Microsoft InTune (macOS)	Provides a tutorial for Intune (macOS clients). A mass deployment package is created and deployed with a scripted task.
Shared Folder Installation (Windows)	Provides an example on how to install from a shared folder installation source using a script. In this example, the script is triggered using a scheduled task (Windows group policy).
GPO Installation (Windows)	Provides Cisco Secure Client to deploy as an application package using Windows group policy (GPO). The Umbrella profile is deployed to the endpoint using Windows group policy (GPO).
JAMF (macOS)	Provides a tutorial for JAMF (macOS Clients). The software, profile, and install choices (module selection) are bundled together using the JAMF composer.
Deploy Cisco Secure Client	Provides instructions for installing Cisco Secure Client and all modules (non-Umbrella specific) from cisco.com.

Remote Monitoring and Management Deployment Tutorials

The following tutorials are suitable for MSPs using Remote Monitoring and Management (RMM) to deploy the Umbrella Roaming Security Module to multiple end customers. A different Umbrella profile (OrgInfo.json) can be supplied for each customer in the RMM tool.

ConnectWise	Cisco-provided sample ConnectWise configuration templates
Kaseya	Cisco-provided sample Kaseya configuration templates

Manage Device Deployment

Describes Manage Device Deployment in Cisco Secure Access. The Deployment keys feature provides an effective way to manage device registration within organizations while mitigating unauthorized access.

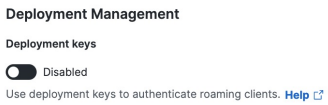
The **Deployment keys** feature provides an effective way to manage device registration within organizations while mitigating unauthorized access. This functionality introduces the concept of a **deployment key** that can be activated, deactivated, and revoked. By utilizing deployment keys, administrators gain control over the credentials used by devices during registration for Secure Access protection. A deployment key is a field in the OrgInfo.json file, which is used when registering devices to your organization's network. This feature ensures that only authorized devices are enrolled by requiring an active deployment key for registration.

This feature facilitates seamless device registration and ongoing validation while offering the flexibility to deactivate keys when necessary. If any unauthorized devices try to connect, administrators can swiftly deactivate the current deployment key and delete the suspected devices from the dashboard, ensuring a secure and efficient network environment. The devices will not be able to reregister with the now-deactivated deployment key. Administrators can then activate a new deployment key. This allows IT teams to maintain operational continuity while safeguarding against unauthorized access.

Prerequisites for Device Deployment Management

- Uninstall all the existing Cisco Secure Client installations.
- Enable the Deployment keys feature (**Connect** > **End User Connectivity** > **Internet Security**) if it is disabled.

> **Note**
>
> For the Global deployment, the Deployment key feature is optional. In other deployments, such as in China, the **Deployment key** feature is mandatory, and is automatically enabled.

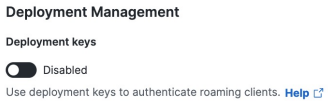


Prerequisites for Device Deployment Management

Describes Prerequisites for Device Deployment Management in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

- Uninstall all the existing Cisco Secure Client installations.
- Enable the Deployment keys feature (**Connect > End User Connectivity > Internet Security**) if it is disabled.

> **Note**
>
> For the Global deployment, the Deployment key feature is optional. In other deployments, such as in China, the **Deployment key** feature is mandatory, and is automatically enabled.

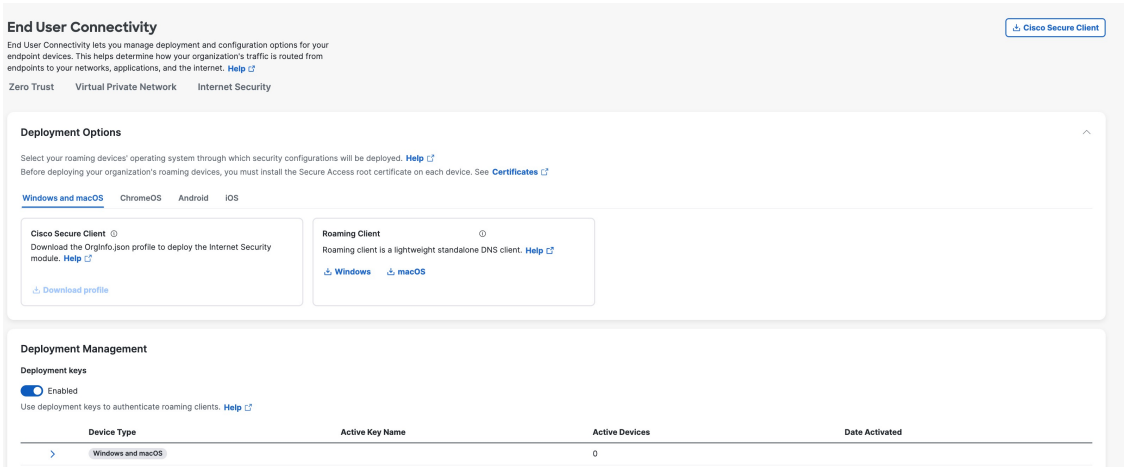


Add and Activate Deployment Key

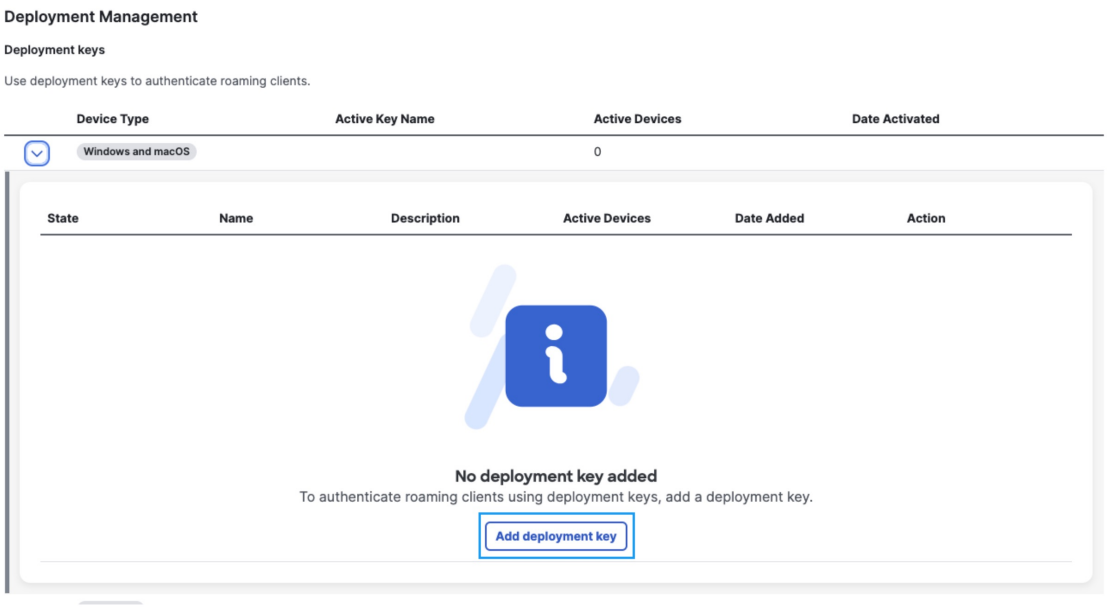
Provides instructions for completing the Add and Activate Deployment Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

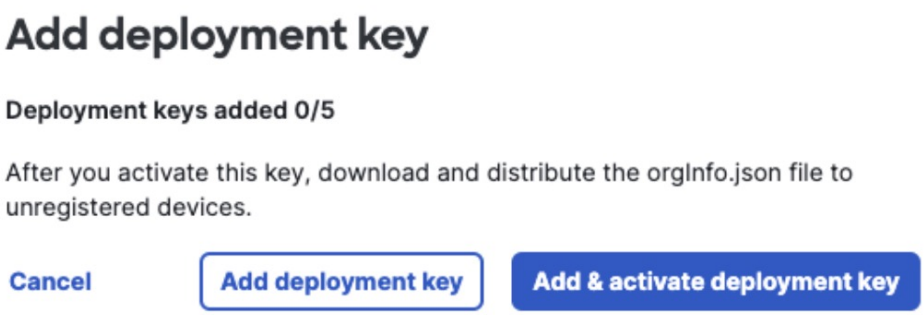
1. Navigate to **Connect** > **End User Connectivity**.
2. Click **Internet Security**.
3. In the **Deployment Management** section, expand the device type (Windows and macOS).



4. Click **Add deployment key**.



5. In the **Add deployment key** window, click **Add & activate deployment key** to create and activate a deployment key for inclusion in your organization's OrgInfo.json file.



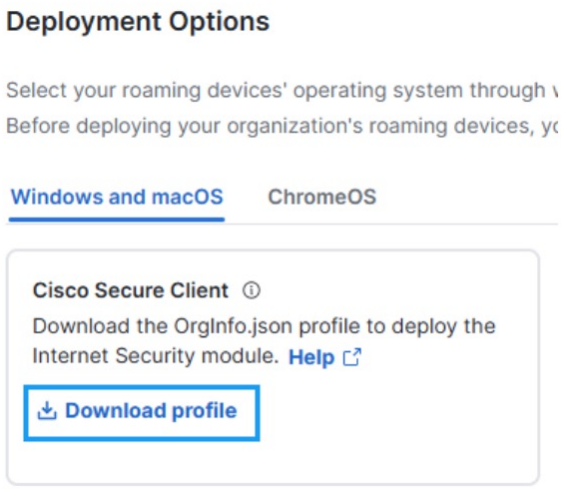
What to do next

You can choose to add the deployment key immediately, but activate it later. In such a scenario, click **Add deployment key**. The deployment key is added to the table. When you are ready to activate the deployment key, click **Activate** in the **Action** column.

Important

- Only one deployment key can be active at a time for each device type.
- You can add up to five deployment keys per device type. To remove a key, contact Cisco support or your Account Manager.
- The deployment key name includes a random number to ensure its uniqueness.

If your Secure Access deployment requires a deployment key, or if your organization has already enabled them, the `OrgInfo.json` file can only be downloaded when there is an active deployment key (see image below). For more information on how to download the `OrgInfo.json` file, see Download the OrgInfo.json File.



> **Note**
>
> To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

Manage Deployment Key Compromise

Provides instructions for completing the Manage Deployment Key Compromise workflow in Cisco Secure Access. If you determine that a key has been compromised, take action to protect your network's integrity and security.

If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

This section outlines the necessary actions to be taken to ensure network security and continuity, including deactivating compromised keys, understanding the effects on existing clients, and steps for activating and distributing a new key for secure device registration.

> **Note**
>
> The `OrgInfo.json` file is case-sensitive only in the region-specific subdirectory, not in the umbrella directory.

Procedure

1. **Deactivate the Compromised Key**: This action prevents any further device registrations using the deactivated key, ensuring that your network remains secure.

   To deactivate a deployment key, perform the following steps:

   a. From the Secure Access dashboard, navigate to **Connect** > **End User Connectivity**.

   b. Click **Internet Security**.

   c. In the **Deployment Management** section, expand the device type.

   d. Click **Deactivate** in the **Action** column.

   Upon deactivating the compromised deployment key, it is important to consider its implications on both existing clients and the registration of new devices:

- **Effect on existing clients**: It's important to note that deactivating a key will not disrupt the operation of clients already using it. These clients will continue to function normally, minimizing any potential impact on your current network operations.
- **Limitations for new devices**: However, deactivated keys cannot be used for registering new devices. This means that any device attempting to register itself with the deactivated key will be unable to do so.

> **Note**
>
> Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, but only if the deployment key in their `OrgInfo.json` file is active.

2. **Activate the new deployment key**: To facilitate the registration of new devices, you must activate a different deployment key. This new key will replace the compromised one and will be used for future device registrations.
3. **Download a new profile**: After the new key is activated, download a new profile, specifically the `OrgInfo.json` file. This file contains the updated information, including the new active deployment key.
4. **Distribute the new profile to new devices**: Distribute the updated `OrgInfo.json` profile to any new devices that need to connect to your network. This ensures that they have the correct and secure credentials to register and operate within your network environment.
5. **Update the OrgInfo.json file for registered devices**: For devices that are already registered and need the `OrgInfo.json` file to be updated, place the new file in the correct subdirectory within the `Umbrella/data/regionaldata/<region_name>` directory, where the original `OrgInfo.json` file was located. After updating the file, restart the Cisco Secure Client-Umbrella Agent Windows service to apply the changes. The region_name in the directory should match the region tag found in the `OrgInfo.json` file. If the region tag is missing, it is assumed to be "global".

> **Note**
>
> The `OrgInfo.json` file is case-sensitive only in the region-specific subdirectory, not in the Umbrella directory.

Delete a Deployment Key

Describes Delete a Deployment Key in Cisco Secure Access. To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

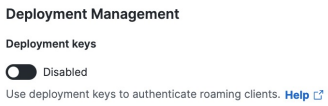
> **Caution**
>
> Deleting a Deployment Key is a high-impact action. It immediately disconnects existing roaming devices and stops new device registrations and synchronizations. Ensure that you have identified the correct key before performing any management actions.

If an active deployment key is deleted, administrators must generate a new key, download the updated profile, and distribute the profile to all affected devices to restore connectivity. For detailed recovery steps, see Manage deployment key compromise.

Reverting to Using Legacy Deployment Implementation

Describes Reverting to Using Legacy Deployment Implementation in Cisco Secure Access. If needed, you can revert to the legacy registration mechanism by disabling the Deployment Keys feature (Connect End User Connectivity Internet Security).

If needed, you can revert to the legacy registration mechanism by disabling the **Deployment Keys** feature (**Connect** > **End User Connectivity** > **Internet Security**).



- After disabling the Deployment Keys feature, devices that are currently using the last activated deployment key will continue to be protected by Secure Access. However, new devices will not be able to register with the deactivated deployment key.
- To revert to the legacy registration mechanism, download the updated **OrgInfo.json**, which will no longer include the deployment key. New devices can now register using the legacy method.

Backward Compatibility

Describes Backward Compatibility in Cisco Secure Access. This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

For example, on Windows and macOS:

- Cisco Secure Client Release 5.1.7 or earlier will continue to use the legacy User ID and fingerprint for registration purposes, regardless of whether a deployment key is present.
- Cisco Secure Client Release 5.1.8 or later will use the deployment key for registration, regardless of whether the User ID and fingerprint are present. If the deployment key is unavailable, the legacy User ID and fingerprint will be used for registration instead.

59 Zero Trust Access using Cisco Secure Client

Topics:

- Manage Zero Trust Access using Cisco Secure Client

Provides an overview of Zero Trust Access using Cisco Secure Client in Cisco Secure Access, including Manage Zero Trust Access using Cisco Secure Client. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Zero Trust Access using Cisco Secure Client

Describes Manage Zero Trust Access using Cisco Secure Client in Cisco Secure Access. Zero Trust Access means that no one is trusted by default, whether inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.

Zero Trust Access means that no one is trusted by default, whether inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. Enrolling in Zero Trust Access implies an enhanced level of security that reduces the attack surface by ensuring that only authenticated and authorized users and devices can access specific resources. This method aligns well with cloud adoption, remote work, and mobile device usage by securing access regardless of location.

Cisco Secure Client supports Zero Trust Access to private resources and internet resources from user devices. To use the Secure Client with Zero Trust Access on a supported device, a user must enroll in Zero Trust Access on the Secure Client. Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, SaaS apps, and internet resources protected by Secure Access. Secure Client is configured with various software modules. A Secure Client module may require the deployment of a certain profile to run module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Secure Client on an organization's user devices. For more information about the Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Supported Use Cases

To allow these users to access the resource, use the solution described on this page to ensure that the egress IP address associated with their devices is within your organization's IP address space.

The following scenarios are supported:

- Option 1: Allow Zero Trust Access connections to internet and SaaS destinations you specify.
- Option 2: Allow Zero Trust Access connections using private resources as the internet destination. See Traffic Steering for Zero Trust Access Client-Based Connections for more information.

Limitations

For a full matrix of platform and feature support see Zero Trust Access Requirements and Limitations on page 1207.

Zero Trust Access Logs

When a Zero Trust Access request passes through the different services in Secure Access, various scenarios or configurations generate a variety of logs. See the following explanations on how to investigate and process the logs created:

Secure Private Access (SPA)

- Zero Trust Access client-based logs for policy enforcement, verdicts and block reasons, as well as any handling issues that prevented enforcing at all.
- Firewall logs in case a security feature (IPS, Security profiles, DLP) is enabled for your Zero Trust Access traffic and is so passed through the firewall service for enforcement.

Secure Internet Access (SIA)

- Zero Trust Access client-based logs for request handling and any issues that come up for it, as well as global posture enforcement details in case of a posture block.
- Firewall or Secure Web Gateway (SWG) logs for the outcome of the Secure Access SIA stack policy evaluation, after Zero Trust Access as the headend has handed off the traffic for enforcement.

- DNS logs for the internet DNS resolution that happens at the Zero Trust Access proxy (which is done against the Secure Access resolvers).

Overview of How to Manage ZTA with Cisco Secure Client

The following outline is a general overview of the steps required, or recommended, to successfully complete this task:

1. Install the Cisco Secure Client on either your Windows, macOS, or Linux environment.

   Note

   Zero Trust Network Access (ZTNA) does not support multi-user login in any of these environments.

   A Secure Client module may require the deployment of a certain profile to run module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Secure Client on an organization's user devices. For more information about the Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

2. Enroll Devices in Zero Trust Access Using Certificates. You can do this by using certificates or with an SSO Authentication service. Before users can access resources using client-based Zero Trust Access, they must first enroll. Note that Zero Trust Network Access (ZTNA) does not support multi-user macOS machines. If you use macOS and have Duo Security enabled, Duo may overwrite some states.

Note

If you enable both methods, a device can use either method if the per-device and per-user requirements are met. Each device requires only one method to enroll.

If you deploy a certificate-based configuration file on a device, SAML-based enrollment is automatically disabled. If you remove the certificate-based configuration file from the device, SAML-based enrollment automatically becomes available for that device.

Both enrollment authentication mechanisms are used only for enrollment and enrollment renewal; they are not involved in per-session connectivity when end users access resources. Per-session authentication is managed by the Zero Trust Access feature.

Both methods require periodic enrollment renewal.

Enroll Devices in Zero Trust Access Using Certificates

Describes Enroll Devices in Zero Trust Access Using Certificates in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Before you use this procedure to enroll your environment, either a Windows, macOS, or Linux device, in Zero Trust Access (ZTA) without requiring any action or awareness from users, review the following prerequisites:

- Use this method to enroll user devices without requiring user action or awareness.
- Users cannot accidentally or intentionally unenroll the zero trust client module on their device.
- Periodic enrollment renewal is automatic if requirements are still met.
- On user devices:
  - Minimum device operating system version:

- Windows 10
- macOS version 11
- Linux Red Hat 9.0

  Ubuntu 24.04

  > **Note**
  >
  > IPv6-only networks are not supported on Ubuntu 24.04.

- Windows devices must support Trusted Platform Module (TPM) 2.0
- Mac devices must support Secure Enclave

- Cisco Secure Client must be installed on user endpoint devices. The Zero Trust Access module is integrated into the Cisco Secure Client.
  - For Windows, macOS, and Linux devices, see Download the Cisco Secure Client and Install the Cisco Secure Client.
  - Minimum Cisco Secure Client version: see 5.1.17.

- Each device must have an identity certificate signed by your corporate certificate signing authority (CA). The identity certificate must be tied to a specific user, not to the device, so:
  - The certificate Subject Alternative Name (SAN) must include the user's RFC 822-compliant email address, or the User Principal Name (UPN) field must include the username.
  - The ZTA Client will evaluate certificates with an Issuer Common Name that matches any of the CA certificates enabled in the ZTA enrollment dashboard. If multiple identity certificates share the same Common Name, the client will select the first matching certificate.
  - The identity certificate must be installed in the machine or user-specific keystore on each device.
    - On Windows: Use Windows user keystore
    - On macOS: Use Keychain access in the user store
    - On Linux: Copy the certificate to

      ```
      ~/.cisco/certificates/client/
      ```

Step 1 - Upload or choose a CA certificate

Provides instructions for completing the Step 1 - Upload or choose a CA certificate workflow in Cisco Secure Access. User endpoint devices present an identity certificate when enrolling and renewing enrollment.

User endpoint devices present an identity certificate when enrolling and renewing enrollment.

Secure Access must hold the certificate that verifies these user identity certificates.

You can upload a new certificate or choose an already-uploaded certificate. Zero Trust Access enrollment can use the same certificate that validates identity certificates for VPN connections, or use a different certificate for zero trust enrollment. You must specify the purpose or purposes of each certificate during upload. You can modify the purpose later. Uploads must include the intermediate certificates required to complete the chain of trust.

To upload the certificate:

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. Click the **Zero Trust Access** tab.
3. In the Enrollment Methods section, select **Manage**.
4. Click **Upload a CA Certificate** and complete the form as described in Manage CA Certificates for VPN Connections and Zero Trust Access Enrollment.

> **Note**
>
> As an alternative method, you can upload certificates to the client authentication certificates page. See Manage CA Certificates for VPN Connections and Zero Truts Access Emrollment for more information.

Step 2 - Download the enrollment configuration file

Describes Step 2 - Download the enrollment configuration file in Cisco Secure Access. Before you download the configuration file, you must upload the CA certificate that validates the identity certificate that a device presents at enrollment and renewal.

Before you download the configuration file, you must upload the CA certificate that validates the identity certificate that a device presents at enrollment and renewal. Each time a CA certificate is uploaded for ZTA enrollment purposes, the ZTA enrollment configuration file is regenerated. The configuration file includes information about all CA certificates that have been uploaded and designated for ZTA enrollment.

You can download the configuration file from either of two locations:

- Navigate to **Connect** > **End User Connectivity**, click the **Zero Trust Access** or **Virtual Private Network** tab, then click the **Cisco Secure Client** button.

  or

- Navigate to **Connect** > **End User Connectivity**, click the **Zero Trust Access** tab. In the **Enrollment Methods** section, click **Manage**. Download the file from the **Use Certificates** section.

The configuration file name is *orgID*_ZTA_Enroll_Cert.json.

Step 3 - Install the enrollment configuration file on user devices

Describes Step 3 - Install the enrollment configuration file on user devices in Cisco Secure Access. In order to prevent tampering, this configuration file is installed in a directory that requires Administrator access, and the file is signed.

In order to prevent tampering, this configuration file is installed in a directory that requires Administrator access, and the file is signed. Do not attempt to modify it.

Install the configuration file on each user device in the following location:

- On Windows devices:

```
C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices
```

- On macOS and Linux devices:

```
/opt/cisco/secureclient/zta/enrollment_choices
```

If a CA certificate expires or is replaced, deleted, or revoked, you must distribute a new configuration file to authorized devices, with information about the replacement CA certificate.

You can change the file name, but make sure there is only one ZTA enrollment configuration file on the device.

Switch from SAML-based enrollment to Certificate-based enrollment

Install a certificate-based enrollment configuration file on the device. This automatically disables SAML-based enrollment for that device.

Enroll Devices in Zero Trust Access Using SSO Authentication Overview

Describes Enroll Devices in Zero Trust Access Using SSO Authentication Overview in Cisco Secure Access. This method requires users to sign in on their device and follow simple prompts using information that you provide to them outside of Secure Access.

This method requires users to sign in on their device and follow simple prompts using information that you provide to them outside of Secure Access. Before you use SSO authentication such as SAML to enroll Cisco Secure Client for Zero Trust Access, review the following prerequisites for this enrollment method and the recommended use case:

Prerequisites

Ensure the following items have been completed prior to enrolling your device in ZTA with an SSO authetncation method:

- This is the default enrollment method and is always enabled.
- Users of managed or unmanaged devices can use this enrollment method.
- Install the Secure Client with the Zero Trust Access module on user devices.
- Provision the users and groups in your organization. For more information, see Manage Users and Groups.
- Ensure that user authentication profiles are configured for SSO authentication. See Manage User Authentication Profiles.
- On user devices:
  - Minimum device operating system version:
    - Windows 10
    - macOS version 11
    - Linux Red Hat 9

      Ubuntu 24.04

      > **Note**
      >
      > IPv6-only networks are not supported on Ubuntu 24.04.

    - Windows and Linux devices must support Trusted Platform Module (TPM) 2.0
    - Mac devices must support Secure Enclave

Recommended Use Case

We **strongly** recommend using the **Use MFA Authentication and Biometric Identity** feature.

For the highest security during end-user enrollment, we strongly advise that you take advantage of your established MFA-based authentication and the use of biometric identity for user authentication.

Now continue to the Enroll Devices in Zero Trust Access Using SSO Authentication on page 2030.

Enroll Devices in Zero Trust Access Using SSO Authentication

Provides instructions for completing the Enroll Devices in Zero Trust Access Using SSO Authentication workflow in Cisco Secure Access. Zero Trust Access may not be familiar to your users, so we recommend that you educate them on its benefits before prompting them to enroll.

Zero Trust Access may not be familiar to your users, so we recommend that you educate them on its benefits before prompting them to enroll. To help with that effort, following is some suggested language that you can use to speak about Zero Trust Access that includes instructions on how to enroll.

Note

Many of today's workers, like you, work remotely from time to time. That helps you to be productive, but it also increases risk from cyberthreats such as ransomware.

That's why we're adopting a new approach, called Zero Trust Access, for you to securely access corporate resources. Zero Trust Access complements VPN access, making it simpler for you to access certain corporate apps while providing increased security. Please enroll in Zero Trust Access promptly to continue accessing these applications without interruption.

The initial list of corporate applications that will be available using Zero Trust Access includes (*insert apps for initial rollout*). We will share further updates as more applications are made available through Zero Trust Access.

How to enroll

Zero Trust Access is a software component of Cisco Secure Client that is already installed on your company device. To enroll in Zero Trust Access, follow these steps:

1. Open the Cisco Secure Client window.
    - If you can't find the window, try searching for **Secure Client**.
2. In the Zero Trust Access section, click **Enroll**.
3. Enter your company email address.
4. Sign in using your SSO credentials.

Result: You are now enrolled in Zero Trust Access. Depending on IT security requirements, you may be asked to authenticate from time to time to continue accessing certain applications.

Need enrollment help? Contact the IT help desk.

If you choose to send the text as an email to end users, follow these instructions:

Procedure

1. Create an email list of users for whom you have provisioned the prerequisites.
2. Customize the text as desired.

- In particular, look for the "insert apps for initial rollout" section of the text. Replace that section with the applications that are available for your organization using Zero Trust Access.

3. Send the email to your list of users.

Troubleshoot Client-Based Zero Trust Access

Describes Troubleshoot Client-Based Zero Trust Access in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- Pre-Enrollment Errors
- Enrollment Errors
- Post-Enrollment Errors
- Requests to Reauthenticate

Pre-Enrollment Errors

Describes Pre-Enrollment Errors in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Error	Description	Condition
Cannot begin enrollment	Cannot begin enrollment. Contact your IT help desk about these errors.	Occurs when there is a KDF, DHA, or TPM error or some combination.
Device registration error	An issue with the Device Desktop occurred. Contact your IT help desk.	Occurs when Duo desktop is not installed, is not running, or is non-responsive. The user is asked to ensure that the app is running or contact IT help desk for assistance.
Server certification error	Error initiating enrollment	Client is unable to verify the proxy server certificate.
Cannot connect to DHA		Occurs when the client is unable to communicate with the Device Health application because DHA is not installed. **Note** Not applicable for devices running Linux operating system.

Enrollment Errors

Describes Enrollment Errors in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Error	Description	Condition
Certification enrollment error		Occurs when the certificate does not install in the background during enrollment. The certificate is required for Zero Trust Access to work properly.
No network connection		Occurs when the user doesn't have an active or working internet connection (wired or wireless).
User auth error during enrollment	Error initiating enrollment. Contact your IT help desk.	Occurs when the user has provided an invalid email address or password (or both). The system is unable to verify the user's credentials.

Post-Enrollment Errors

Describes Post-Enrollment Errors in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Error	Description	Condition
Network not allowed	Your organization requires you to be on an authorized network to log in.	Occurs when a private resource is not configured to allow Zero Trust access. Also occurs when the destination is not a configured private resource, but rather is an IP address that was typed directly into an access rule.
User IP address block	Your organization requires you to be on an authorized network to log in.	Occurs when the system is configured to allow access only from specific IP addresses, and the user is trying to access private resources from an unapproved IP address.
Application blocked for everyone	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user did not match any rule and was blocked by default or when a rule was not created to allow access to the application.
User blocked implicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user did not match any rule and was blocked by default or when a rule was not created to allow the user access to the application either directly or via a group.
Time-based application block	You do not have permission to access this application at this time. Contact your IT help desk.	Occurs when the user does not match any rule and was blocked by default or the application does not allow access at this time.
User IP block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is using an unauthorized device to access; the user's credentials aren't associated with the IP or with that device.

Error	Description	Condition
User blocked explicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is blocked by a rule that denies access or when the user does not have permission to connect or access the resource.
Access protocol block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	User does not have permission to connect to the resource using the current protocol.
User location block	Location is not allowed.	Occurs when the user did not match any rule and is blocked by default or when the user is not allowed access to the application from their current location.
Cannot connect to DHA		Occurs when there is no response when the client tried to communicate with DHA. **Note** Not applicable for devices running Linux operating system.

Requests to Reauthenticate

Describes Requests to Reauthenticate in Cisco Secure Access. If an end user is offline for an extended time, for example on vacation, Secure Access may prompt the user to reauthenticate in order to restore access to private resources.

If an end user is offline for an extended time, for example on vacation, Secure Access may prompt the user to reauthenticate in order to restore access to private resources. This is normal and expected.

Unenroll a Device from Zero Trust Access

Describes Unenroll a Device from Zero Trust Access in Cisco Secure Access. For certificate based enrollment remove the enrollment configuration file from the device.

Immediately unenroll a device

1. For certificate based enrollment remove the enrollment configuration file from the device. For file location, see Enroll Devices in Zero Trust Access Using Certificates.
2. To remove SAML based ZTA enrollment from the user's device see: Unenroll Devices for Client-Based Zero Trust Access.

Permanently unenroll a device

To revoke Zero Trust Access for a device and prevent re-enrollment, perform the following steps in order:

1. Remove the user from the identity provider. (This may take up to 30 minutes to take effect.)
2. Unenroll the user's device from Zero Trust Access here: Unenroll Devices for Client-Based Zero Trust Access.

Additional steps for certificate-based enrollment:

1. Remove the identity certificate from the user identity keystore on the device. This certificate may be used for multiple purposes, including VPN access.
2. Revoke the identity certificate on your Certificate Authority (CA).
3. Remove the enrollment configuration file from the device. For file location, see Enroll Devices in Zero Trust Access Using Certificates.

   If you do not perform all of these steps, the user may be able to re-enroll using the SSO authentication method.

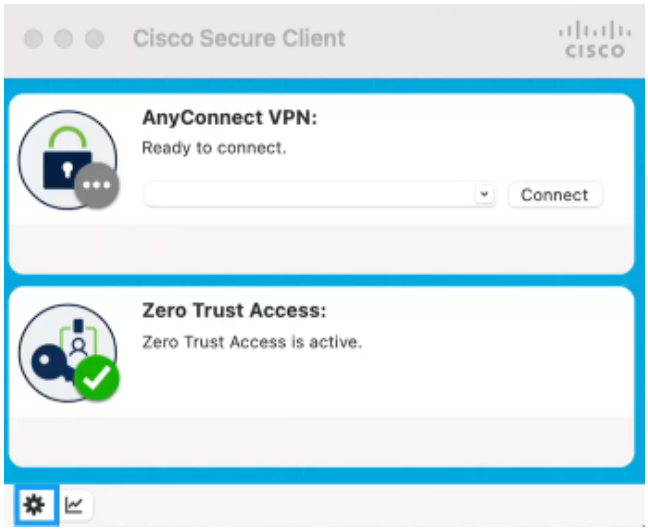
Unenroll from the user endpoint device (for enrollments using SSO Authentication only)

Describes Unenroll from the user endpoint device (for enrollments using SSO Authentication only) in Cisco Secure Access and explains On Windows devices, On macOS devices, and On Linux devices. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

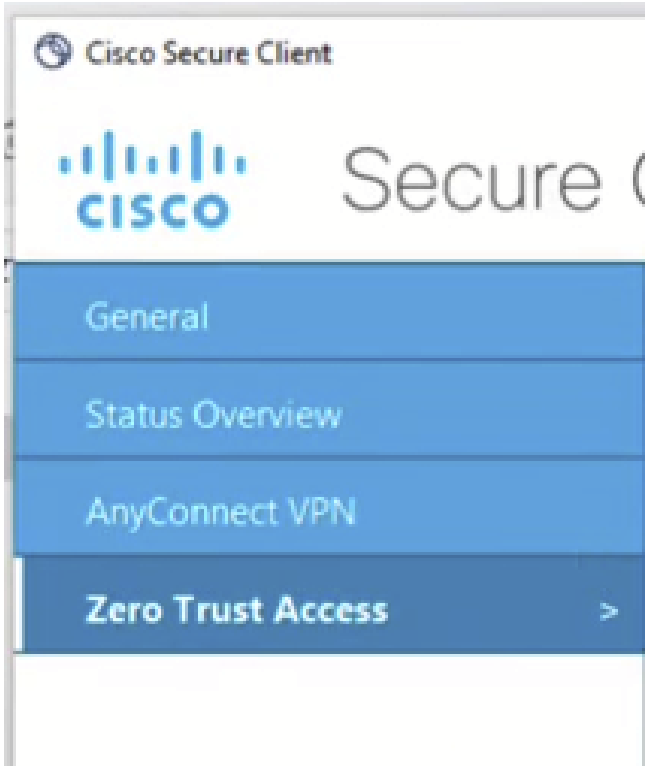
Administrator access is not required. Users can perform this action themselves. Users can re-enroll unless you perform the steps for permanent unenrollment, above.

On Windows devices

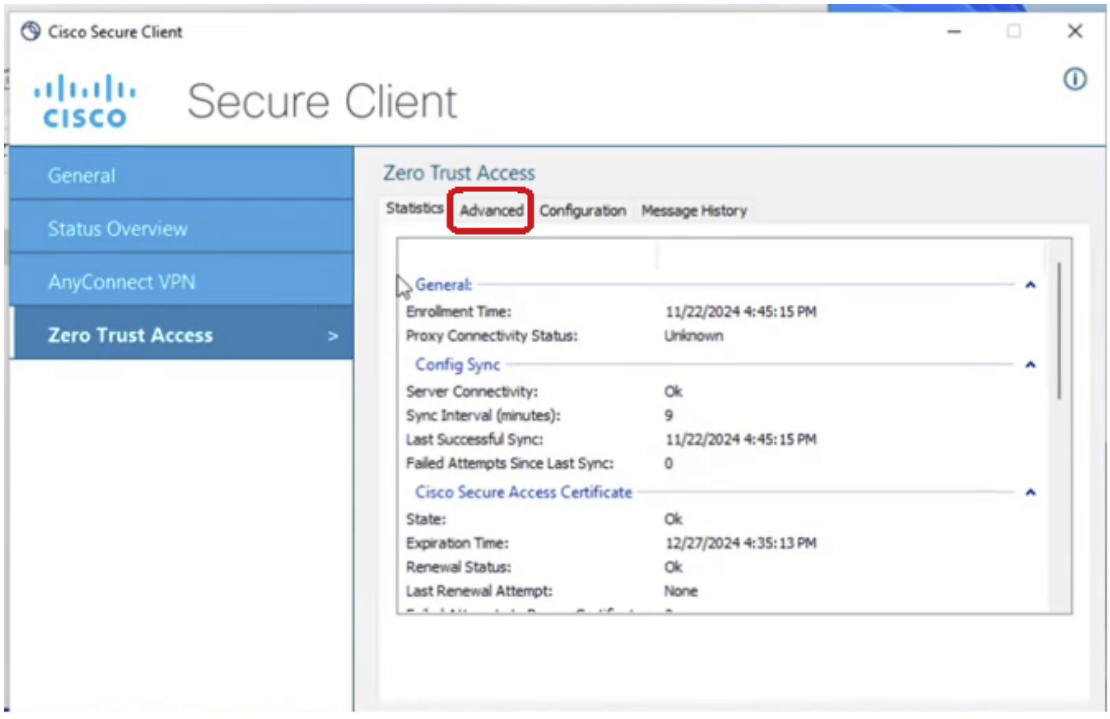
1. On the user endpoint device, launch Cisco Secure Client
2. Click the Advanced Window button:



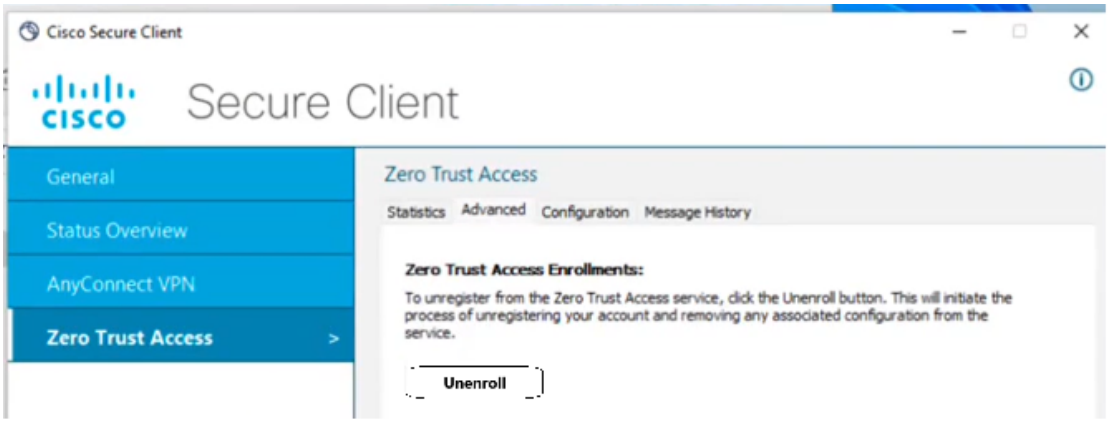
3. Click **Zero Trust Access**:



4. Click the **Advanced** tab:



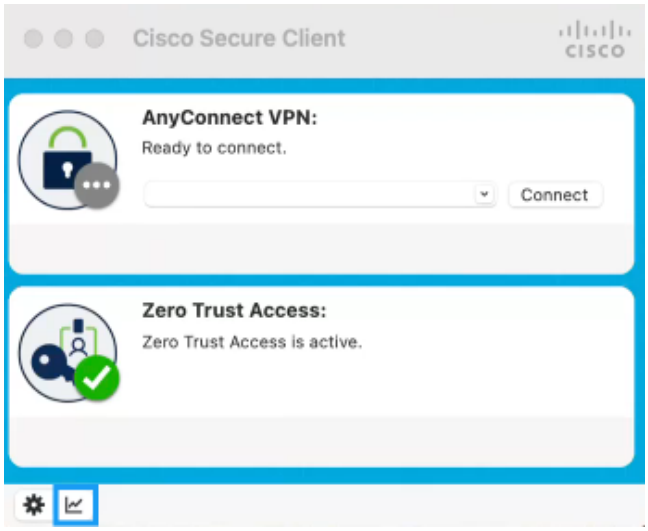
5. Click **Unenroll**.



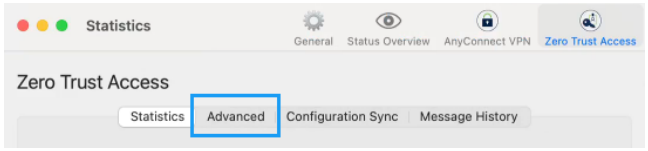
If the Unenroll button is not available and you see "This setting is managed by your administrator.", the device was enrolled using certificate-based enrollment and Administrator privileges are required to unenroll.

On macOS devices

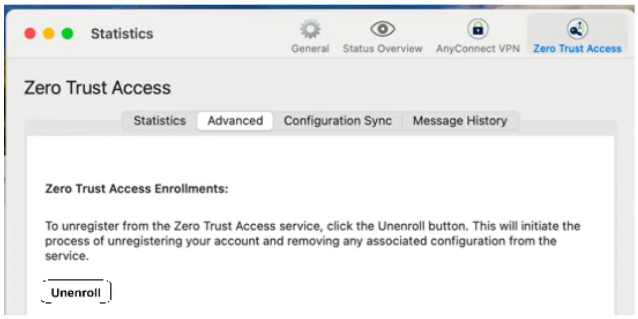
1. On the user endpoint device, launch Cisco Secure Client.
2. Click the Statistics button:



3. Click the **Advanced** tab.



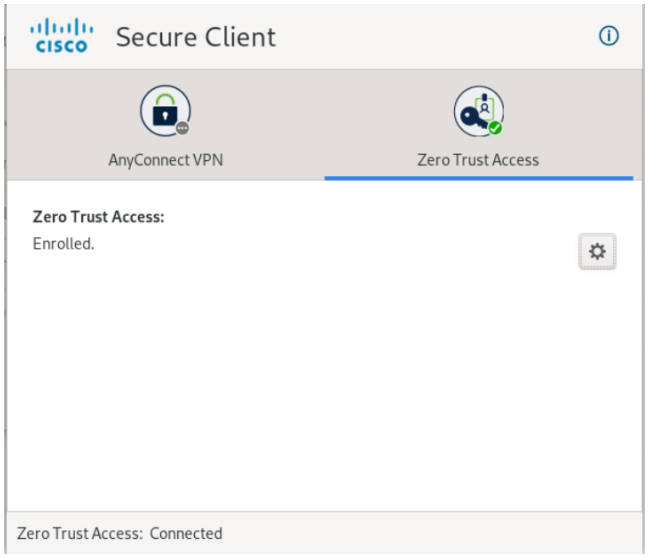
4. Click **Unenroll**.



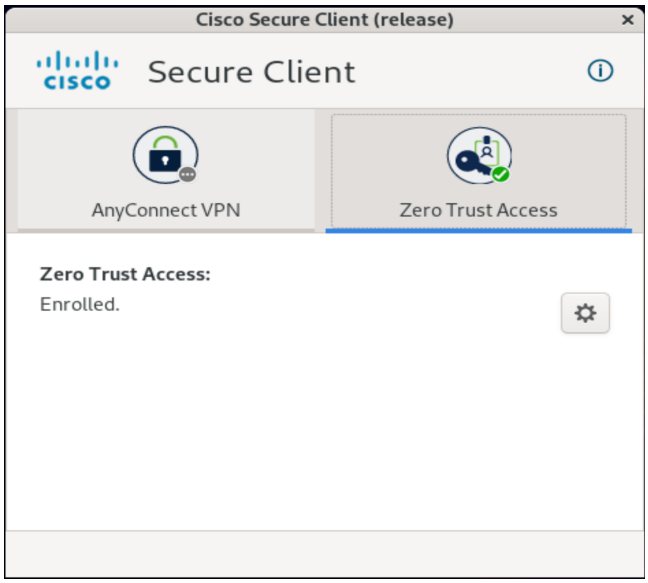
If the **Unenroll** button is unavailable and you see "This setting is managed by your administrator.", the device was enrolled using certificate-based enrollment and Administrator privileges are required to unenroll.

On Linux devices

1. On the user endpoint device, launch Cisco Secure Client.



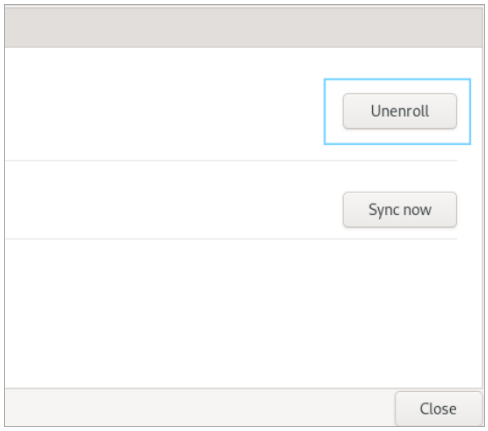
2. Click the **Details** icon.



3. Click the **Advanced** tab.



4. Click **Unenroll**.



If the **Unenroll** button is unavailable and you see "This setting is managed by your administrator.", the device was enrolled using certificate-based enrollment and Administrator privileges are required to unenroll.

60 Endpoint Data Loss Prevention using Cisco Secure Client

Topics:

- Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac
- Troubleshoot Endpoint Data Loss Prevention for Windows
- Troubleshoot Endpoint Data Loss Prevention for Mac
- Troubleshoot Endpoint Data Loss Prevention for Linux
- Deploying Cisco Secure Client – Endpoint DLP on macOS using a generic MDM
- Grant Required Privacy Permissions Using MDM
- Uninstall Cisco Secure Client - Endpoint DLP on macOS
- Uninstall Cisco Secure Client Endpoint DLP on Linux

Provides an overview of Endpoint Data Loss Prevention using Cisco Secure Client in Cisco Secure Access, including Manage Endpoint Data Loss Prevention using Cisco Secure Client and Troubleshoot Endpoint Data Loss Prevention. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Endpoint Data Loss Prevention Using Cisco Secure Client for Windows and Mac

This topic explains how Cisco Secure Client manages Endpoint Data Loss Prevention by controlling data transfers to external devices, ensuring sensitive data remains secure.

Cisco Endpoint Data Loss Prevention (Endpoint DLP) enables you to protect sensitive data on endpoints by controlling what data is transferred to external devices. It extends your organization's data protection policies to the endpoint. This ensures that sensitive data remains secure and compliant with your security requirements.

Key Capabilities for Windows

Endpoint DLP can prevent the exfiltration of the sensitive data through these endpoint channels:

- **USB drives and Network Shares (SMB)**: Blocks copy or move operations through Windows File Explorer (GUI) and common command-line (CLI) flows.
- **Bluetooth transfers**: Blocks file movement using Windows' default Bluetooth transfer utility.
- **Printers**: Prevents printing of sensitive data on both local and network printers.
- **Paste to Applications**: Prevents users from pasting sensitive data into specified applications.
- **Application File Access**: Prevents specified applications from opening files that contain sensitive data.
- **Media/Portable Devices**: Prevents sensitive files from being exfiltrated to Android phones and cameras.

Key capabilities for Mac

Endpoint DLP can prevent the exfiltration of the sensitive data through these endpoint channels:

- **USB drives and network shares (SMB, NFS)**: Blocks copy or move operations.
- **Bluetooth transfers**: Blocks file transfers using the macOS Bluetooth File Exchange app.
- **Printers**: Applies data protection policies to local, network, AirPrint, and direct USB printing workflows.
- **AirDrop transfers**: Block sensitive files from being transferred using AirDrop.
- **Paste to Applications**: Prevents users from pasting sensitive data into specified applications.

Key capabilities for Linux

Endpoint DLP can prevent the exfiltration of the sensitive data through these endpoint channels:

- **USB drives and network shares (SMB, NFS)**: Blocks copy and move operations through Nautilus (Gnome File Explorer) and common command-line (CLI) flows.
- **Printers**: Applies data protection policies to jobs processed through the local CUPS service, including jobs sent to local, network, and USB-connected printers.

Known limitations for Mac

- Bluetooth support is only available through the Apple Bluetooth File Exchange.
- During multi-file transfers, the entire transfer is canceled if one or more files are sensitive.
- Paste to Applications evaluates supported text and image content. Files placed on the clipboard as file items are not evaluated by this destination.

Known limitations for Linux

- Application **Save As** operations that stream content directly to a GIO or GVFS network URI might not be scanned. Operations to supported mounted file system paths are blocked.
- Printer support is limited to scanning the print spool contents. Files with sensitive filenames or sensitivity label warnings can be printed if their contents are safe.

How to Use Endpoint Data Loss Prevention

1. **Provision Users** - Only provisioned users can enroll to Endpoint DLP. Configure identity providers using the Cisco Secure Access dashboard. For more information, see configure identity providers.
2. **Enroll Devices in Endpoint DLP** - Enroll before Endpoint DLP module can prevent data loss. For more information about enrollment, see Enroll Devices in Endpoint DLP using Certificates.
3. **Configure Policy** - Define and manage Endpoint DLP rules using the Cisco Secure Access dashboard. The Real Time DLP rules specify which types of data transfers are allowed, blocked, monitored or allowed with justification, to provide visibility into endpoint data movement and enabling consistent enforcement across your organization's devices.
4. **Global Settings** - Endpoint DLP operates directly on the endpoint device to protect data before it leaves. You can maintain data protection when users are offline or connected outside the corporate network. For more information, see Global Settings.

Prerequisites for Endpoint Data Loss Prevention

This concept explains in detail the minimum system and network prerequisites for deploying Endpoint DLP effectively.

Currently, Endpoint DLP supports Windows, Mac and Linux systems. Ensure your system meets the minimum requirements to install Endpoint DLP.

Ensure your system meets the minimum requirements to install Endpoint DLP.

System Requirements for Windows

The minimum system requirements include:

- Operating System:
  - Version: Windows 11 (x64), Windows Server 2025 (x64) Standard (Std) and Datacenter (DC)
  - Release: 23H2 or later
  - Architecture: AMD64 or Intel 64 only
- CPU: Dual Core
- RAM: 4 GB
- Hard Disk capacity: 64 GB, with at least 1 GB of free space available
- Trusted Platform Module (TPM) 2.0

The recommended system requirements are:

- CPU: Quad Core
- RAM: 8 GB

System Requirements for macOS

The minimum system requirements include:

- Operating System:
  - Versions: macOS 15, macOS 26, macOS 27
  - Architecture: Apple Silicon ARM64 processors
- Disk space: At least 1 GB of free disk space available
- Mac devices must support Secure Enclave

System Requirements for Linux

The minimum system requirements include:

- Operating System:
  - Red Hat Enterprise Linux 9.x and 10.x
  - Ubuntu 22.04 LTS, 24.04 LTS, and 26.04 LTS
- Architecture: AMD64 or Intel 64 only
- CPU: Dual Core
- RAM: 4 GB
- Hard Disk capacity: At least 1 GB of free disk space
- Single local graphical session (SSH-only, headless, and multi-user sessions will defer enrollment).

Network Requirements

Endpoint DLP module connects to the Secure Access cloud to enroll, sync configuration, and scan data for sensitive content.

- Domains to allow: The following domains must be reachable by the Endpoint DLP module for proper functioning.
  - *.sse.cisco.com
  - *.api.umbrella.com
- Ports to allow: HTTPS:443
- Healthcheck URL: www.cisco.com

> **Note**
>
> To use Endpoint Data Loss Prevention, create at least one Real Time DLP policy.

If using other Cisco Secure Access modules for traffic acquisition, ensure these domains and their subdomains are bypassed to avoid conflicts on policy enforcement.

`dlpaas.dlp.sse.cisco.com`

For more information, see Manage Internet Security Bypass.

Enroll Devices in Endpoint Data Loss Prevention Using Certificates

This concept explains various steps involved in enrolling devices in Endpoint Data Loss Prevention using certificates.

Install Endpoint DLP without user intervention (zero-touch deployment) using these steps:

- Check Prerequisites for Endpoint Data Loss Prevention on page 2042.
- On user devices:
  - Step 1 - Upload or choose a CA certificate
  - Step 2 - Download installer
  - Step 3 - Download the Endpoint DLP enrollment choice file
  - Step 4 - Install the User Certificate and Enrollment Choice File on User Devices on page 2049
  - Step 4a - Install the User Certificate and Enrollment Choice File on User Devices for Windows on page 2049
  - Step 4b - Install the User Certificate and Enrollment Choice File on User Devices for macOS on page 2049
  - Step 4c - Install the User Certificate and Enrollment Choice File on User Devices for Linux on page 2050

Enrollment

Enrollment is a multi-step process. The process starts with the availability of the choice file and mutual trust between the Endpoint DLP module and the server. After device registration, the Secure Access cloud provisions a Cisco-signed certificate, which binds the end user and the target device. The generated certificate will be persisted in the target device.

Note

- It is not possible to unenroll the Endpoint DLP module from a device.
- Periodic enrollment renewal is automatic if requirements are met.

The Endpoint DLP module stores successful enrollments at the following location:

```
%ProgramData%\\Cisco\\Cisco Secure Client\\EDLP\\enrollments
```

Note

Ensure that you do not tamper with the contents of this or the parent folder.

The Endpoint DLP module stores successful enrollments at the following location for Mac and Linux :

```
/opt/cisco/secureclient/edlp/enrollments
```

Note

Ensure that you do not tamper with the contents of this or the parent folder.

The Endpoint DLP module synchronizes with the Secure Access cloud. During synchronization, the client shares its information, status, and metrics. The cloud returns configuration information such as fail-open or fail-close. This configuration can change the state of Endpoint DLP.

Step 1 - Upload or Choose a CA Certificate

Use this procedure to upload a CA certificate required for user identity verification during enrollment and renewal.

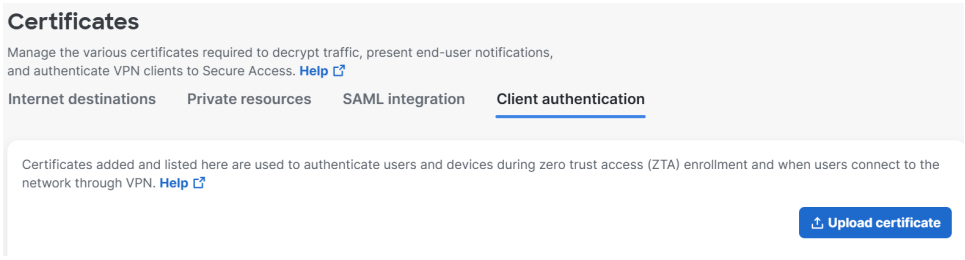
During enrollment and renewal, user endpoint devices present an identity certificate. Secure Access requires the certificate to verify user identity certificates. You can upload a new certificate or choose an existing certificate.

You can use the same certificate for Endpoint DLP enrollment that validates identity certificates for VPN connections or ZTA, or choose a different one. You specify the purposes for each certificate during upload, and update the purpose later if needed.

To upload the certificate:

Procedure

1. Navigate to **Connect** > **End User Connectivity**.
2. Click the **Client Authentication** tab.
3. Click **Upload a CA Certificate**.



> **Note**
>
> Before you upload a CA certificate, ensure you include the intermediate certificates required to establish a chain of trust.

4. In the **Upload Certificate** dialog, choose the root CA file you want to upload. Optionally, you can drag and drop the root CA.
5. Check the **Endpoint DLP Enrollment** check box to enable user certificate verification with the uploaded root CA.
6. Click **Save** to save the root CA and the configuration.

   The Certificate list displays all the uploaded root CAs. The **Purpose** column indicates whether the root CA was chosen for EDLP, ZTA,VPN, or a combination.

> **Note**
>
> - Ensure at least one root CA is selected for Endpoint DLP to ensure successful enrollment.
> - Use the same root CA to sign the identity (bootstrap) certificate.
> - The identity (bootstrap) certificate may be shared between ZTA, RAVPN, and EDLP when using the same root CA. Separate user certificates for each are not required.

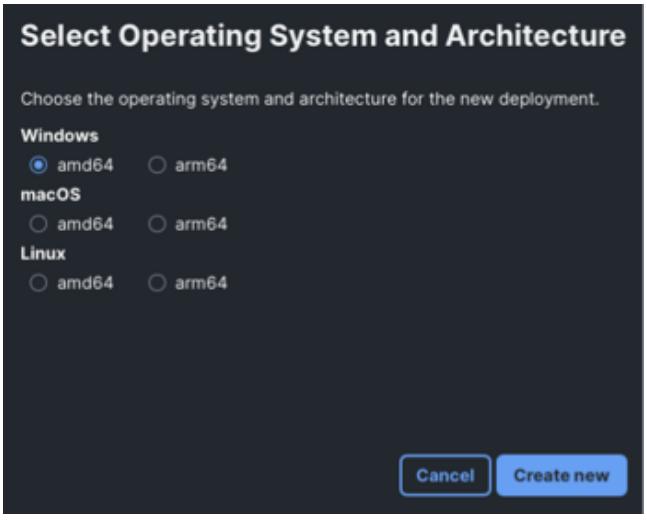
Step 2 - Centralized Deployment and Management of Endpoint Data Loss Prevention

Use this procedure to deploy Endpoint DLP using Cisco Secure Client Management.

You can create and manage deployments of Endpoint DLP using Cisco Secure Client Management. Deployments include selecting various modules (for example, Endpoint Data Loss Prevention, Secure Client, Secure Endpoint) and associating profiles that configure each module. For more information, see SCCM.

Procedure

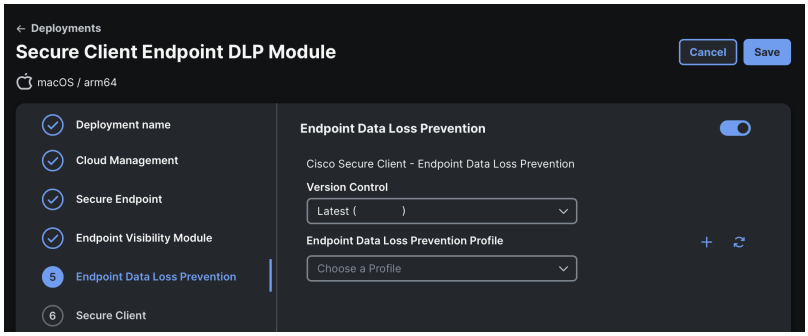
1. Sign in to the Secure Client Management portal (https://apps.security.cisco.com) .
2. Under **Applications**, navigate to your region and click **Secure Client Management**.
3. Create a Secure Client package which includes the Endpoint DLP module or update an existing package to include the Endpoint DLP module.
   a. Create a deployment for Windows AMD64.
   b. Click **Create New** to create a new deployment or edit an existing one if you had previously created a deployment.
   c. Select **amd64** and click **Create New**.
   d. Enter a name for the deployment.
   e. Include the Endpoint DLP module with other desired modules.
   f. For each module that is selected above, you can optionally add the necessary configuration file(s) or profiles downloaded from the corresponding Secure Access dashboard pages. If not already downloaded, see Configuration for downloading EDLP choice file.
   g. Save the Deployment.
4. Create or update a Secure Client package to include the Endpoint DLP module:
   a. In the Secure Client Management portal, click **Create New** to create a new deployment, or edit an existing deployment.
   b. Enter a name for the deployment.
   c. Under the Windows section, select **amd64**. Under the macOS section, select **arm64**. Under the Linux section, select **amd64**



   d. Add the Endpoint DLP module and any other required modules to the package.

e. For each selected module, optionally add configuration files or profiles downloaded from the Secure Access dashboard pages. If you have not already downloaded these files, see the configuration instructions for downloading the Endpoint DLP choice file.

f. Click **Save** to save the deployment.



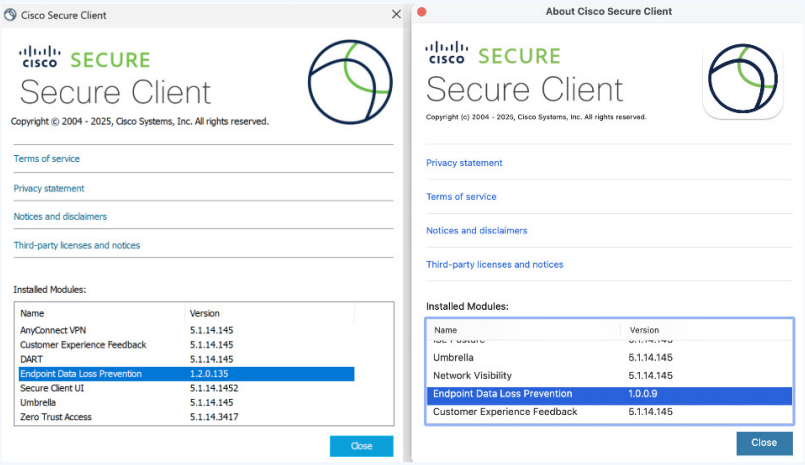
> **Note**
>
> Endpoint DLP supports only Windows (amd64), macOS (arm64) and Linux (amd64) distributions. Intel-based Macs, Windows or Linux on ARM64 are not supported.

5. Download the installer based on your requirement.

Two types of installers are available:

- **Network Installer**: A light-weight installer installs the Cloud Management client first, then automatically downloads and installs other modules and configurations in the background.
- **Full Installer**: A comprehensive package containing all selected modules and profiles for complete installation on endpoints.

> **Note**
>
> After installing the Endpoint DLP module, it does not appear as a tile in Cisco Secure Client. Confirm the installation and check the module version from the **About** dialog box in Cisco Secure Client.



Step 3 - Download the Enrollment Choice File

Use this procedure to learn about choice file and how to download it for Endpoint DLP enrollment.

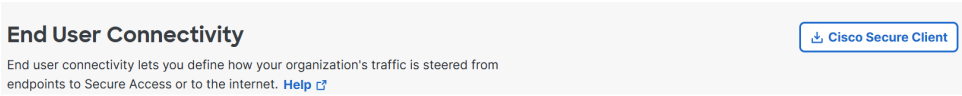
Before you download the choice file, upload the CA certificate to validate the identity certificate presented by a device during enrollment and renewal. Each time a CA certificate is uploaded for Endpoint DLP enrollment, the choice file is regenerated. The choice file includes information about all CA certificates you have uploaded and designated for Endpoint DLP enrollment.

The choice file name is ***orgID*_EDLP_Enroll_Cert.json**.

To download the choice file:

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Cisco Secure Client**.



2. Click **Download** next to **For Endpoint DLP Devices Security module: <org_id>_EDLP_Enroll_Cert.json** to download the choice file for Endpoint DLP enrollment.

> **Note**
>
> The choice file applies to all devices in the organization. Transfer it to the target devices using MDM, UEM, or Windows Group Policy.

Step 4 - Install the User Certificate and Enrollment Choice File on User Devices

The Endpoint DLP module uses information from the choice file to enroll itself to the Secure Access cloud using the user identity certificate and additional device information. Ensure you store the choice file in a secure location.

Step 4a - Install the User Certificate and Enrollment Choice File on User Devices for Windows

This concept explains the role and installation of user certificates and enrollment choice files in securing devices accessing Secure Access cloud.

To prevent tampering, the choice file is installed in a directory that requires Administrator access, and the file is signed. Do not attempt to modify it.

Install the User Certificate

Provision the user certificate on to the User Certificate store and ensure it contains an associated private key. Use a protocol like SCEP for provisioning the user certificate.

Each device must have an identity certificate signed by your corporate certificate signing authority (CA). The identity certificate must be associated with a specific user, not the device.

The Endpoint DLP module evaluates certificates if the Issuer Common Name matches any enabled CA certificates in the EDLP enrollment dashboard. If multiple identity certificates share the same Common Name, the client selects the first matching certificate.

- Include the user's RFC 822-compliant email address in the Subject Alternative Name (SAN) certificate or include the username in the User Principal Name (UPN) field.
- Install the identity certificate in the machine or user-specific keystore on each device.

Install the Enrollment Choice File

Install the choice file on each user device in this location:

- On Windows devices: `%ProgramData%\\Cisco\\Cisco Secure Client\\EDLP\\enrollment_choices`

If a CA certificate expires or is replaced, deleted, or revoked, you must distribute a new choice file to authorized devices with information about the replacement CA certificate.

You can change the file name, but you can have only one EDLP enrollment choice file on the device.

Step 4b - Install the User Certificate and Enrollment Choice File on User Devices for macOS

This concept explains the role and installation of user certificates and enrollment choice files for securing devices that access Secure Access cloud.

On macOS, you need administrator (elevated) privileges to access the folder.

Install the User Certificate

On macOS install the user certificate the user's login keychain.

On macOS, your app must be able to access the enrollment certificate.

If MDM system pushes the certificate, enable private key access for all apps in the MDM configuration portal. Select **Allow all app access**. This setting prevents prompts during auto enrollment.

If you manually import the certificate, run command line steps to allow your app to access the private key without macOS prompts.

Follow this procedure to allow Endpoint DLP on macOS to read the certificate from the Login keychain.

Procedure for macOS

1. Import the client certificate: `security import "PATH_To_CLIENT_CERT" -k ~/Library/Keychains/login.keychain-db -x -A`
2. Set the correct partition list: `security set-key-partition-list -S teamid:DE8Y96K9QP -l "PRIVATE_KEY_LABEL" -t private`

Install the Enrollment Choice File

Install the enrollment choice file on each device at this location.

- On Mac devices: `/opt/cisco/secureclient/edlp/enrollment_choices`

If a certificate authority (CA) certificate expires, or is replaced, deleted, or revoked, distribute a new choice file to authorized devices. The new file must include information about the replacement CA certificate .

You can change the file name, but you can have only one EDLP enrollment choice file on the device at a time.

Step 4c - Install the User Certificate and Enrollment Choice File on User Devices for Linux

This concept explains the role and installation of user certificates and enrollment choice files for securing devices that access Secure Access cloud.

On Linux, you need administrator (elevated) privileges to access the folder.

Install the User Certificate

On Linux the user certificate is installed to the user's home directory under `"~/.cisco/certificates"` folder. Install the user certificate by copying the client certificate and private key to the following paths.

- `~/.cisco/certificates/client/<user_certificate.pem>`
- `~/.cisco/certificates/client/private/<user_certificate.key>`

Install the Enrollment Choice File

Install the enrollment choice file on each device at this location:

- `/opt/cisco/secureclient/edlp/enrollment_choices/`

If a certificate authority (CA) certificate expires, or is replaced, deleted, or revoked, distribute a new choice file to authorized devices. The new file must include information about the replacement CA certificate .

You can change the file name, but you can have only one EDLP enrollment choice file on the device at a time.

Troubleshoot Endpoint Data Loss Prevention for Windows

This concept provides information about the location of the Endpoint DLP logs on the endpoint device and various enrollment errors.

Use the following tips to troubleshooting Endpoint Data Lose Prevention issues:

Endpoint Data Loss Prevention Logs

The Endpoint DLP logs are stored at this location on the endpoint device:

Windows:

```
%ProgramData%\\Cisco\\Cisco Secure Client\\EDLP\\logs
```

Pre-Enrollment Errors

Use the following table to troubleshoot errors encountered before you enroll:

Error	Description	Condition
Cannot begin enrollment	Cannot begin enrollment. Contact your IT help desk for error information.	Occurs when there is a TPM error.
Device registration error	An issue with the Device Desktop occurred. Contact your IT help desk for assistance.	Occurs when Duo desktop is not installed, is not running, or is non-responsive. The user is asked to ensure that the app is running or contact IT help desk for assistance.
Server certification error	Error initiating enrollment	Client is unable to verify the proxy server certificate.

Enrollment Errors

Use the following table to troubleshoot errors encountered as you enroll:

Error	Description	Condition
Certification enrollment error		Occurs when the certificate does not install in the background during enrollment. The certificate is required for Endpoint DLP to work properly.
No network connection		Occurs when the user doesn't have an active or working internet connection (wired or wireless).
Missing Choice File		Occurs when the the choice file downloaded from the Secure Access dashboard is not pushed to the target device and is not available at the location `C:\ProgramData\Cisco\Cisco Secure Client\EDLP\enrollment_choices`
Missing Identity (aka bootstrap or user) Certificate		Occurs when the identity certificate is not available on the device cert store.
Expired Identity Certificate		Occurs when the identity certificate is not valid during and after enrollment. Expired certificates lead to enrollment failure or if certificate expires after enrollment then existing enrollment will be removed.
Unsigned Identity Certificate		Occurs when the identity certificate is not signed by the same root CA uploaded into secure access dashboard and marked for EDLP. For more information, see Upload a Root CA.

Error	Description	Condition
User Not Provisioned		Occurs when the user for which enrollment is failing is not provisioned in your secure access org. View Users Provisioned in Secure Access
401 error messages during enrollment	Contact your IT help desk.	Occurs when the client lacks sufficient authorization.
56 error enrollment processing failed		Occurs when the root CA certificate is not uploaded and enabled for Endpoint DLP.
Trusted Platform Module (TPM) is unavailable		Occurs when the TPM is unavailable.
Expired or Invalid or Revoked Secure Access Certificate		Occurs when the secure access certificate is not valid during and after enrollment. Expired or revoked certificates will lead to deletion of enrollments.
Timeouts		Occurs when the domains mentioned under the networking requirements are not allowed in your network firewall and that the destinations are not reachable.

Post-Enrollment Errors

Use the following table to troubleshoot errors encountered after you enroll:

Error	Description	Condition
Intelligence mode disabled	Cloud intelligence is unavailable during a network failure.	Unable to establish connections with the server.
Unable to see notifications	Notifications on event triggers are not seen on endpoint devices.	Ensure system notifications are enabled or Focus mode is off. Additionally, ensure **Pop up Notifications** option is enabled in the applicable policies.
Network not allowed	Your organization requires you to be on an authorized network to log in.	Occurs when a private resource is not configured to allow Endpoint DLP. Also occurs when the destination is not a configured private resource, but rather is an IP address that was typed directly into an access rule.
User blocked explicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is blocked by a rule that denies access or when the user does not have permission to connect or access the resource.
Access protocol block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	User does not have permission to connect to the resource using the current protocol.

Error	Description	Condition
User location block	Location is not allowed.	Occurs when the user did not match any rule and is blocked by default or when the user is not allowed access to the application from their current location.

Troubleshoot Endpoint Data Loss Prevention for Mac

This concept describes how to locate Endpoint DLP logs and troubleshoot common enrollment errors on macOS devices.

Pre-Enrollment Errors

Error	Description	Condition
Cannot begin enrollment	Cannot begin enrollment. Contact your IT help desk about these errors.	Occurs when there is a TPM error .
Device registration error	An issue with the Device Desktop occurred. Contact your IT help desk.	Occurs when Duo desktop is not installed, is not running, or is non-responsive. The user is asked to ensure that the app is running or contact IT help desk for assistance.
Server certification error	Error initiating enrollment	Client is unable to verify the proxy server certificate.

Enrollment Errors

Error	Description	Condition
Certification enrollment error		Occurs when the certificate does not install in the background during enrollment. The certificate is required for Endpoint DLP to work properly.
No network connection		Occurs when the user doesn't have an active or working internet connection (wired or wireless).
Missing Choice File for Windows		Occurs when the the choice file downloaded from the Secure Access dashboard is not pushed to the target device and is not available at the location `C:\ProgramData\Cisco\Cisco Secure Client\EDLP\enrollment_choices`
Missing Choice File for mac		Occurs when the the choice file downloaded from the Secure Access dashboard is not pushed to the target device and is not available at the location `/opt/cisco/secureclient/edlp/enrollment_choices`

Error	Description	Condition
Missing Identity (aka bootstrap or user) Certificate		Occurs when the identity certificate is not available on the Login Keychain.
Expired Identity Certificate		Occurs when the identity certificate is not valid during and after enrollment. Expired certificates lead to enrollment failure or if certificate expires after enrollment then existing enrollment will be removed.
Unsigned Identity Certificate		Occurs when the identity certificate is not signed by the same root CA uploaded into secure access dashboard and marked for EDLP. See section Upload a Root CA.
User Not Provisioned		Occurs when the user for which enrollment is failing is not provisioned in your secure access org. View Users Provisioned in Secure Access
401 error messages during enrollment	Contact your IT help desk.	Occurs when the client lacks sufficient authorization.
Trusted Platform Module (TPM) is unavailable		Occurs when the TPM is unavailable.
Expired or Invalid or Revoked Secure Access Certificate		Occurs when the secure access certificate is not valid during and after enrollment. Expired or revoked certificates will lead to deletion of enrollments.
Timeouts		Occurs when the domains mentioned under the networking requirements are not allowed in your network firewall and that the destinations are not reachable.

Post-Enrollment Errors

Error	Description	Condition
Network not allowed	Your organization requires you to be on an authorized network to log in.	Occurs when a private resource is not configured to allow Endpoint DLP. Also occurs when the destination is not a configured private resource, but rather is an IP address that was typed directly into an access rule.
User blocked explicitly	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	Occurs when the user is blocked by a rule that denies access or when the user does not have permission to connect or access the resource.
Access protocol block	Location not allowed. Your organization requires you to use a different operating system. Contact your IT help desk.	User does not have permission to connect to the resource using the current protocol.

Error	Description	Condition
User location block	Location is not allowed.	Occurs when the user did not match any rule and is blocked by default or when the user is not allowed access to the application from their current location.

Extract and Stream Logs for Cisco Secure Client - Endpoint DLP on macOS

This concept explains how to extract and stream logs for Cisco Secure Client - Endpoint Data Loss Prevention (DLP) on macOS using the Unified Logging System.

This document explains how to extract and stream logs for **Cisco Secure Client - Endpoint DLP** on macOS.

Overview

macOS uses the **Unified Logging System**, which can be accessed using the log CLI utility.

You can use two primary commands:

- log show → Extract **historical logs**
- log stream → View **live / real-time logs**

Filtering uses a **predicate**, typically by subsystem or optionally by category.

Historical Logs (log show)

Use the *log show* command to view past logs. You can filter by time window and subsystem.

```
log show --style syslog --info --predicate 'subsystem ==
"com.cisco.secureclient.edlp"' --last 1h
```

Example time filters:

--last 30m → last 30 minutes

--last 2h → last 2 hours

--last 1d → last 1 day

Specify explicit time ranges:

```
log show --style syslog --info --predicate 'subsystem ==
"com.cisco.secureclient.edlp"' \
  --start "2026-03-10 10:00:00" \
  --end   "2026-03-10 11:00:00"
```

Live Logs (log stream)

Use *log stream* to monitor logs as they are generated.

```
log stream --style syslog --level info --predicate 'subsystem ==
"com.cisco.secureclient.edlp"'
```

Filter by Category (Optional)

A specific functional area, filter by category:

- **Core Agent Logs**

```
log stream --style syslog --level info --predicate 'subsystem ==
"com.cisco.secureclient.edlp" AND category == "agent"'
```

- **Enrollment Logs**

```
log stream --style syslog --level info --predicate 'subsystem ==
"com.cisco.secureclient.edlp" AND category == "csc_edlpenroll"'
```

When to Filter by Category

- Use **subsystem only** → When debugging full product behavior.
- Add **category filter** → When isolating issues in core agent or enrollment flows.

Logging Levels

Use different logging levels depending on your troubleshooting needs:

- **default** → Normal operational logging
- **info** → Standard troubleshooting
- **debug** → Deep troubleshooting (high volume)

> **Note**
>
> The *log show* command does not use --level flag. Use --info or --debug instead.

The *log stream* command supports both --level info and --level debug options.

Enable debug logging:

In addition to specifying the appropriate debug flag, you must update the config.ini file to enable debug logging.

Open

```
 /opt/cisco/secureclient/edlp/etc/config.ini
```

```
[logger]
level = info
```

Change the value under [logger] from level = info to level = debug. Save the file and restart the Endpoint DLP service.

Save Logs to a File

- **Save historic logs**

```
log show --style syslog --info --predicate 'subsystem ==
"com.cisco.secureclient.edlp"' --last 1h > edlp.txt
```

- **Stream and Save Live Logs**

```
log stream --style syslog --level info --predicate 'subsystem ==
"com.cisco.secureclient.edlp"' | tee edlp.log
```

Best Practices

- Use **subsystem-only filtering** for complete log capture.
- Add **category filtering** only when narrowing investigation scope.
- Use --level debug only when necessary.
- Always include a time window (--last) when using *log show* to avoid large outputs.
- Redirect logs to a file when collecting for support or bug reports.

Log Retention

On macOS, log retention is **not time-based**, but it is based on **size** and **storage size**.

Unified Logging system keeps in a rolling store and automatically older entries when:

- The log store reaches internal size limits.
- The system needs disk space.
- The Mac is rebooted (some transient logs may be lost).

  Retention depends on:

- System activity volume.
- Whether debug logging is enabled.
- Available disk space.
- macOS version.

High-volume debug logging can cause older logs to be replaced quickly. When you troubleshoot using debug logs, collect debug logs promptly to avoid losing important entries.

Log Type	Typical Retention
default, error, fault	Several days to weeks
info	Usually hours to a few days
debug	Often only hours (sometimes less under load)

Logging with the Console Application

Learn how to use the Console graphical user interface (GUI) application to stream and monitor logs in real time. This procedure guides you through leveraging the Console app for effective log streaming and live monitoring.

You can use the console graphical user interface (GUI) application on macOS to stream and monitor Endpoint DLP logs in real time.

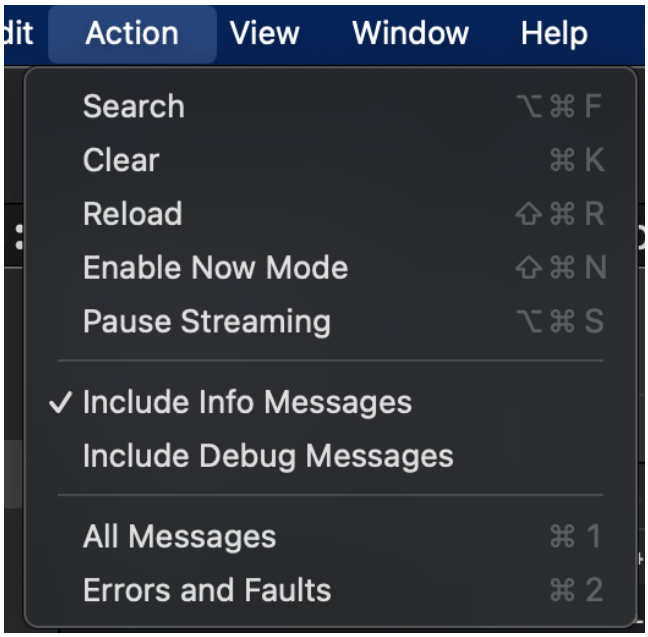
Procedure

1. Launch the **Console** application.
2. In the search bar at the top right, enter **“edlp”**.
3. By default, the search filter is set to **ANY**. Double-click on **ANY** to change it to **SUBSYSTEM.**



4. To view **Info or Debug Messages**, from the **Action** menu, choose **Include Info Messages** or **Include Debug Messages**.
5. You can add additional keyword searches for a category or specific keywords if you are looking for a particular log line.

> **Note**
>
> By default, the console application does not display info or debug level logging. To enable these, select **Action** in the top menu bar and choose **Include Info Messages** or **Include Debug Messages**.



> **Note**
>
> Logs streamed in the console application are not retained indefinitely and may disappear after some time. To save logs for later review, use the command line **log stream** command and redirect output to a file.

Troubleshoot Endpoint Data Loss Prevention for Linux

This concept describes how to locate Endpoint DLP logs and troubleshoot common enrollment errors on Linux devices.

Log files: You can find log files for EDLP for Linux under the directory:

- `/var/log/cisco/secureclient/edlp`
- `~/.cisco/secureclient/edlp/logs`

> **Note**
>
> For information about specific log message errors and debugging procedures on Linux, see Troubleshoot Endpoint Data Loss Prevention for Windows on page 2050 and Troubleshoot Endpoint Data Loss Prevention for Mac on page 2053.

Deploying Cisco Secure Client – Endpoint DLP on macOS using a generic MDM

This concept explains the administrative workflow for deploying Cisco Secure Client - Endpoint DLP on macOS via Mobile Device Management.

This section describes steps for administrators to deploy Cisco Secure Client – Endpoint Data Loss Prevention (DLP) on macOS devices.

MDM Profiles

Deploy Cisco Secure Client – Endpoint DLP on macOS using a Mobile Device Management (MDM) profile that grants the required approvals. Install the MDM profiles before you install, upgrade, or remove the Mac connector to ensure you obtain the required permissions.

Approval of the Endpoint DLP Service

The Endpoint DLP service requires Full Disk Access to monitor the file system for sensitive data. The service cannot function without this approval. This approval can be granted manually or through MDM.

The Endpoint DLP service requires Accessibility permissions to monitor the clipboard for sensitive data. The service cannot function without this approval. This approval can be granted manually or through MDM.

Grant Required Privacy Permissions Using MDM

This concept describes how to use Mobile Device Management (MDM) to deploy a Privacy Preferences Policy Control (PPPC) payload, and enable Full Disk Access for the Cisco Secure Endpoint DLP service on macOS devices to ensure it operates with the required system-level permissions.

You can grant Full Disk Access to the Cisco Secure Endpoint DLP service on macOS by deploying an MDM management profile that includes a Privacy Preferences Policy Control (PPPC) payload. This payload must specify the `SystemPolicyAllFiles` property with the required entries for the services.

> **Note**
>
> A reboot is not required after you grant Full Disk Access.

Property	Value
Allowed	true
CodeRequirement	anchor apple generic and identifier "com.cisco.secureclient.edlp.app" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ *or certificate 1[field.1.2.840.113635.100.6.2.6]* / exists / *and certificate leaf[field.1.2.840.113635.100.6.1.13]* / exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)

Property	Value
Identifier	com.cisco.secureclient.edlp.app
IdentifierType	bundleID

Clipboard paste protection runs in the user context through the Endpoint DLP User Agent. To avoid local TCC prompts on managed devices, the same PPPC profile should also approve the user agent for 'Accessibility' and 'ListenEvent'.

Property	Value
Allowed	true
CodeRequirement	anchor apple generic and identifier "com.cisco.secureclient.edlp.useragent" and *(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists **/ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */* and *certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */* and certificate leaf[subject.OU] = DE8Y96K9QP) |
Identifier	com.cisco.secureclient.edlp.useragent
IdentifierType	bundleID

Uninstall Cisco Secure Client - Endpoint DLP on macOS

Provides instructions for completing the Uninstall Cisco Secure Client - Endpoint DLP on macOS workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Uninstall Cisco Secure Client - Endpoint Data Loss Prevention (DLP) from your macOS device using the following steps:

Procedure

1. Locate the uninstaller file named **Uninstall Cisco Secure Client - Endpoint DLP.pkg**. You can find the uninstaller at `/Applications/Cisco/Cisco Secure Client - Endpoint DLP Service.app/Contents/Resources`.
2. Run the uninstaller:
   a) Double-click the **Uninstall Cisco Secure Client - Endpoint DLP.pkg** file.
   b) Alternatively, open the terminal application and run: `sudo installer -pkg /Applications/Cisco/Cisco\ Secure\ Client\ -\ Endpoint\ DLP\ Service.app/Contents/Resources/Uninstall\ Cisco\ Secure\ Client\ -\ Endpoint\ DLP.pkg -target/`
3. To locate the uninstaller using Finder:
   a) Right-click on **Cisco Secure Client - Endpoint DLP Service** in `/Applications/Cisco`.
   b) Select **Show Package Contents**.
   c) Open the **Contents** folder, then open the **Resources** folder to find the uninstaller.

   Use administrator privileges when running the uninstall command. This process removes the Cisco Secure Client - Endpoint DLP application from your macOS system.

Uninstall Cisco Secure Client Endpoint DLP on Linux

Use this procedure to uninstall the Cisco Secure Client - Endpoint Data Loss Prevention (DLP) module from your Linux device. This guide provides the specific command-line instructions required to remove the software from both Ubuntu and Enterprise Linux distributions effectively.

Uninstall Cisco Secure Client - Endpoint Data Loss Prevention (DLP) from your Linux device using the following steps:

Procedure

1. Uninstalling Endpoint DLP for Linux on Ubuntu
   a) Use the following command to uninstall Endpoint DLP for Linux on Ubuntu.
      - `sudo apt remove cisco-secure-edlp`

2. Uninstalling Endpoint DLP for Linux on Enterprise Linux.
   a) Use the following command to uninstall Endpoint DLP for Linux on Enterprise Linux.
      - `sudo rpm --erase cisco-secure-edlp`

61 Virtual Private Networks on Cisco Secure Client

Topics:

- Manage Virtual Private Networks on Cisco Secure Client

Provides an overview of Virtual Private Networks on Cisco Secure Client in Cisco Secure Access, including Manage Virtual Private Networks on Cisco Secure Client. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Virtual Private Networks on Cisco Secure Client

Describes Manage Virtual Private Networks on Cisco Secure Client in Cisco Secure Access. Cisco Secure Client supports virtual private network (VPN) connections from user devices to private resources and Software as a Service (SaaS) resources in data centers and private and public clouds.

Cisco Secure Client supports virtual private network (VPN) connections from user devices to private resources and Software as a Service (SaaS) resources in data centers and private and public clouds. The Cisco Secure Client VPN module requires the Secure Access VPN XML file deployed on the user device.

Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access. The Cisco Secure Client is configured with various software modules. A Cisco Secure Client module may require the deployment of a certain profile to run the module successfully. A system configuration manager or remote monitoring and management (RMM) system can download, install, and deploy the Cisco Secure Client on an organization's user devices.

Prerequisites

Describes Prerequisites in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

- Administrative privileges on the user devices in the organization.
- Download the virtual private network (VPN) XML connection metadata from your Secure Access organization. For more information, see Download the Virtual Private Network XML Profile.

For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Download the Virtual Private Network XML Profile

Describes Download the Virtual Private Network XML Profile in Cisco Secure Access. The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules.

The Cisco Secure Client supports the use of various profiles to configure the deployment of the client modules. A Cisco Secure Client module may require a certain profile present to install the module successfully.

The Cisco Secure Client virtual private network (VPN) module requires the VPN XML profile. Cisco Secure Client installs with the VPN module. You can download the Cisco Secure Client VPN profile from Secure Access.

The Cisco Secure Client VPN profile configures the VPN module on the user device and connects clients securely to resources protected by Secure Access.

Download the Cisco Secure Client VPN profile to the user device.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.

Step 1 – Download the Cisco Secure Client VPN Profile

The Cisco Secure Client VPN profile describes the connection and security metadata for the VPN module.

1. Navigate to **Connect** > **End User Connectivity** > **Virtual Private Network**.
2. For a VPN profile, click **Download XML** to save the Cisco Secure Client VPN profile to the local system.

Step 2 – Copy the VPN Profile to the Target Directory

Copy the Cisco Secure Client VPN XML file to the Cisco Secure Client VPN profile directory on the user devices.

OS	Location	File	Description
Windows	**%Program Data%\Cisco\Cisco Secure Client\VPN\Profile**	AnyConnect VPN Profile	
macOS	**/opt/cisco/secureclient/vpn/profile**	AnyConnect VPN Profile	

CA Certificates for VPN Connections

Provides instructions for completing the CA Certificates for VPN Connections workflow in Cisco Secure Access. To authenticate users and devices when connected over a virtual private network (VPN), Secure Access must have the root certificate authority (CA) certificate for the user devices.

To authenticate users and devices when connected over a virtual private network (VPN), Secure Access must have the root certificate authority (CA) certificate for the user devices.

Set up the trust between Secure Access and the user devices in the organization that connect over a VPN:

Procedure

1. Install a certificate signed by your organization's Certificate Authority (CA) on all devices where you have deployed the Cisco Secure Client with the VPN module.
2. Upload your organization's signed CA root certificate to Secure Access. For more information, see VPN Certificates for User and Device Authentication.

62 Internet Security on Cisco Secure Client

Topics:

- Manage Internet Security on Cisco Secure Client
- Interpret Internet Security Diagnostics
- DNS Protection Status
- SWG Protection Status

Provides an overview of Internet Security on Cisco Secure Client in Cisco Secure Access, including Manage Internet Security on Cisco Secure Client, Interpret Internet Security Diagnostics, and DNS Protection Status. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Internet Security on Cisco Secure Client

Describes Manage Internet Security on Cisco Secure Client in Cisco Secure Access. Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access.

Cisco Secure Client is Cisco's endpoint security client application that enables secure connections to private resources, software as a service (SaaS) apps, and internet resources protected by Secure Access. The Cisco Secure Client is configured with various software modules. A Cisco Secure Client module may require the deployment of a certain profile to run the module successfully. A system configuration manager or remote monitoring and management (RMM) system can download and deploy the Cisco Secure Client on an organization's user devices.

A Roaming Device is a user device that has Cisco Security Client deployed on the device with the Umbrella (Roaming Security) module.

Cisco Secure Client deployed with the Umbrella module enables secure internet access on user devices. The Umbrella module includes:

- DNS-layer security
- Web security–Secure web gateway (SWG)

Once deployed, Cisco Secure Client registers the user device with Secure Access and the device is added to the list of Roaming Device resources. Cisco Secure Client syncs with Secure Access periodically and the user device's web traffic is protected by the Secure Access policy. An organization's administrators can manage Roaming Devices protected by internet security in Secure Access. For more information, see Manage Internet Security.

For more information about the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

Important

Internet Security Bypass Sizing: Cisco Secure Access supports up to 5,000 combined domain entries (and up to 9,000 entries upon request to your Cisco representative or Cisco Support). While large lists are supported, maintaining consolidated domain lists is recommended for optimal performance and reduced memory utilization on roaming devices running Cisco Secure Client. For more information, see Manage Internet Security Bypass.

Umbrella Roaming Security Module Requirements

Describes Umbrella Roaming Security Module Requirements in Cisco Secure Access. To ensure that the Cisco Secure Client Umbrella Roaming Security module deploys and operates successfully, your device must meet specific system and network requirements.

To ensure that the Cisco Secure Client Umbrella Roaming Security module deploys and operates successfully, your device must meet specific system and network requirements. This topic outlines the necessary prerequisites for installation, including supported network settings, security protocols, DNS configurations, and internal domain handling.

- System Requirements on page 2068
- Network Requirements on page 2068
- Transport Layer Security Protocol on page 2068
- Network Access on page 2068
- Roaming Security DNS Requirements on page 2069
- Internal Domains on page 2069

System Requirements

Describes System Requirements in Cisco Secure Access. The Cisco Secure Client supports all vendor-maintained, generally available releases of an operating system unless otherwise noted.

The Cisco Secure Client supports all vendor-maintained, generally available releases of an operating system unless otherwise noted. The Umbrella Roaming Security Module for Cisco Secure Client is not supported on Windows Server. For more information on the Cisco Secure Client and supported operating systems, see Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1.

Network Requirements

Describes Network Requirements in Cisco Secure Access and explains Secure Access DNS Block Pages and Secure Access and SAML Identity Provider Domains. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access DNS Block Pages

- For more information, see Network Requirements for Secure Access: DNS Block Pages.

Secure Access and SAML Identity Provider Domains

- For more information, see Network Requirements for Secure Access: SAML Identity Provider Domains.

> **Note**
>
> When using an SSL-VPN, add the IP address of the VPN head-end to the external domains settings. For more information, see Manage Domains.

Transport Layer Security Protocol

Describes Transport Layer Security Protocol in Cisco Secure Access. For more information, see Network Requirements for Secure Access: Transport Layer Security Protocol.

- For more information, see Network Requirements for Secure Access: Transport Layer Security Protocol.

Network Access

Describes Network Access in Cisco Secure Access and explains Host Names, Secure Access DNS Resolvers, and Encrypted DNS. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Host Names

The Cisco Secure Client Umbrella Roaming Security module uses hostnames for registration. All machines must have a hostname that is unique within your organization.

Secure Access DNS Resolvers

For more information, see Network Requirements for Secure Access: DNS Resolvers.

Encrypted DNS

For more information, see Network Requirements for Secure Access: Encrypted DNS.

External DNS Resolution

For more information, see Network Requirements for Secure Access: External DNS Resolution.

HTTP and HTTPS

The Cisco Secure Client Umbrella Roaming Security module uses HTTP (80/TCP) and HTTPS (443/TCP) to communicate with Secure Access for the following uses:

- Initial registration upon installation
- Checking for new versions of the Cisco Secure Client Umbrella (Roaming Security) module
- Reporting the status of Cisco Secure Client Umbrella (Roaming Security) module to Secure Access
- Checking for new internal domains

Windows Only: If you utilize an HTTP proxy that is configured at the user-level (normally using GPO), make sure the `SYSTEM` user is also configured to use the proxy. Otherwise, add the following rules to your firewall to ensure the Cisco Secure Client Umbrella (Roaming Security) module can reach Secure Access.

Secure Access DNS – Client Configuration Services

For more information, see Network Requirements for Secure Access: Client Configuration Services.

Secure Access DNS – Client Sync Services

For more information, see Network Requirements for Secure Access: Client Sync Services.

Secure Access DNS and Web – Client Certificate Revocation Services

For more information, see Network Requirements for Secure Access: Client Certificate Revocation Services.

Roaming Security DNS Requirements

Describes Roaming Security DNS Requirements in Cisco Secure Access. The Cisco Secure Client Umbrella Roaming Security module is not compatible with other DNS serving software.

- The Umbrella Roaming Security Module for Cisco Secure Client is not supported on Windows Server and is incompatible with other DNS-serving software. Do not install the module on a device that serves DNS requests. The module's `dnscryptproxy` subprocess encrypts DNS traffic and listens on UDP and TCP port 53. This port usage conflicts with the Windows DNS Server service. The module is also generally incompatible with other software that binds to UDP or TCP port 53 on localhost, regardless of the operating system.
- Uninstall **DNSCrypt** before your install the Cisco Secure Client Umbrella (Roaming Security) module. The Cisco Secure Client Umbrella (Roaming Security) module installer automatically detects installations of DNSCrypt and prompts the administrator to uninstall before proceeding with the installation.
- Install the Cisco Secure Client Umbrella Roaming Security module on the `C:\ drive`. The Cisco Secure Client Umbrella module does not support secondary or remote drive installations.
- The Cisco Secure Client Umbrella Roaming Security module only supports dual-stack IPv4/IPv6 for macOS and Windows. Standalone support for IPv6 for both macOs and Windows is not supported.

Internal Domains

Describes Internal Domains in Cisco Secure Access. The Cisco Secure Client sends all of your DNS lookups directly from your computer to the Secure Access global network resolvers.

The Cisco Secure Client sends all of your DNS lookups directly from your computer to the Secure Access global network resolvers. Thus, to ensure that Cisco Secure Client directs internal DNS requests to your internal DNS servers for resolution,

you must add your local domain names to the internal domains list in Secure Access. The Cisco Secure Client's Umbrella module syncs with Secure Access periodically to check for new internal domains. This is a **critical** part of the setup process. We recommend that you populate the list of internal domains before you deploy the Umbrella (Roaming Security) module. For more information, see Domain Management.

Domain Management

Describes Domain Management in Cisco Secure Access. Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file.

Cisco Secure Access provides the option to manage domains when endpoints connect to internet resources with the Cisco Secure Client or a PAC file. Domain management allows DNS queries for certain domains to query the local network's DNS servers instead of the Secure Access DNS servers.

If you do not specify a list of internal domains, all DNS queries are sent directly to Secure Access, and as a result, cannot reach your network's local resources (for example: computers, servers, printers) on internally-hosted domains that rely on local DNS servers.

When you add internal domains to your bypass list, these internal domain queries sent from an endpoint with a Secure Access PAC file or the Cisco Secure Client bypass the Secure Access DNS resolvers. However, in the case of a tunnel, this configuration is not passed down, so there is no way to bypass traffic to the proxy per-organization with a custom configuration for network tunnels.

To ensure uninterrupted access to these resources, administrators should add the appropriate domains to the organization's domain bypass list. The domain bypass list syncs to all Cisco Secure Clients in your organization.

Internal Domains List

Describes Internal Domains List in Cisco Secure Access. Populate the internal domains list with domains used by your organization to access local resources while on the organization's network (at the physical location or connected through VPN).

Populate the internal domains list with domains used by your organization to access local resources while on the organization's network (at the physical location or connected through VPN). The internal domains list is pre-populated with the **.local TLD** and all **RFC-1918 (private network)** reverse DNS address space. Secure Access syncs newly added domains to Cisco Secure Clients within about one hour. For more information, see Manage Domains.

DNS Suffixes

Describes DNS Suffixes in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The domains contained in the DNS suffixes configuration on a computer's adapter and global network settings are imported automatically into a Cisco Secure Client's internal domains list each time the Cisco Secure Client starts or a new network adapter (such as a VPN or wireless connection) is initiated. This sync process helps Cisco Secure Clients adapt when on newly seen networks where they may want to access local resources without adding the domain through the Secure Access.

Operational Flow

Describes Operational Flow in Cisco Secure Access and explains Configure Internal Domains, Cisco Secure Client and External Queries, and Cisco Secure Client and Internal Queries. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Cisco Secure Client can handle internal and external DNS queries gracefully.

Configure Internal Domains

The Cisco Secure Client's internal domains list is populated by two sources:

- Syncs from the Secure Access internal domains list.

- The DNS Suffixes list located in the local computer's networking configuration settings.

Cisco Secure Client and External Queries

External DNS queries that do not match a domain located on either of the internal domains lists are sent straight to Secure Access.

Cisco Secure Client and Internal Queries

DNS queries for domains contained in the domain bypass list (internal domains list) are sent through the local network's DNS servers.

- Internal domains that are hosted on the local network are resolved by the internal DNS server directly.
- Internal Domains that are not hosted on the local network are resolved by Secure Access or whichever public DNS servers are used for resolution.

Advanced Topics

Describes Advanced Topics in Cisco Secure Access. The following sections focus on more in-depth information and logic with internal domains and expected behavior.

The following sections focus on more in-depth information and logic with internal domains and expected behavior.

Unencrypted

Although the Cisco Secure Client is able to send encrypted DNS queries to Secure Access **when in the encrypted state**, domains listed on the bypass domains list are sent unencrypted, because they are not sent to Secure Access.

DNS Suffixes (Continued)

There are implications that should be considered with DNS Suffixes.

- This could allow an organization to not add any domains to the internal domains list in Secure Access. If DHCP is configured to use your domains as DNS Suffixes, the Cisco Secure Client automatically considers the domain as local, even without adding the domain to the internal domains list in Secure Access.
- If you use DNS suffixes to rely on internal domain resolution instead of populating the internal domains list in Secure Access, the endpoint traffic has increased security. Since DNS queries sent to domains on the internal domains list are sent unencrypted, this implies that a machine performing DNS queries for domains on the Secure Access internal domains list always sends unencrypted traffic on *all* networks.

> **Note**
>
> During the deployment of the Cisco Secure Client on user devices, you can disable the feature that adds the domains contained in the DNS suffixes list.

Interpret Internet Security Diagnostics

Describes Interpret Internet Security Diagnostics in Cisco Secure Access. When deployed on a user device, the Cisco Secure Client with the Umbrella (Roaming Security) module can generate detailed diagnostic reports about the device's DNS and web traffic.

When deployed on a user device, the Cisco Secure Client with the Umbrella (Roaming Security) module can generate detailed diagnostic reports about the device's DNS and web traffic. The Cisco Secure Client's Diagnostic Tool (DART) module provides the diagnostic information about the device. As an administrator on the device, generate a diagnostic report from the Cisco Secure Client GUI or the Cisco Secure Client's DART command-line interface (CLI).

For information about the administration of the Cisco Secure Client, see Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.

Procedure

Describes Procedure in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Generate the Cisco Secure Client diagnostic report on the user device.

Prerequisites

- Administrative privileges on the user device.

The following procedures describe how to:

- Generate the Diagnostic Report from the Cisco Secure Client on page 2072
- Generate the Diagnostic Report on the Command Line on page 2072

Generate the Diagnostic Report from the Cisco Secure Client

Provides instructions for completing the Generate the Diagnostic Report from the Cisco Secure Client workflow in Cisco Secure Access. From the Cisco Secure Client menu, select Diagnostics and Reporting Tool, and then select Run.

Procedure

1. From the Cisco Secure Client menu, select **Diagnostics and Reporting Tool**, and then select **Run**.
2. Send the generated **.zip** file to Cisco Support. For more information, see Welcome to Cisco Secure Access.

Generate the Diagnostic Report on the Command Line

Provides instructions for completing the Generate the Diagnostic Report on the Command Line workflow in Cisco Secure Access. Find the Cisco Secure Client Umbrella module diagnostic tool on your system and run the Cisco Secure Client's DART executable.

Procedure

1. Find the Cisco Secure Client Umbrella module diagnostic tool on your system and run the Cisco Secure Client's **DART** executable.

OS	Location
Windows	`%ProgramData%\Cisco\Cisco Secure Client\UmbrellaDiagnostic.exe`
macOS	`/opt/cisco/secureclient/bin/UmbrellaDiagnostic.app`

2. Send the generated **.zip** file to Cisco Support. For more information, see Welcome to Cisco Secure Access.

DNS Protection Status

Describes DNS Protection Status in Cisco Secure Access. After you deploy the Umbrella module in the installed Cisco Secure Client, IPv4 and IPv6 DNS protection status changes appear in the Cisco Secure Client endpoint.

After you deploy the Umbrella module in the installed Cisco Secure Client, IPv4 and IPv6 DNS protection status changes appear in the Cisco Secure Client endpoint. If you do not see DNS protection status, the Umbrella module is installed, but Internet Security (`OrgInfo.json`) is not deployed.

View DNS Protection Status

Provides instructions for completing the View DNS Protection Status workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View status information in the Cisco Secure Client Secure Access module on the user device.

Before you begin

- Administrative privileges on the user device.

Procedure

1. Open the **Cisco Secure Client**.
2. Click the chart icon at bottom left to open the **Statistics** menu.



3. Navigate to **Secure Access** to see DNS and IP security information.
4. The following table provides descriptions of the DNS protection status information displayed in the Cisco Secure Client Secure Access module on the user's device.

Status	Description	Condition
Reserved	`Checking Connection Status.` No active network connections. The Secure Access module waits for an active network connection.	This operating state occurs during the following conditions: - When the module is first activated. - When a network interface change occurs. For example, as detection of a new network adapter, IP changes on an existing adapter, or a new VPN tunnel being established or torn down.
Open	`You are not currently protected by Secure Access.` There is at least one active network connection; however, the Roaming Security agent can not connect to the Secure Access resolvers over port 53/UDP or 443/UDP on any active connection. The user is not protected by Secure Access and traffic events are not reported to Secure Access. The system's DNS settings revert to their original settings–DHCP or Static.	This operating state occurs during the following conditions: - No UDP port 443 or UDP port 53 connectivity to Secure Access resolvers (IPv4 or IPv6)). - The VPN tunnel may temporarily be in a state of tear down or establishment.

Status	Description	Condition
Protected	`You are protected by Secure Access.` A network connection is active, and the Secure Access module is able to connect to Secure Access resolvers over port 53/UDP, but not 443 UDP. The user is protected by Secure Access and traffic events are reported to Secure Access, but the connection is not encrypted.	This state may occur when the module is first activated or when there is a network interface change.
Encrypted	`You are protected by Secure Access.` The module in Cisco Secure Client has established a connection to Secure Access resolvers over port 443/UDP. The user is protected by Secure Access and traffic events are reported to Secure Access. The DNS queries are encrypted. Internal Domains are forwarded to DHCP-delegated or statically-set DNS servers and are therefore not encrypted.	This operating state occurs during the following conditions. **Note:** TCP is only used when UDP responses are truncated. - UDP port 443 connectivity to Secure Access resolvers (IPv4 or IPv6). - TCP port 443 and TCP port 53 connectivity to Secure Access resolvers (IPv4 or IPv6).
VPN Trusted Network State	`Disabled while you are on a trusted network.` The Secure Access module DNS protection is not active because the current endpoint network is configured as a Cisco Secure Client VPN trusted network.	This operating state occurs during the following conditions. **Note:** This setting is true for all roaming package customers and cannot be changed by the administrator. - AnyConnect VPN module is reporting the Trusted Network Detection state as trusted. - AnyConnect VPN tunnel is either not connected or established in full tunnel mode.The Secure Access policy rule indicates that the Secure Access module should be disabled when on an Cisco Secure Client VPN trusted network.
Disabled due to Full Tunnel VPN	`Disabled while your VPN is active.` The Secure Access module DNS protection is not active because the endpoint currently has an active Cisco Secure Client VPN established in full tunnel mode.	This operating state occurs during the following conditions. - Cisco Secure Client VPN module is reporting the Trusted Network Detection state as not trusted. - Cisco Secure Client VPN tunnel is established in full tunnel mode. Policy rule configured with Secure Access requires that the module is disabled when a Cisco Secure Client VPN tunnel is established and active. **Note:** This setting is true for all Secure Access module configurations and cannot be changed by the administrator.

Status	Description	Condition
No OrgInfo.json State	`You are not currently protected by Secure Access.` The Secure Access profile is not deployed. The module's DNS protection is not active because the endpoint currently has an active AnyConnect VPN tunnel established.	This operating state occurs when the **OrgInfo.json** file is not deployed to the correct directory. For more information, see Download the OrgInfo.json File.
Agent Unavailable State	`You are not currently protected by Secure Access.` Service unavailable. The module's DNS protection is not active because the Roaming Security agent is not running.	This operating state occurs when the Secure Access agent service is not currently running because of a crash or manual service stop.
Missing .NET Dependency State (Windows only)	`You are not currently protected by Secure Access.` Microsoft 4.0 NET framework is not installed. Roaming Security module DNS protection is not active because the Roaming Security agent is not running. The .NET runtime framework is missing.	This operating state occurs when the Secure Access agent service is not running due to a missing .NET 4.0 runtime.
Disabled	A Secure Access administrator disables DNS protection.	This operating state occurs when the Secure Access administrator disables DNS protection on IPv4, IPv6, or both through the instance of Secure Access.
Disabled (no network)	(IPv6 only) Cisco Secure Client disables DNS protection over IPv6.	If the Cisco Secure Client Secure Access module detects an IPv6 link-local address while performing an IPv6 connectivity probe, then the client disables DNS protection over IPv6.
Not Required	The client is not attempting coverage in this state, as it is not expected nor required. This state applies individually to IPv4 and to IPv6 on Windows.	The client was not able to find a suitable local DNS resolver for the IP Protocol, and therefore is disabled awaiting the discovery of a suitable local DNS resolver. This is most common when on a dual stack network, but only IPv4 resolvers are configured.

SWG Protection Status

Describes SWG Protection Status in Cisco Secure Access. After you deploy the Umbrella module in the installed Cisco Secure Client, a Web Protection Status appears in the Cisco Secure Client endpoint.

After you deploy the Umbrella module in the installed Cisco Secure Client, a Web Protection Status appears in the Cisco Secure Client endpoint. If you do not see a Web Protection Status, the Umbrella module is installed, but Internet Security (`OrgInfo.json`) is not deployed.

View SWG Protection Status

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

View status information in the Cisco Secure Client Umbrella module on the user device.

Before you begin

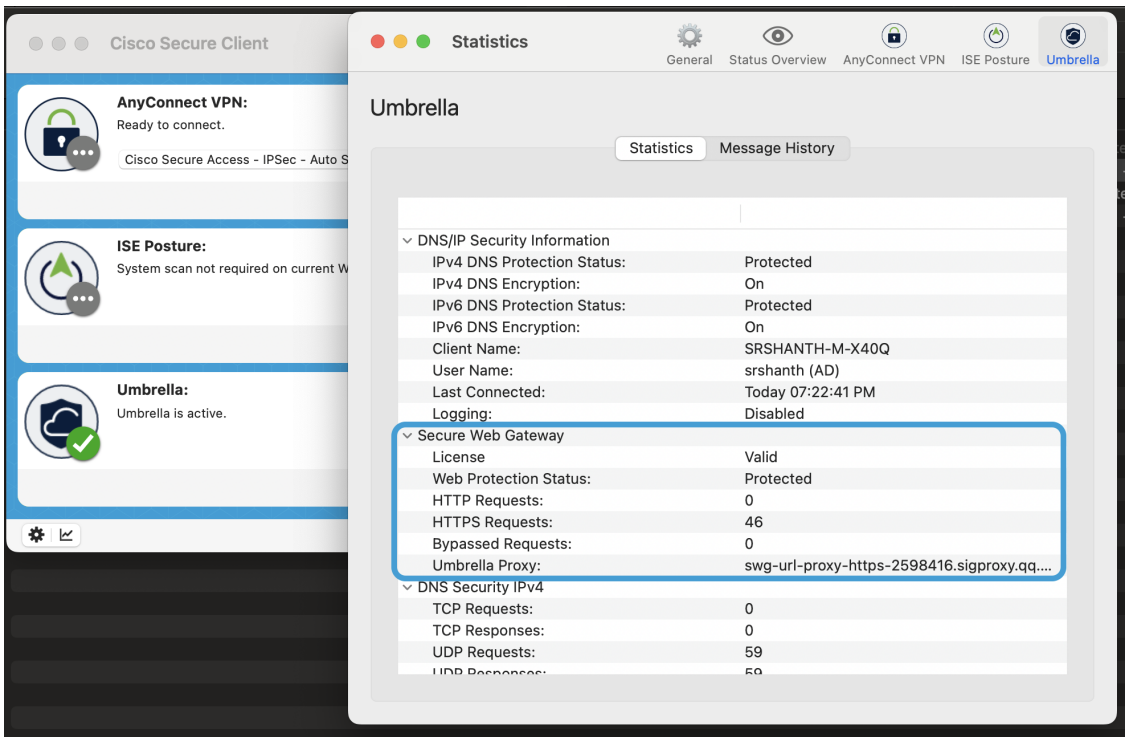
- Administrative privileges on the user device.
- Cisco Secure Client version 5.1.8.105 or later deployed with the Umbrella Roaming Security module or a PAC file for browsers in the environment is required for SWG protection status in Secure Access. For more information, see Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1.

Procedure

1. Open the **Cisco Secure Client**.
2. Click the chart icon at bottom left to open the **Statistics** menu.



3. Navigate to **Umbrella** to see Secure Web Gateway information.



4. The following table provides descriptions of the Secure Web Gateway protection status information displayed in the Cisco Secure Client Umbrella module on the user's device.

Status	Description	Condition
Offline	The device is unable to sync with Secure Access and SWG state is unknown.	Secure Client on the device has not been able to sync with Secure Access for 100 minutes or longer.
Protected	The device is protected by SWG.	SWG Agent service `csc_swgagent` is running and intercepting web traffic.
Unprotected	The device is not protected by SWG.	SWG Agent service `csc_swgagent` failed to start.
Configuration Error	Failed to update SWG Configuration.	Incorrect value in `SWGConfig.json`
Cloud Service Unavailable	SWG Agent was unable to connect to SWG Proxy.	SWG proxy is not reachable.
Disabled due to trusted network	SWG protection is disabled.	The device is connected to an AnyConnect trusted network or a network that matches a trusted context defined by your organization's SWG backoff settings. For more information, see the Secure Web Gateway Backoff Settings section of the Configure Cisco Secure Client Settings page.
Disabled	SWG protection is disabled.	Depending on the organization's SWG backoff settings, you may see this state if SWG protection is disabled when the device is not on AnyConnect VPN or a trusted network.

What to do next

For more information, see Manage Roaming Devices and the Umbrella Roaming Security chapter of the Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1.

63 Endpoint Diagnostic Tool

Topics:

- Cisco Endpoint Diagnostic Tool

Provides an overview of Endpoint Diagnostic Tool in Cisco Secure Access, including Client Endpoint Diagnostic Tool. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Cisco Endpoint Diagnostic Tool

Use this procedure to download and run the Cisco Endpoint Diagnostic Tool (CEDT), collect diagnostic data from Cisco Secure Access modules, and generate a diagnostic archive that you can upload to a Cisco Technical Assistance Center (TAC) case for troubleshooting.

Use the Cisco Endpoint Diagnostic Tool (CEDT) to collect diagnostic data from macOS or Windows endpoints and troubleshoot Cisco Secure Access modules. CEDT provides these capabilities:

- **System scanning:** Detects installed Cisco Secure Access modules.
- **Application logs:** Collects diagnostic logs generated by client software and the service infrastructure.
- **System data:** Securely collects and encrypts system data related only to Cisco Secure Access diagnostics.
- **Network diagnostics:** Collects network diagnostic data relevant to Cisco Secure Access components.

CEDT packages the collected data into a diagnostic archive that you can save locally or upload directly to a Cisco TAC support case. The tool does not capture personal data.

CEDT automatically detects installed Cisco Secure Access modules and displays each module with its version number. The detected components can include Zero Trust Access (ZTNA), Secure Web Gateway (SWG), Remote Access VPN (RAVPN), and Common System Information.

The tool runs several diagnostic tests, including Domain Name System (DNS) lookup, packet capture, host connectivity tests, policy testing, network speed tests, and HTTP Archive (HAR) capture. You can also use the tool to collect a Diagnostics and Reporting Tool (DART) bundle from Cisco Secure Client. When the diagnostic run completes, the tool packages all collected data into a compressed archive file. Upload this file to your Cisco TAC support case.

Before you begin

- Download the latest version of the Cisco Endpoint Diagnostic Tool (CEDT) for macOS or Windows.
- Install Cisco Secure Client on your system so the tool can detect Secure Access modules.
- If you want to upload the diagnostic archive to a Cisco Technical Assistance Center (TAC) case ensure that the system has an active internet connection.
- Obtain a Cisco TAC Case ID and Token if you plan to upload diagnostic results directly from the tool.
- Use administrator privileges to run diagnostics that require elevated access, such as packet capture or debug flag collection.
- Install Google Chrome if you plan to run HAR capture. CEDT does not currently support HAR capture inFirefox or Safari.

System Data Collected

The tool collects this system data, organized by category. No personal data of any kind is captured.

- General System Information

Data	macOS	Windows
OS, hardware, CPU, RAM, storage	system_profiler SPSoftwareDataType SPHardwareDataType	systeminfo, WMI classes Win32_OperatingSystem, Win32_ComputerSystem, Win32_BIOS
Kernel parameters	sysctl -a	N/A

- Network Configuration

Data	macOS	Windows
Network interfaces & IP addresses	`ifconfig-a`	`ipconfig/all`
Routing table	`netstat--rn`	`netsat-rn`
DNS configuration	`scutil--dns`	(include in `ipconfig/all`)
Network services	networksetup-listallnetworkservices	`netsh interface show interface`
WiFi profiles	N/A	`netsh wlan show profiles`

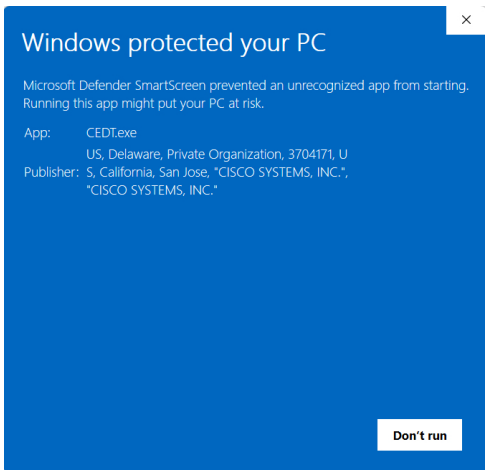
- Product Information

Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco*`	Registry exports (HKLM\SOFTWARE\Cisco, HKCU\SOFTWARE\Cisco, acsock service)
Installation directories	`1s-1as/opt/cisco`	%ProgramFiles%\Cisco, %ProgramFiles(x86)%\Cisco, %ProgramData%\Cisco
Running Cisco processes	`ps aux |grep -i cisco`	`tasklist|findstr/icisco`, WMI `Win32_Process`
Installed Cisco products	`mdfind` for Cisco apps	WMI `Win32_Product(Vendor Cisco)`
Application logs	Cisco Secure Client log directories	`%ProgramData%\Cisco\Cisco Secure Client\Logs`
Event logs	N/A	Windows Event Log (`Cisco Secure Client - Zero Trust Access`, Application provider `*Cisco*`)
Crash reports	~/Library/Logs/DiagnosticReports/Cisco*	N/A

Procedure

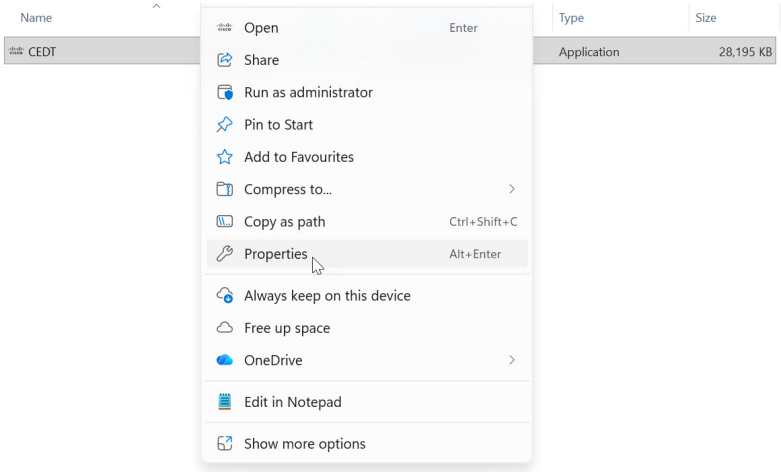
1. Launch the **CEDT** tool.

   For Windows users, **Windows protected your PC** warning may appear.

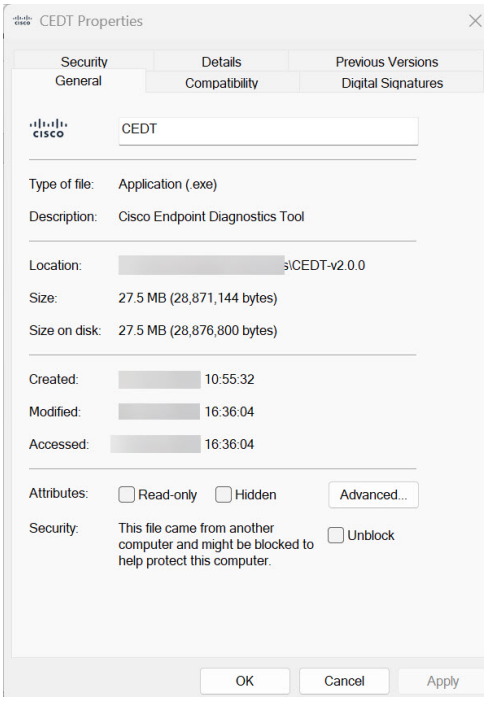


This warning may appear even if the executable is digitally signed. This situation often occurs with newly created or internally distributed applications that have not yet gained enough reputation with Microsoft SmartScreen. To trust the executable, follow this process:

a) Right-click on the **CEDT.exe** application file.
b) Select **Properties**.



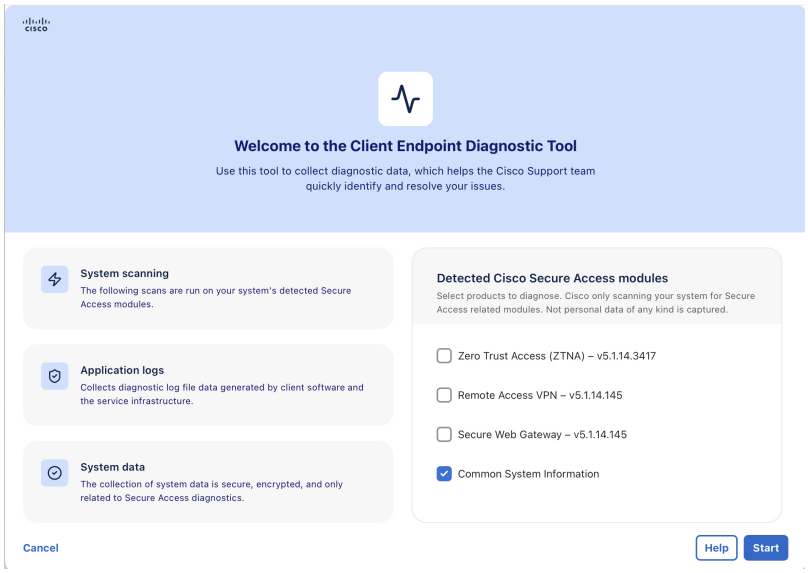
c) In the **General** tab, look for the **Security** section at the bottom.
d) Check the **Unblock** check box.



e) Click **Apply** and **OK**.

f) Run the **CEDT** executable file again.

2. On the welcome screen, review the detected modules and their version numbers. CEDT can display **Secure Web Gateway (SWG)**, **Zero Trust Network Access (ZTNA), Remote Access Virtual Private Network (RAVPN)** and **Common System Information**.



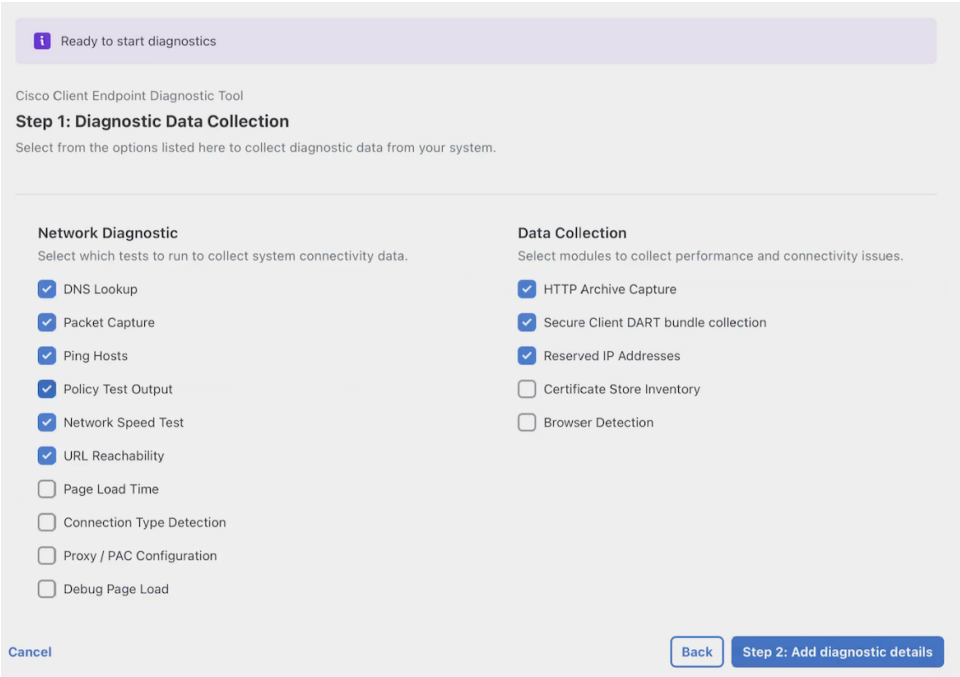
3. Select or deselect the modules that you want to diagnose, and then click **Let's Start**.
4. On the **Diagnostic Data Collection** screen, select the connectivity tests to run.
   - **DNS Lookup**–Tests DNS resolution for specified hosts. You can specify custom resolver IP addresses.CEDT saves the consolidated results in dns/dns_lookups.txt.
   - **Packet Capture** – Captures network packets for a specified duration. This test requires administratorprivileges.
   - **Ping Hosts**–Pings specified hosts to verify connectivity.

- **Policy Test Output**–Tests policy enforcement for up to 10 specified URLs throughpolicy.test.sse.cisco.com. The results include structured policy output and automatically captured HARdata.
- **Network Speed Test**–Measures download speed, upload speed, latency, and jitter throughspeed.test.sse.cisco.com. CEDT saves the results in JSON and text-summary formats.
- **URL Reachability**–Uses HTTP GET requests to test up to 20 URLs, with a 30-second timeout for eachURL. The results include reachability, HTTP status, response time, content length, resolved IP address,TLS version, and timestamp.

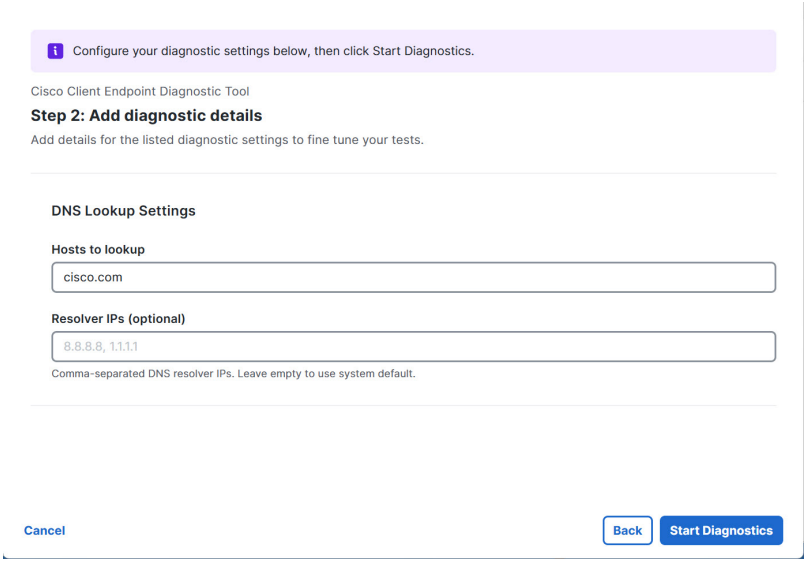
5. Select the data-collection and debugging options to include.
   - **HAR Capture**–Records browser-session network data. CEDT currently supports Google Chrome only.
   - **DART Bundle Collection**–Collects a DART bundle from Cisco Secure Client, including logs from allinstalled modules.
   - **Reserved IP**–Runs reserved-IP traceroute or tracert and DNS diagnostics.
   - **Enable Debug Flags**–Collects detailed endpoint-activity logs. This option is available only when at leastone detected Cisco Secure Access product is selected.
   - **DebugView Capture**–Enables debug logging for the Windows Secure Endpoint Connector. This optionis available only on Windows.
6. Optionally, check the checkbox for each Secure Access module you want to diagnose.
7. Click **Start** to begin the diagnostic workflow.
8. Under the **Network Diagnostic** section, check the relevant diagnostic tests check box to collect connectivity data.
9. Under the **Data Collection** section, check the relevant diagnostic tests check box to collect the performance and connectivity issues data.
10. The **Enable the debug flag** check box is checked by default for the detected Secure Access modules.

> **Note**
>
> If the CEDT does not automatically detect any Secure Access modules, you must select a product module in the welcome screen to enable the **Enable debug flags** check box. This check box is disabled when no product module is selected and is automatically turned off when only Common system information is selected.

11. Click **Step 2: Add diagnostic details**.

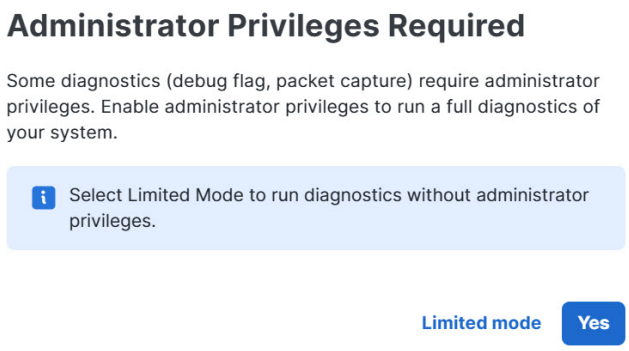


12. Configure the settings for each selected test. CEDT displays settings only for the tests that you selected.
    - For DNS Lookup, enter one or more hostnames and, optionally, custom resolver IP addresses.
    - For Packet Capture, select the interfaces, packet count, and capture duration.
    - For Ping Hosts, enter one or more hosts.
    - For URL Reachability, enter the URLs to test. HTTP uses port 80 and HTTPS uses port 443 by default.Include the port in the URL when you use a nonstandard port.
    - For Policy Test Output, enter up to 10 host URLs.
    - For HAR Capture, enter the target URLs and ensure that Google Chrome is installed.
    - Configure any selected KDF, reserved-IP, performance, certificate-store, or debug-page-load settings.



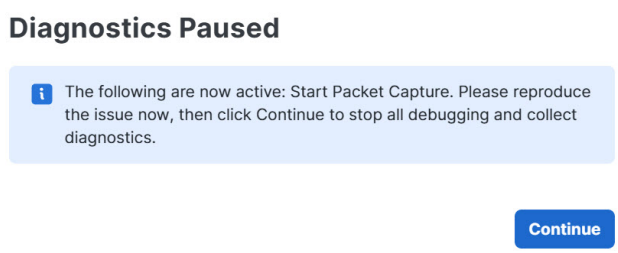
13. Click **Start Diagnostics** to begin the diagnostic run.

If you selected network diagnostic options such as **Dart Bundle** or **Packet Capture**, the **Administrator Privileges Required** window appears. Click **Yes** to allow full diagnostics or **Limited mode** to continue without elevated privileges.



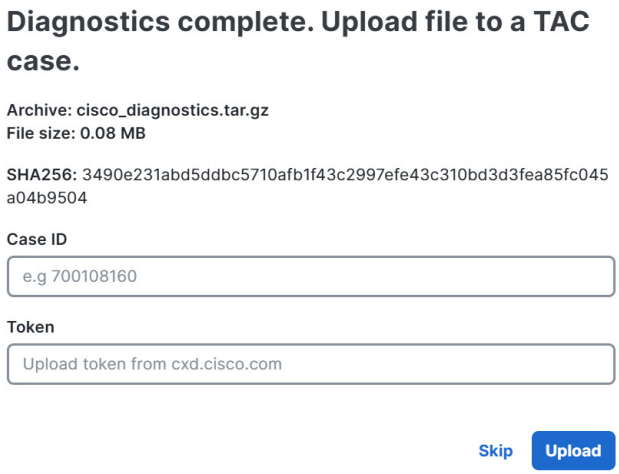
The diagnostic output files are saved in a tar.gz archive on your desktop. You can view the status of each task in the progress bar.

14. If CEDT pauses during advanced troubleshooting, reproduce the issue while detailed logging is active. Do not close CEDT while the diagnostic run is paused. Click **Continue** after you reproduce the issue.
    - Reconnect to the VPN.
    - Open the internal application that is failing.
    - Repeat the steps that cause the error.



> **Note**
>
> Packet capture uses a circular buffer limited to 64 MB. The tool retains only the most recent data to prevent excessive file sizes.

15. Wait for all selected diagnostic tasks to complete. The progress bar displays the overall status. Do not close CEDT while diagnostics are running.
16. When the run completes, review the archive filename, **file size,** and **SHA-256 checksum**.
17. To upload the archive directly, enter the Cisco TAC**Case ID** and **Token**, and then click **Upload** to send the diagnostic archive to your Cisco Technical Assistance Center (TAC) case. To retain the archive without uploading it, click **Skip**. See Contact Cisco Secure Access Support.



18. After a successful upload, click **Run Again** to start another diagnostic run or click **Close** to exit CEDT.
    The CEDT generates a compressed diagnostic archive file that contains system information, application logs, and network diagnostic data related to Cisco Secure Access modules.

    The tool saves the diagnostic output in the following location:

    - macOS: ~/Desktop/cisco_diagnostics/
    - Windows: %USERPROFILE%\Desktop\cisco_diagnostics\

    The archive file uses the name **cisco_diagnostics.tar.gz**. You can upload this file to a Cisco Technical Assistance Center (TAC) case or share it with Cisco support engineers for further troubleshooting.

64 Managed iOS

Topics:

- Cisco Security Connector: Secure Access Setup Guide
- Meraki Registration
- Register an iOS Device Through Apple Configurator 2
- IBM MaaS360 Registration
- Intune Registration
- Jamf Registration
- MobileIron Registration
- MobiConnect Registration
- Workspace ONE Registration
- Register an iOS Device Through a Generic MDM System
- Apply an Access Policy to Your Mobile Device
- Add User Identity for Cisco Security Connector
- Anonymize Devices
- Export Device Data to CSV
- Push the Cisco Root Certificate to Managed Devices
- Configure Cellular and Wifi Domains
- Configuring DNS Suffix Allow List
- Troubleshooting

Provides an overview of Managed iOS in Cisco Secure Access, including Cisco Security Connector: Secure Access Setup Guide, Meraki Registration, and Register an iOS Device Through Apple Configurator 2. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Cisco Security Connector: Secure Access Setup Guide

Describes Cisco Security Connector: Secure Access Setup Guide. The Cisco Security Connector: Secure Access Setup Guide only explains how to configure the Secure Access portion of the Cisco Security Connector (CSC).

> **Note**
>
> - The *Cisco Security Connector: Secure Access Setup Guide* only explains how to configure the Secure Access portion of the Cisco Security Connector (CSC). For information about how to configure your Mobile Device Manager (MDM) system, see your MDM system's documentation.
> - The Cisco Security Connector is only supported for DNS policies.

The Cisco Security Connector provides visibility and control for organization-owned and MDM managed mobile Apple iOS devices, such as iPhones and iPads. The CSC's Secure Access component directs DNS traffic, including functionality for the intelligent proxy, to the Cisco Secure Access cloud where filtering against malicious sites, such as phishing sites or sites that exfiltrate information, takes place.

The CSC's Secure Access portion does not require an on-demand or always-on VPN or a full proxy to gain complete visibility and control through cloud security (not locally on the device). This makes for both easier management and simpler, more effective security.

> **Note**
>
> Your iOS mobile device must be managed by a MDM system.

> **Note**
>
> Remote Browser Isolation (RBI), which protects users by redirecting browsing to a cloud-based host, is not supported on mobile devices running iOS or Android.

For more information about the Cisco Security Connector, see Cisco Security Connector.

Requirements

Describes Requirements in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

For the Cisco Security Connector:

- iOS device must be running iOS 15.0 or higher OR must be running in supervised mode with iOS 13.2 or higher.
- iOS device must be managed by a Mobile Device Manager (MDM) system and use one of the following Apple device managers:
  - Apple School Manager

  - Apple Business Manager

- Five MB free space.

One of the following MDM systems:

- Meraki System Manager (SM) with API access enabled

  > **Note**
  >
  > Only System Manager and Combined network types are supported.

- Apple Configurator 2.5 or higher
- IBM MaaS360
- Intune
- Jamf
- MobiConnect
- MobileIron Enterprise Mobility Management (EMM) On-Prem and Cloud versions 9.4 or higher
- Workspace ONE
- Generic–Other MDMs may be used to manage your organization-owned iOS mobile device; however, success results may vary. For more information, see Register an iOS Device Through a Generic MDM System.

  For information about configuring your specific MDM system, see your MDM system's documentation or contact your MDM's support team.

You will also need:

- Cisco Secure Access account.
- Direct access to the IPv4 IP addresses 208.67.222.222 or 208.67.220.220 is required for IPv4 DNS protection on ports 53 and 443.
- Direct access to the IPv6 IP addresses 2620:119:35::35 or 2620:119:53::53, or access to IPv4 addresses on ports 53 and 443 through NAT64/DNS64 translation is required for IPv6 DNS protection.

  > **Note**
  >
  > If DNS protection fails to engage, DNS traffic is not encrypted.

- The device must be able to communicate with `registration.polaris.qq.opendns.com` for registration and validation purposes at least once a day–when actively used–otherwise, the device cannot be protected.
- Depending on the MDM, you may also require each device's serial number.

Optionally

Describes Optionally in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

- Cisco Secure Endpoint. For more information, see Cisco Secure Endpoint.

Getting Started

Describes Getting Started in Cisco Secure Access. For a quick explanation of how to protect your iOS device with Secure Access through CSC, see Quick Start.

For a quick explanation of how to protect your iOS device with Secure Access through CSC, see Quick Start.

For MDM specific Secure Access procedures, see:

- Meraki Registration
- Register an iOS Device Through Apple Configurator 2
- IBM MaaS360 Registration
- Intune Registration
- Jamf Registration
- MobiConnect Registration
- MobileIron Registration
- Workspace ONE Registration
- Register an iOS Device Through a Generic MDM System

> **Note**
>
> For information about configuring your specific MDM system, see your MDM system's documentation.

Quick Start

Describes Quick Start in Cisco Secure Access. The following is a short description of the general procedure for registering your supervised iOS device through your Mobile Device Manager (MDM) to Secure Access.

The following is a short description of the general procedure for registering your supervised iOS device through your Mobile Device Manager (MDM) to Secure Access. For Secure Access procedures specific to an MDM, see:

- Meraki
- Configurator 2
- IBM MaaS360
- Intune
- Jamf
- MobiConnect
- MobileIron
- Workspace ONE
- Generic

Procedure

Below are the steps to follow for registering your IOS device through your MDM to Secure Access.

Before you begin, confirm that you meet all requirements as listed here.

- Install the Cisco Security Connector App
- Add an organization Admistrator' Email Address
- Register your IOS device through your MDM to secure access

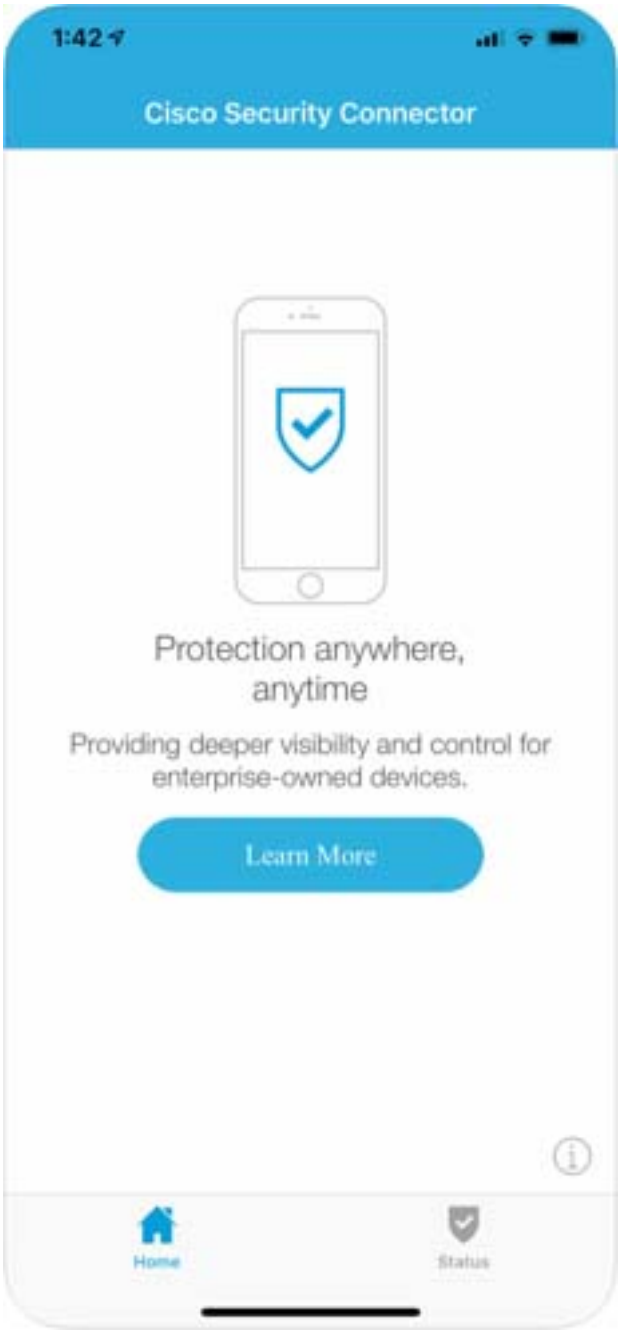
1. Install the Cisco Security Connector App

Provides instructions for completing the 1. Install the Cisco Security Connector App workflow in Cisco Secure Access. On your iOS device, download and install the Cisco Security Connector app.

Procedure

On your iOS device, download and install the Cisco Security Connector app.

Get the Cisco Security Connector app from the App Store. Depending on your MDM, you may be able to deploy the Cisco Security Connector to supervised iOS mobile devices through your MDM.



---

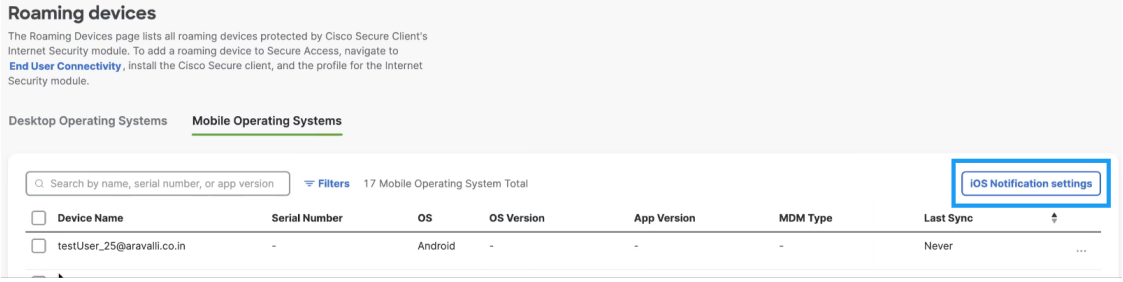
2. Add an Organization Administrator's Email Address

Provides instructions for completing the 2. Add an Organization Administrator's Email Address workflow in Cisco Secure Access. The administrator email address is the email address that your end-user can use to send diagnostic reports from the app by clicking the I icon from within the iOS device.

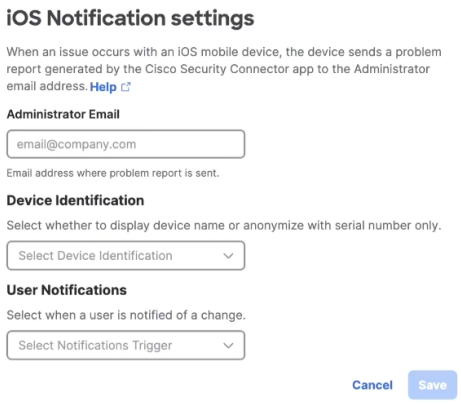
The administrator email address is the email address that your end-user can use to send diagnostic reports from the app by clicking the **I** icon from within the iOS device. These reports can then be passed onto Cisco support. Once set, this email address is automatically added when managing an MDM.

Procedure

1. Navigate to **Resources** > **Roaming Devices** > **Mobile Operating System** and click **iOS Notification settings**.



2. In the **iOS Notification settings** window, enter an administrator email address, choose a device identification method, and choose a notifications level (Protection failure notifications only or notify on all state changes), and click **Save**.

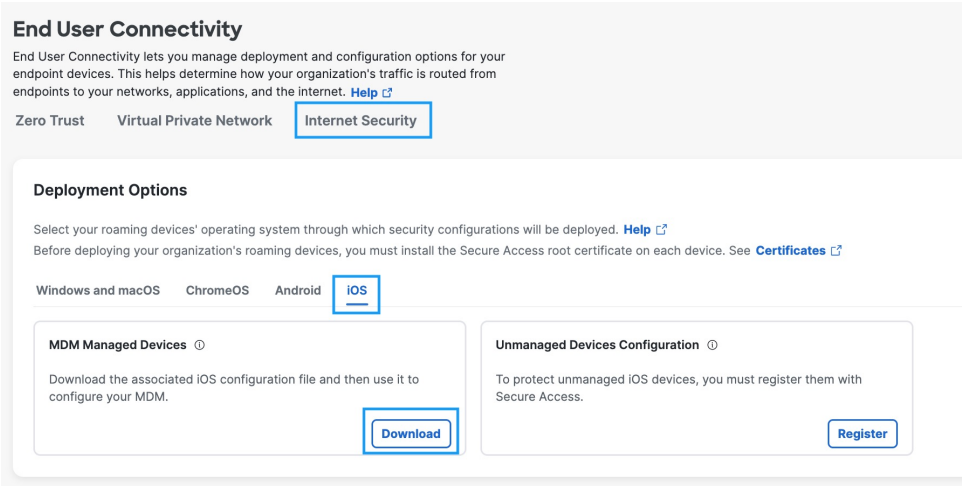


3. Register Your iOS Device Through Your MDM to Secure Access

Provides instructions for completing the 3. Register Your iOS Device Through Your MDM to Secure Access workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

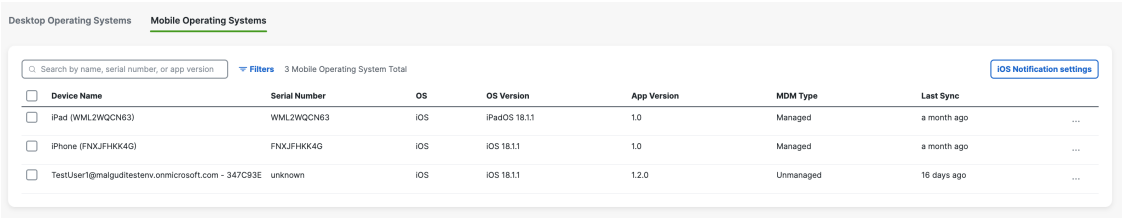
Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**.
2. Click the **IOS** tab.

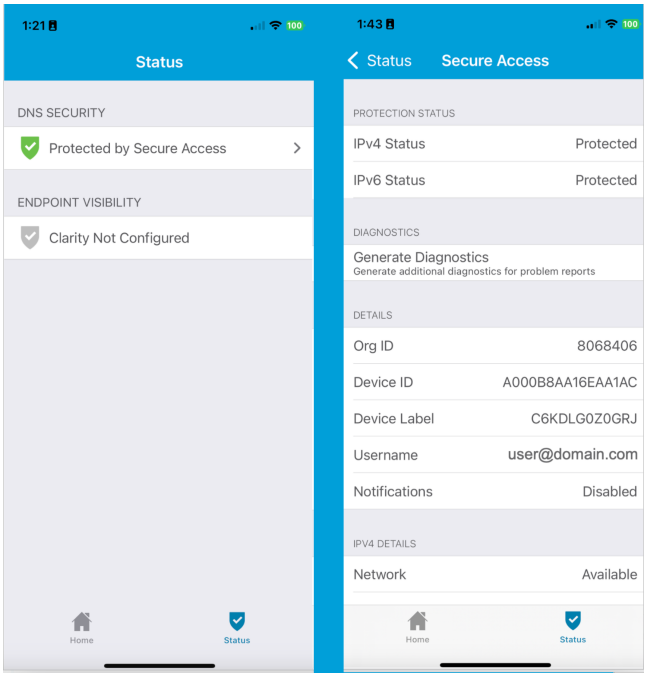


3. Under the **MDM Managed Devices** section, click **Download**
4. Procedures to register your iOS device with Secure Access differ depending on the MDM system you are using:
   - Meraki
   - Configurator 2
   - IBM MaaS360
   - Intune
   - Jamf
   - MobiConnect
   - MobileIron
   - Workspace ONE
   - Generic

   For information about configuring your specific MDM system, see your MDM system's documentation.
5. When you have successfully registered your iOS device, Secure Access lists it in **Resources** > **Roaming Devices** > **Mobile Operating Systems**.



6. On your mobile device, in the Cisco Security Connector app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**. For protection details, tap **Protected by Secure Access**.



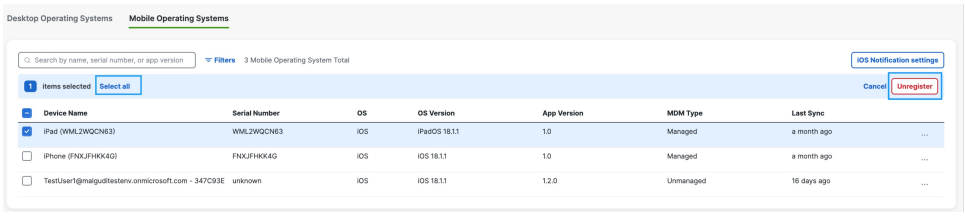
Unregister a Mobile Device

Provides instructions for completing the Unregister a Mobile Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

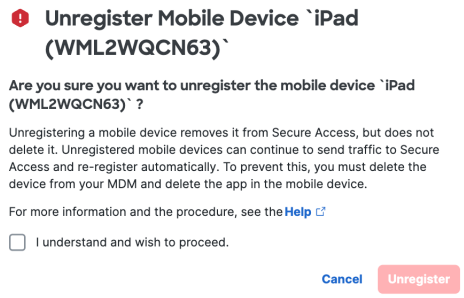
To unregister a mobile device that is successfully registered with Secure Access through MDM, follow these steps:

Procedure

1. Navigate to **Resources** > **Roaming Devices** > **Mobile Operating System**.
2. Choose one of the following options as per your requirement:
   - To unregister a device, check the check box next to the device and click **Unregister** at the top-right corner of the device list.
   - To unregister multiple devices simultaneously, check the check boxes next to all the required devices and click **Unregister** at the top-right corner of the device list.
   - To unregister all the devices, click **Select all** at the top of the table to choose all the devices at once and click **Unregister** at the top-right corner of the device list.



3. In the confirmation dialog box, check the **I Understand and wish to proceed** check box and click **Unregister**.



Note

Unregistering a mobile device from the dashboard does not prevent it from sending traffic to Secure Access. To stop a mobile device from sending traffic to Secure Access, you must delete the device from the MDM and remove the Cisco Security Connector app from the mobile device.

Manage Device Deployment

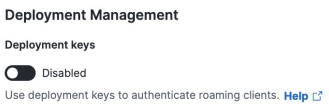
Describes Manage Device Deployment in Cisco Secure Access. The Deployment Keys feature provides an effective way to manage device registration within organizations while mitigating unauthorized access.

The **Deployment Keys** feature provides an effective way to manage device registration within organizations while mitigating unauthorized access. This feature introduces the concept of a **deployment key** that can be activated, deactivated, and revoked. By utilizing deployment keys, administrators gain control over the credentials used by devices during registration for Secure Access protection. A deployment key is a field in the .mobileconfig file, which is used when registering devices to your organization's network. This feature ensures that only authorized devices are enrolled by requiring an active deployment key for registration.

This feature facilitates seamless device registration and ongoing validation while offering the flexibility to deactivate keys when necessary. If any unauthorized devices try to connect, administrators can swiftly deactivate the current deployment key and delete the suspected devices from the dashboard, ensuring a secure and efficient network environment. The devices will not be able to reregister with the now-deactivated deployment key. Administrators can then activate a new deployment key. This allows IT teams to maintain operational continuity while safeguarding against unauthorized access.

Prerequisites for Device Deployment Management

- For the Global deployment, the Deployment key feature is optional. Enable the Deployment Keys feature (**Connect** > **End User Connectivity** > **Internet Security**) if it is disabled.



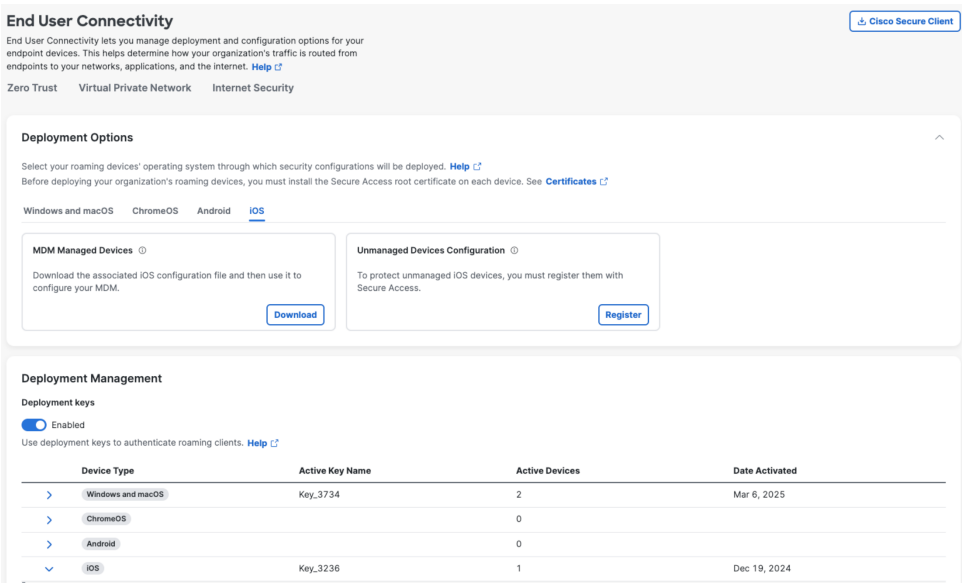
Add and Activate Deployment Key

Provides instructions for completing the Add and Activate Deployment Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

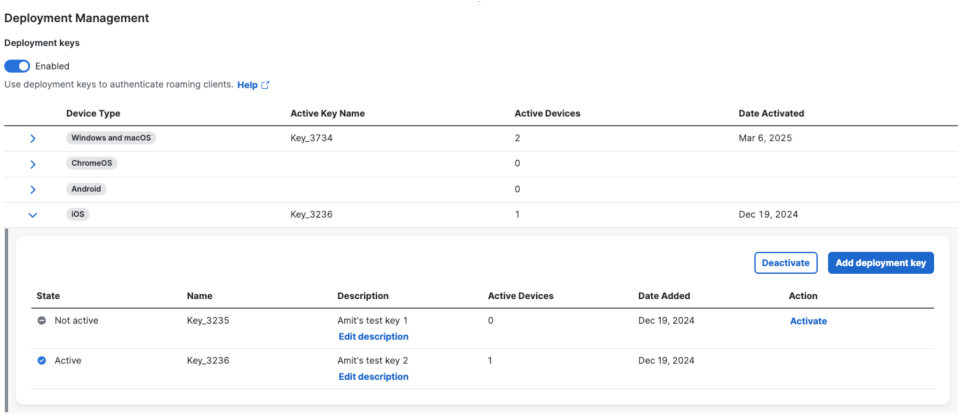
Procedure

1. Navigate to **Connect** > **End User Connectivity**.

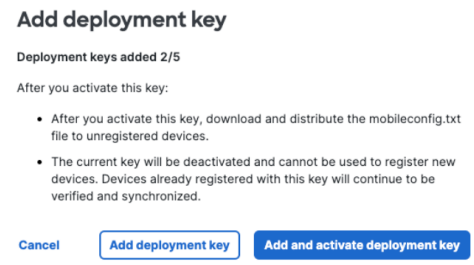
2. Click **Internet Security**.



3. In the **Deployment Management** section, expand the device type (iOS).



4. Click **Add deployment key**.
5. In the **Add deployment key** window, click **Add & activate deployment key** to create and activate a deployment key for inclusion in your organization's .mobileconfig file.



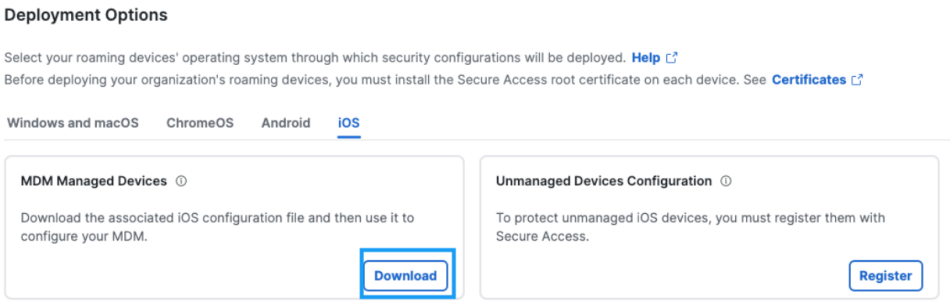
What to do next

You can choose to add the deployment key immediately, but activate it later. In such a scenario, click **Add deployment key**. The deployment key is added to the table. When you are ready to activate the deployment key, click **Activate** in the **Action** column.

Important

- Only one deployment key can be active at a time for each device type.
- You can add up to five deployment keys per device type. To remove a key, contact Cisco support or your Account Manager.
- The deployment key name includes a random number to ensure its uniqueness.

If your Secure Access deployment requires a deployment key, or if your organization has already enabled them, the .mobileconfig file can only be downloaded when there is an active deployment key (see image below). Then, register your supervised iOS device through your Mobile Device Manager (MDM) to Secure Access. For procedures specific to an MDM, see Register Your iOS Device Through Your MDM to Secure Access.



Manage Deployment Key Compromise

Provides instructions for completing the Manage Deployment Key Compromise workflow in Cisco Secure Access. If you determine that a key has been compromised, take action to protect your network's integrity and security.

If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

This section outlines the necessary actions to be taken to ensure network security and continuity, including deactivating compromised keys, understanding the effects on existing clients, and steps for activating and distributing a new key for secure device registration.

Procedure

1. **Deactivate the Compromised Key**: Deactivate the compromised key. This action prevents any further device registrations using the deactivated key, ensuring that your network remains secure.

   To deactivate a deployment key, perform the following steps:

   a. Navigate to **Connect** > **End User Connectivity**.

   b. Click **Internet Security.**

   c. In the **Deployment Management** section, expand the device type.

   d. Click **Deactivate** in the **Action** column.

      Upon deactivating the compromised deployment key, it is important to consider its implications on both existing clients and the registration of new devices:

      - **Effect on existing clients**: It's important to note that deactivating a key will not disrupt the operation of clients already using it. These clients will continue to function normally, minimizing any potential impact on your current network operations.

- **Limitations for new devices**: However, deactivated keys cannot be used for registering new devices. This means that any device attempting to register itself with the deactivated key will be unable to do so.

> **Note**
>
> Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, provided the deployment key in their .mobileconfig file is active.

2. **Activate the new deployment key**: To facilitate the registration of new devices, you must activate a different deployment key. This new key will replace the compromised one and will be used for future device registrations.
3. **Download a new profile**: After the new key is activated, download a new profile, specifically the .mobileconfig file. This file contains the updated information, including the new active deployment key.
4. **Distribute the new profile to new devices**: Distribute the updated .mobileconfig profile to any new devices that need to connect to your network. This ensures that they have the correct and secure credentials to register and operate within your network environment.
5. **Update the .mobileconfig file for registered devices**: Devices that are already registered and require an update to the .mobileconfig file will automatically receive changes once the configuration is updated in the MDM.

Delete a Deployment Key

Provides instructions for completing the Delete a Deployment Key workflow in Cisco Secure Access. To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

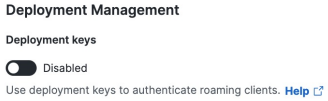
> **Caution**
>
> Deleting a Deployment Key is a high-impact action. It immediately disconnects existing roaming devices and stops new device registrations and synchronizations. Ensure that you have identified the correct key before performing any management actions.

If an active deployment key is deleted, administrators must generate a new key, download the updated profile, and distribute the profile to all affected devices to restore connectivity. For detailed recovery steps, see Manage deployment key compromise.

Reverting to Using Legacy Deployment Implementation

Provides instructions for completing the Reverting to Using Legacy Deployment Implementation workflow in Cisco Secure Access. If needed, you can revert to the legacy registration mechanism by disabling the Deployment Keys feature (Connect End User Connectivity Internet Security).

If needed, you can revert to the legacy registration mechanism by disabling the **Deployment Keys** feature (**Connect** > **End User Connectivity** > **Internet Security**).



Procedure

1. After disabling the Deployment Keys feature, devices that are currently using the last activated deployment key will continue to be protected by Secure Access. However, new devices will not be able to register with the deactivated deployment key.
2. To revert to the legacy registration mechanism, download the updated .mobileconfig file, which will no longer include the deployment key. New devices can now register using the legacy method.

Backward Compatibility

Describes Backward Compatibility in Cisco Secure Access. This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

For example, on iOS:

- Cisco Security Connecter for iOS Release 1.7.3 or earlier will continue to use the legacy registrationToken-based process for registration, regardless of whether a deployment key is present.
- Cisco Security Connecter for iOS Release 1.7.4 or later will use the deployment key for registration, regardless of whether the registrationToken is present. If the deployment key is unavailable, the legacy registrationToken will be used for registration instead.

Meraki Registration

Describes Meraki Registration in Cisco Secure Access. For Meraki administrators, once you have deployed the Cisco Security Connector (CSC), use the Meraki dashboard to deploy the app to devices using the instructions in the Meraki document Apple Volume Purchase Program (VPP).

For Meraki administrators, once you have deployed the Cisco Security Connector (CSC), use the Meraki dashboard to deploy the app to devices using the instructions in the Meraki document Apple Volume Purchase Program (VPP). When your endpoints have registered with Secure Access, they will appear in the dashboard. For support, contact Meraki support.

Anonymization

Describes Anonymization in Cisco Secure Access. Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes.

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized both in the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Register with Meraki

Provides instructions for completing the Register with Meraki workflow in Cisco Secure Access. You must log in to your Secure Access dashboard as an administrator.

Note

Meraki's Hide App Feature Incompatibility

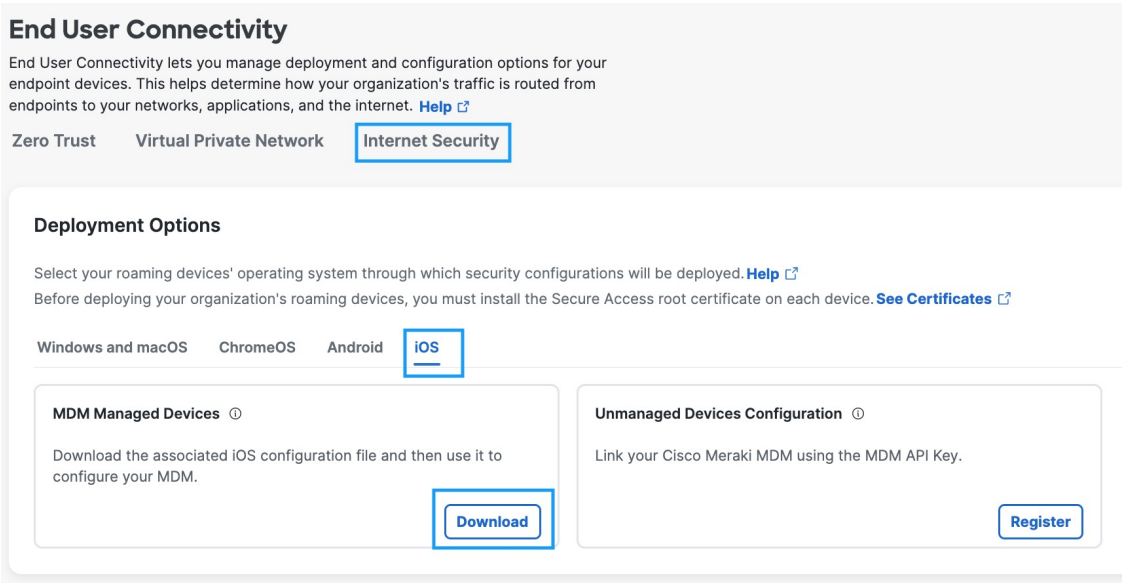
The Cisco Security Connector is not compatible with Meraki's hide app feature.

Before you begin

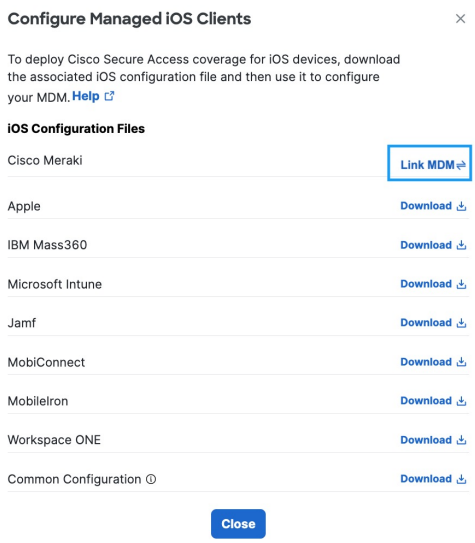
- You must log in to your Secure Access dashboard as an administrator.
- Review and ensure that you meet the Cisco Security Connector requirements.
- Have a Meraki API key. For more information about acquiring a Meraki API key, see Cisco Meraki Dashboard API.
- Install the Cisco Security Connector app on your iOS device (typically through MDM).
- Configure Meraki as required so that it can push configuration information to both CSC and Secure Access. For information about configuring Meraki, see the Meraki documentation.
- If deploying to a supervised device, ensure that the names in Secure Access match the Meraki portal name, enable device name updates under **Restrictions** > **iOS Restrictions (Supervised)** > **Allow Modification of Device Name (Enable)** > **Keep Device Name Up-to-Date with Dashboard (Enable)**.

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.



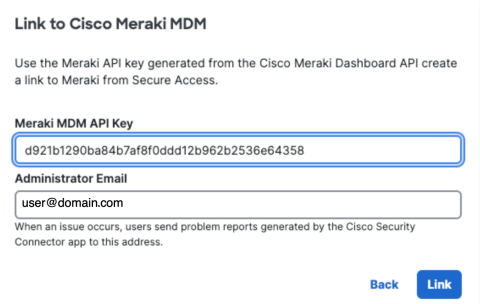
2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Link MDM**.



4. Add your **Meraki MDM API Key**, optionally add an **Administrator Email**, and click **Link**.

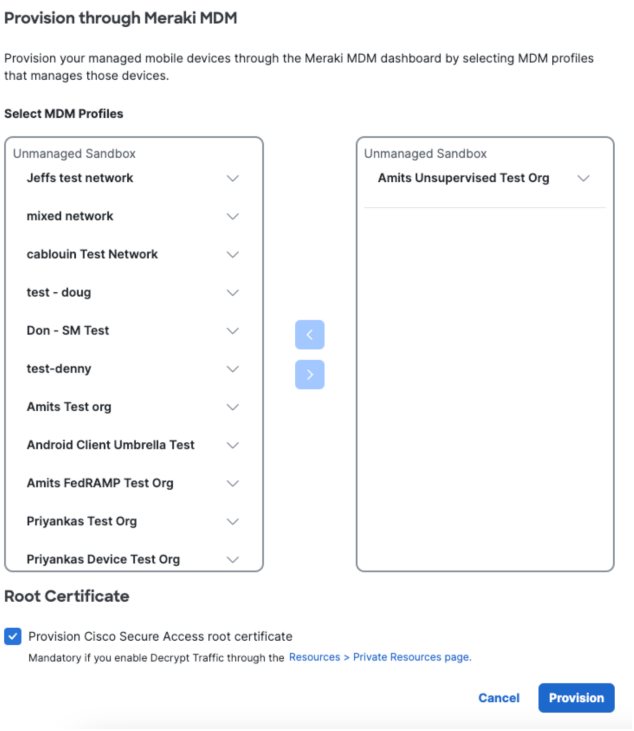
   This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.

> **Note**
>
> You acquire a Meraki MDM API key from the Meraki dashboard. For more information, see Cisco Meraki Dashboard API.



5. In the **Provision through Meraki MDM** modal, select your MDM Profiles.

> **Note**
>
> While you can deploy more than one profile to an iOS device, if you try to deploy more than one profile with Secure Access applied, an error will occur and the second profile will not be applied. You can safely deploy a second profile with only Secure Access applied to a device that has an existing profile that only has Clarity applied.

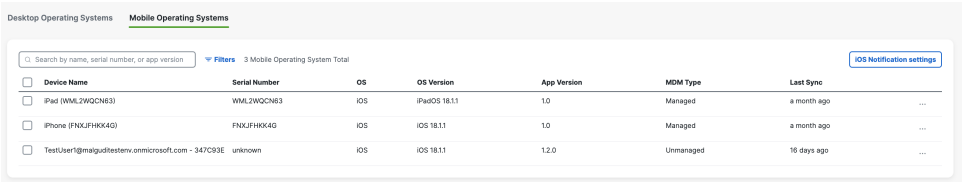


6. Check **Provision Cisco Secure Access Root Certificate**.

   The root certificate is required to perform SSL decryption for the intelligent proxy and also helps avoid error messages when visiting blocked pages.

7. Click **Save**.

   If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



Verify Push of Profile Config

Provides instructions for completing the Verify Push of Profile Config workflow in Cisco Secure Access. Once you have provisioned Secure Access, verify the push of the Secure Access Profile Config on your Meraki dashboard.

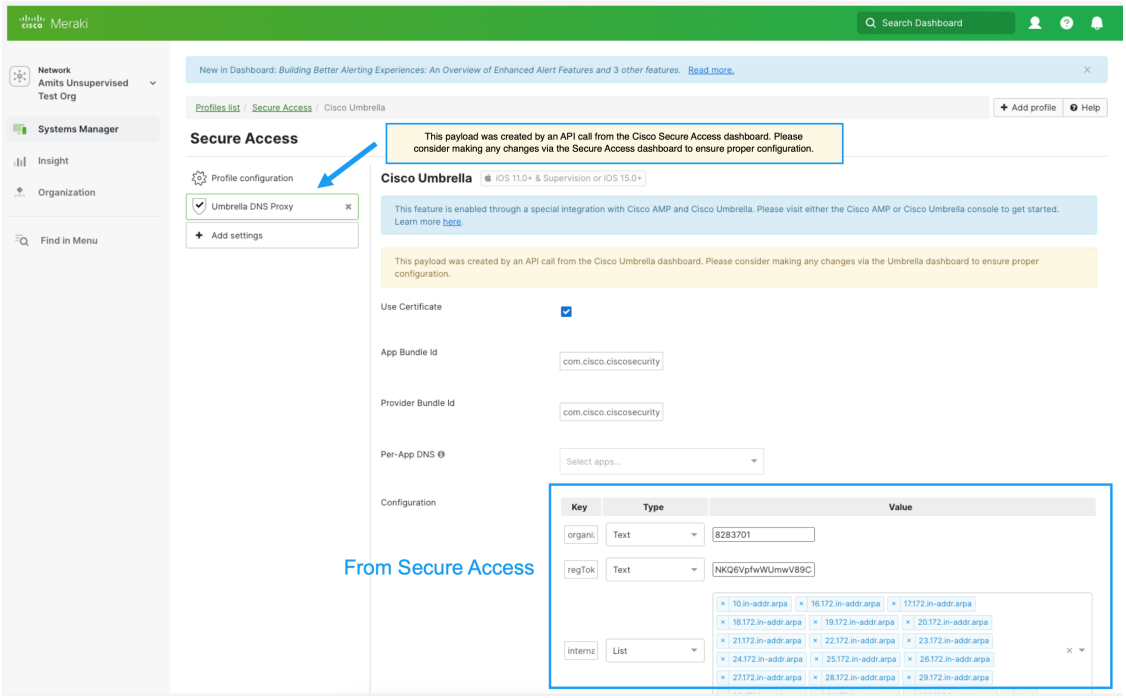
Once you have provisioned Secure Access, verify the push of the Secure Access Profile Config on your Meraki dashboard.

Procedure

In Meraki, navigate to **Systems Manager** > **Settings**.

You'll see an Secure Access DNS Proxy profile with configuration settings populated from Secure Access.

What to do next



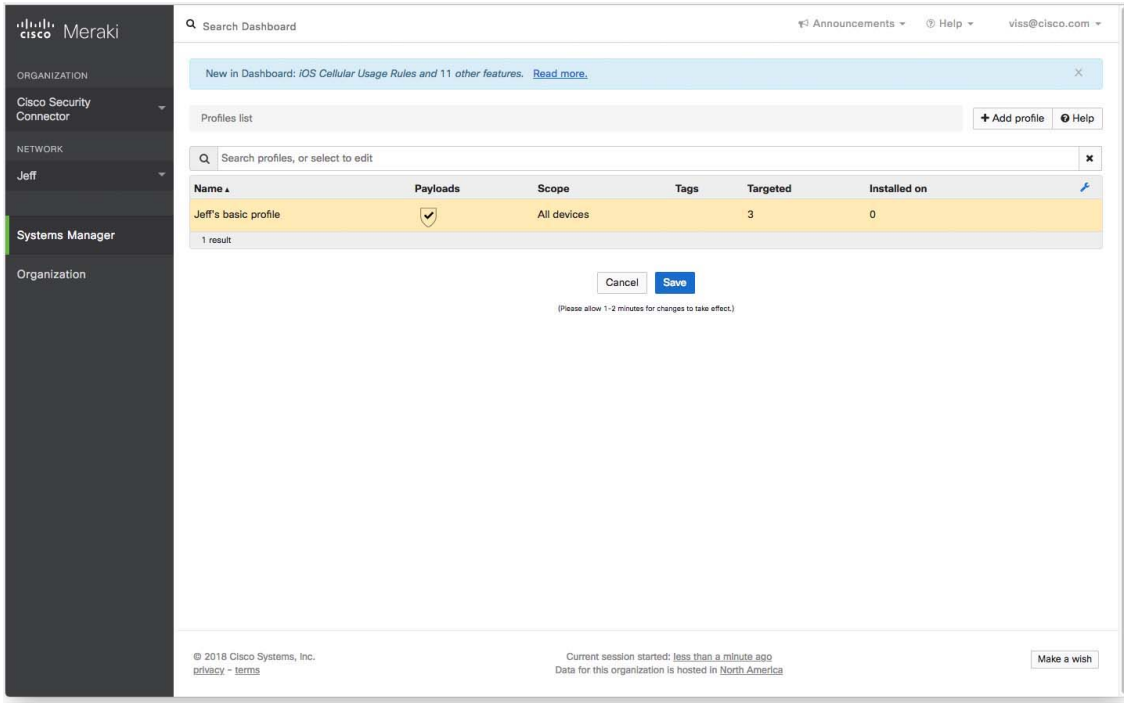
Anonymize Your Device

Provides instructions for completing the Anonymize Your Device workflow in Cisco Secure Access. Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes.

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number.

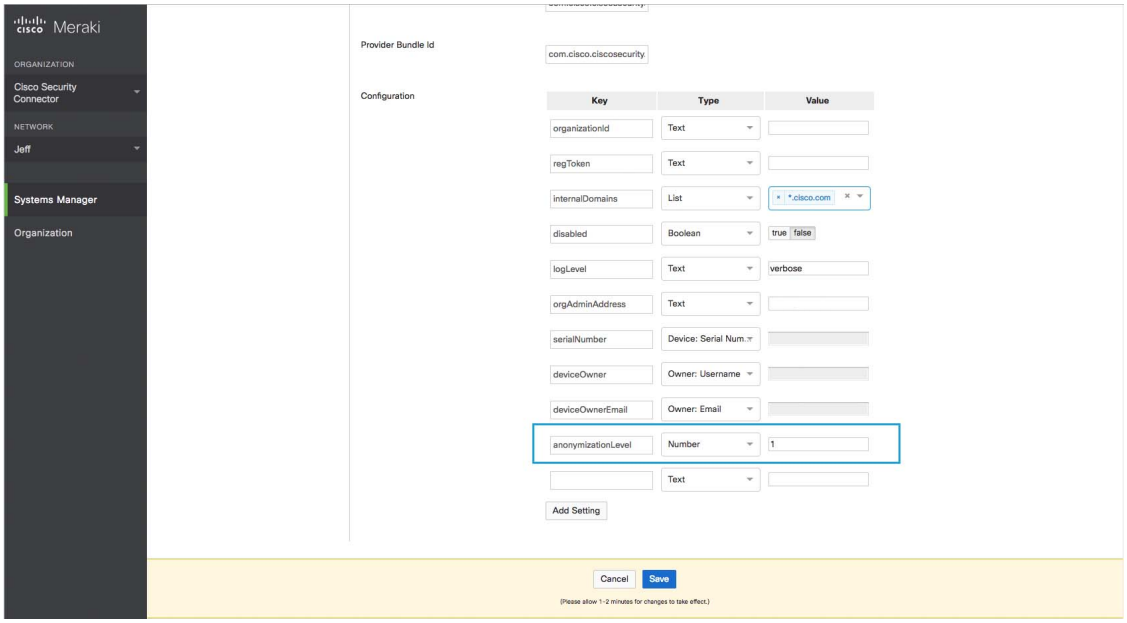
Procedure

1. In Meraki, navigate to **Systems Manager** > **Settings** and then select your profile.



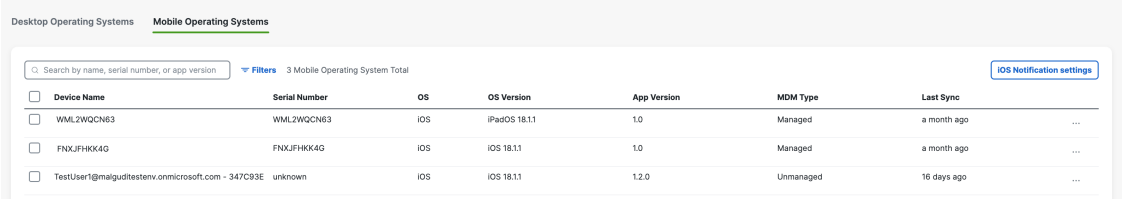
2. Under **Value** for **anonymizationLevel**, type **1**.

> **Note**
>
> If **anonymizationLevel** is not listed, click **Add Setting** and add a **Key** with the value **anonymizationLevel** and **Number** with the value of **1**. A value of **0** turns anonymization off.



3. Click **Save**.

   Meraki pushes settings to Secure Access, and Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



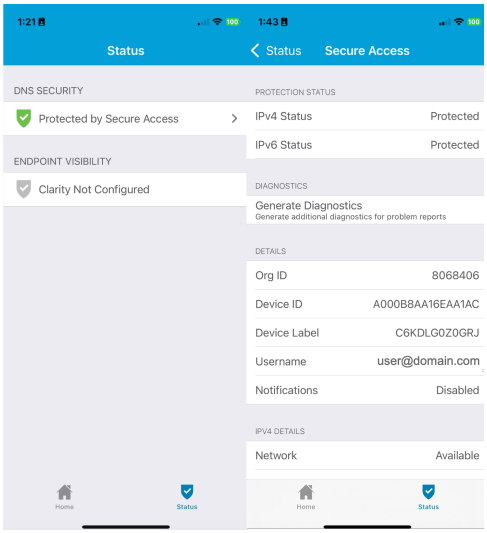
Verify Secure Access on Your Device

Provides instructions for completing the Verify Secure Access on Your Device workflow in Cisco Secure Access. On your iOS device, verify that Secure Access is operational.

On your iOS device, verify that Secure Access is operational.

Procedure

1. In the CSC app, click the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Verify Secure Access with Meraki

Describes Verify Secure Access with Meraki. You can verify the configuration and operation of Secure Access on your Meraki-administrated device.

You can verify the configuration and operation of Secure Access on your Meraki-administrated device.

Prerequisites

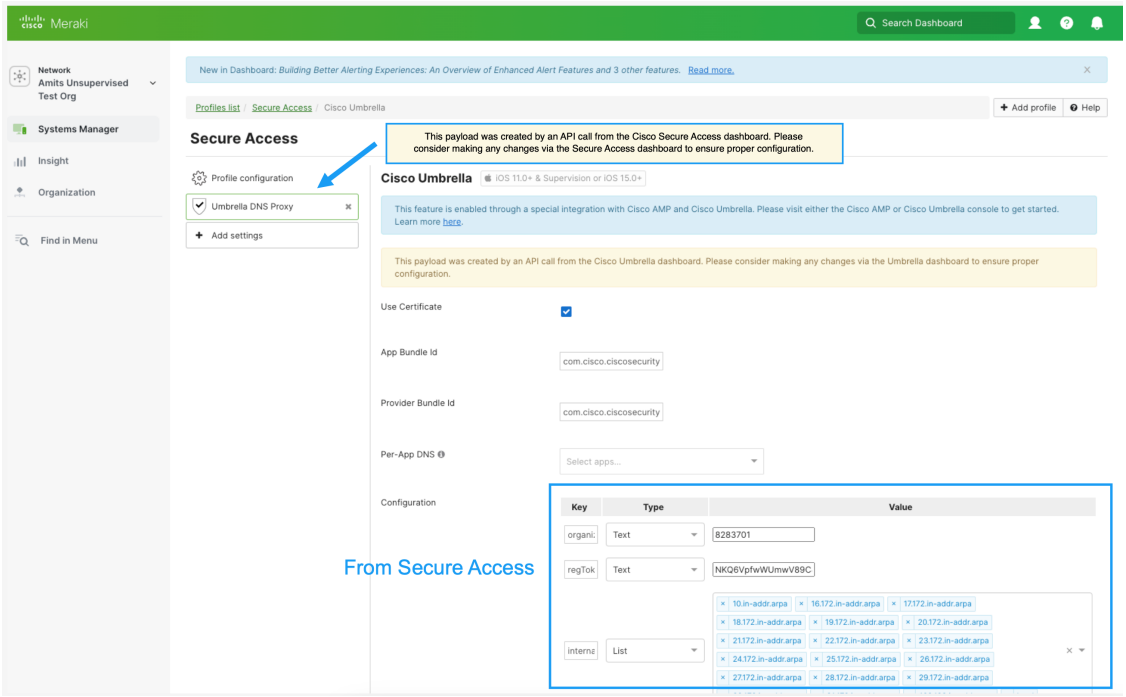
- Meraki is registered in Secure Access. See Meraki Registration.

Procedure

Describes Procedure in Cisco Secure Access. In the Meraki SM, your profile now has a new setting: “Umbrella DNS Proxy”.

In the Meraki SM, your profile now has a new setting: “Umbrella DNS Proxy”.

This setting was pushed from the Secure Access dashboard.



Verify Local Operation on the iOS Device

Provides instructions for completing the Verify Local Operation on the iOS Device workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Check the Meraki Profile.

Procedure

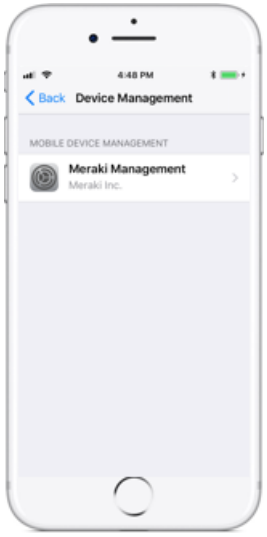
1. On your phone, tap **Settings** > **General**.

   The MDM profile is listed under Device Management.



2. Tap **Meraki Management**.

   Verify that **Web Content Filter** is now listed. This is your confirmation that the updated profile has been pushed to the iOS device.



3. Tap **More Details**.

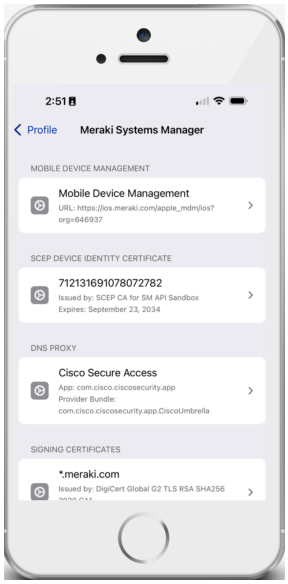


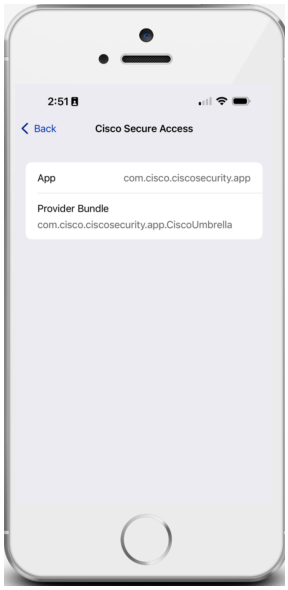
4. Tap **Cisco Umbrella DNS Proxy**.

   Notice the App: **com.cisco.ciscosecurity**

   The Provider Bundle: **com.cisco.ciscosecurity.CiscoUmbrella**

   These indicate that the profile is working correctly.





5. Navigate back to Meraki Management and tap **Restrictions**.



6. Tap **Web Content Filter**.



7. Review the Plugin Bundle ID **com.cisco.ciscosecurity**. This indicates that the profile is working correctly.

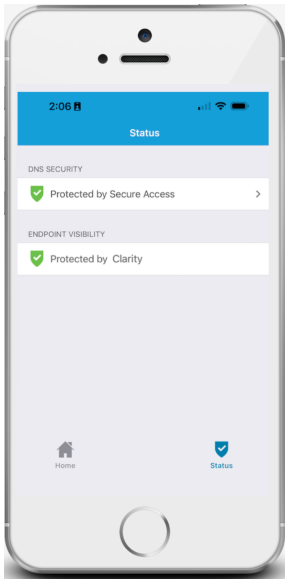


Verify Secure Access

Provides instructions for completing the Verify Secure Access workflow in Cisco Secure Access. In the Cisco Security Connector (CSC) app, tap Status.

Procedure

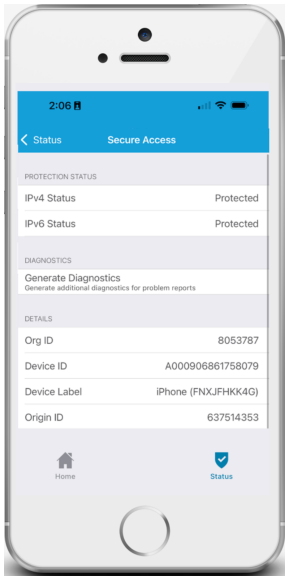
1. In the Cisco Security Connector (CSC) app, tap **Status**.



2. Tap **Protected by Secure Access**.

   CSC lists connection details.

> **Note**
>
> IPv6 is listed as Unprotected because this device does not have an IPv6 address.



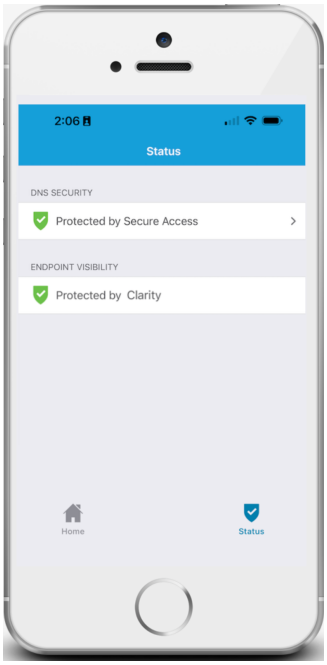
Verify Clarity

Provides instructions for completing the Verify Clarity workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco Security App

Procedure

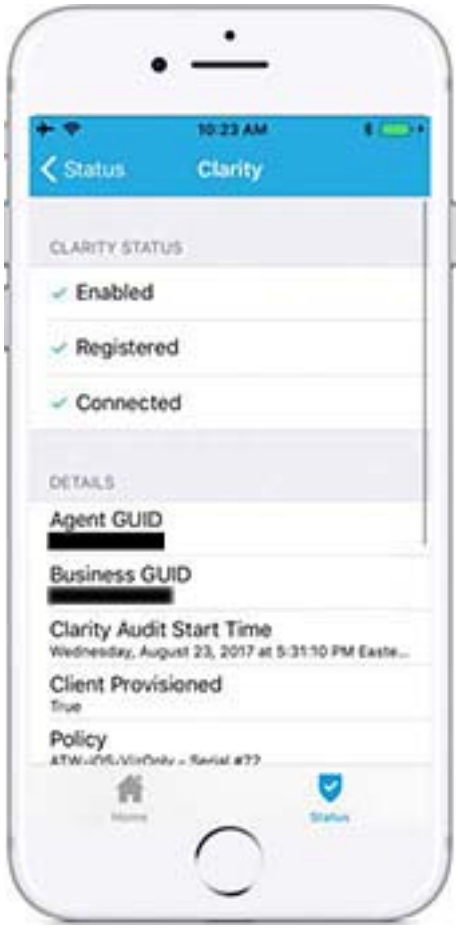
1. In the Cisco Security app, tap **Status**.



2. Tap **Protected by Clarity**.

   The CSC list connection details.

> **Note**
>
> If CSC is enabled and registered, but not connected, generate some new web traffic and try again.



Upgrade the Cisco Security Connector

Describes Upgrade the Cisco Security Connector in Cisco Secure Access. When an updated version of the Cisco Security Connector is available, it will be pushed to the App Store and updated from there.

When an updated version of the Cisco Security Connector is available, it will be pushed to the App Store and updated from there.

Uninstall the Cisco Security Connector

Describes Uninstall the Cisco Security Connector in Cisco Secure Access. For information about removing apps from managed devices, see Meraki SM's documentation.

For information about removing apps from managed devices, see Meraki SM's documentation.

Meraki Documentation

Describes Meraki Documentation in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

For more information about Meraki, see the following:

- Creating and Deleting Dashboard Networks
- Apple MDM Push Certificate
- Apple Volume Purchase Program (VPP)
- Apple Device Enrollment Program (DEP) or Enrolling and Supervising iOS Devices using Apple Configurator 2.0
- Cisco Meraki Dashboard API
- Using Tags in Systems Manager

Register an iOS Device Through Apple Configurator 2

Describes Register an iOS Device Through Apple Configurator 2 in Cisco Secure Access and explains Anonymization and Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, updating it to include your iOS device's serial number, and then adding this XML file to your Apple Configurator system, the Apple Configurator system is able to push configuration information to both Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring your specific Mobile Device Management (MDM) system, see your MDM system's documentation.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Prerequisites

- The Cisco Security Connector requirements
- Apple Configurator 2.5 or higher. For information about configuring Apple Configurator, see Configurator documentation. For support, contact Apple support.

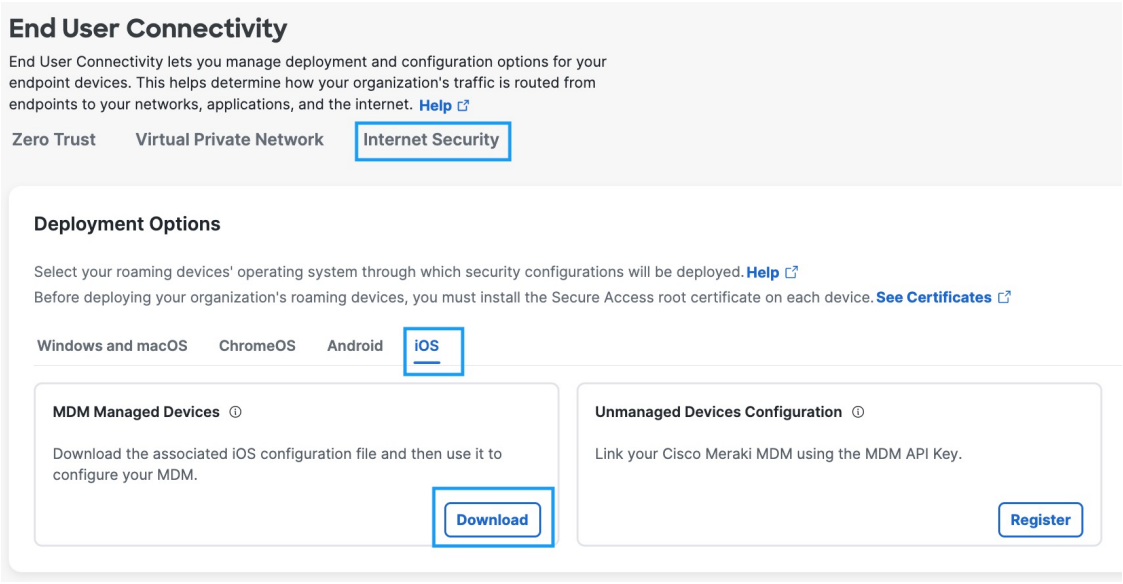
Procedure for Registering an iOS Device Through Apple Configuration 2

Provides instructions for completing the Procedure for Registering an iOS Device Through Apple Configuration 2 workflow in Cisco Secure Access. Navigate to Connect End User Connectivity and click Internet Security.

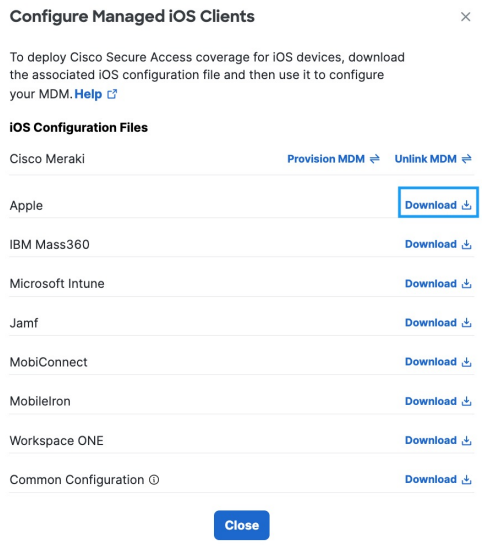
> **Note**
>
> You must log in to your Secure Access dashboard as an administrator.

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.



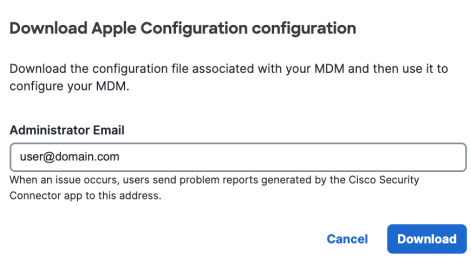
2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   Your browser downloads a `mobileconfigApple.xml` file to your computer.

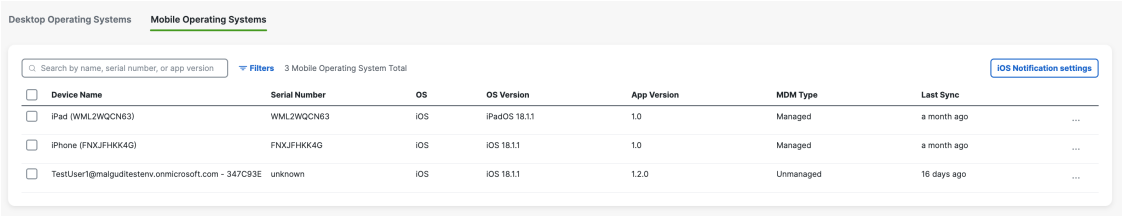
   This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.



5. Open the downloaded XML file and update the line **{SERIAL_NUMBER}** with the device's serial number. For example, 1234567890
6. Change the file extension to .mobileconfig from .xml.
7. Use Apple Configurator 2 to add this profile to your device.
8. Repeat this process for each iOS device. You must download and manually update an XML file for each device you want to register.

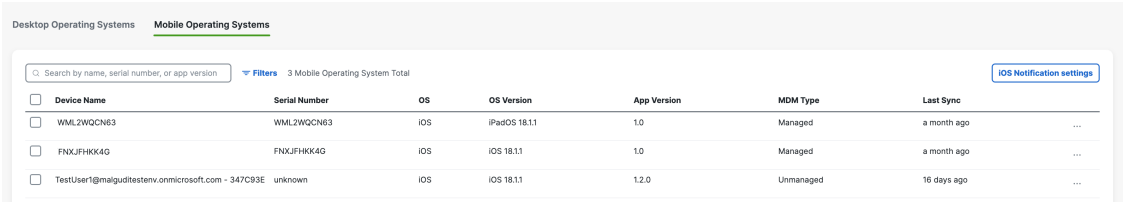
   For information about configuring Configurator 2, see Configurator 2's documentation.

   If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



What to do next

If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

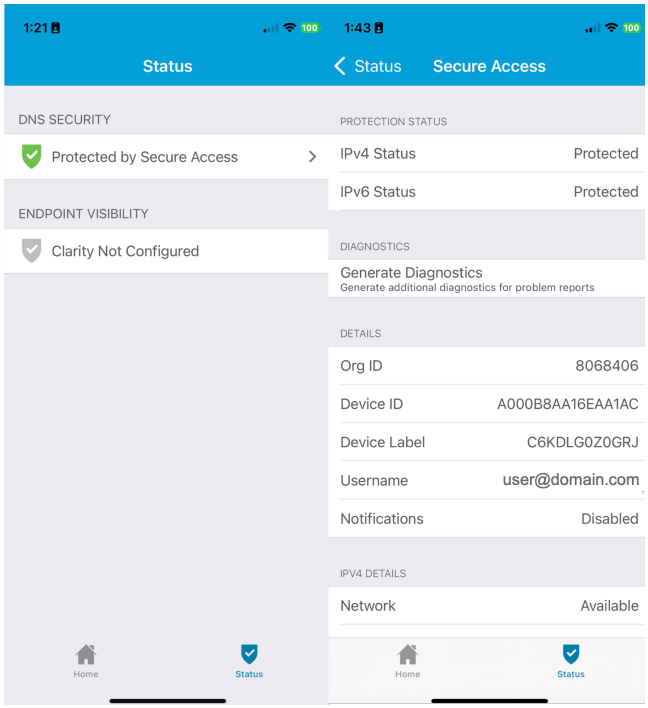
Verify Secure Access on Your Device

Provides instructions for completing the Verify Secure Access on Your Device workflow in Cisco Secure Access. On your iOS device, verify that Secure Access is operational.

On your iOS device, verify that Secure Access is operational.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



IBM MaaS360 Registration

Describes IBM MaaS360 Registration in Cisco Secure Access and explains Anonymization and Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting part of its contents into your MaaS360 system, MaaS360 is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring MaaS360, see IBM's MaaS360 documentation.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Prerequisites

- The Cisco Security Connector requirements
- MaaS360 portal version 10.70 or higher.
- You must first configure your MaaS360 MDM system. Configure MaaS360 as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring MaaS360, see MaaS360 documentation. For support, contact IBM MaaS360 support.

Important

Your device name must be no more than 50 characters long. Longer device names result in registration failure.

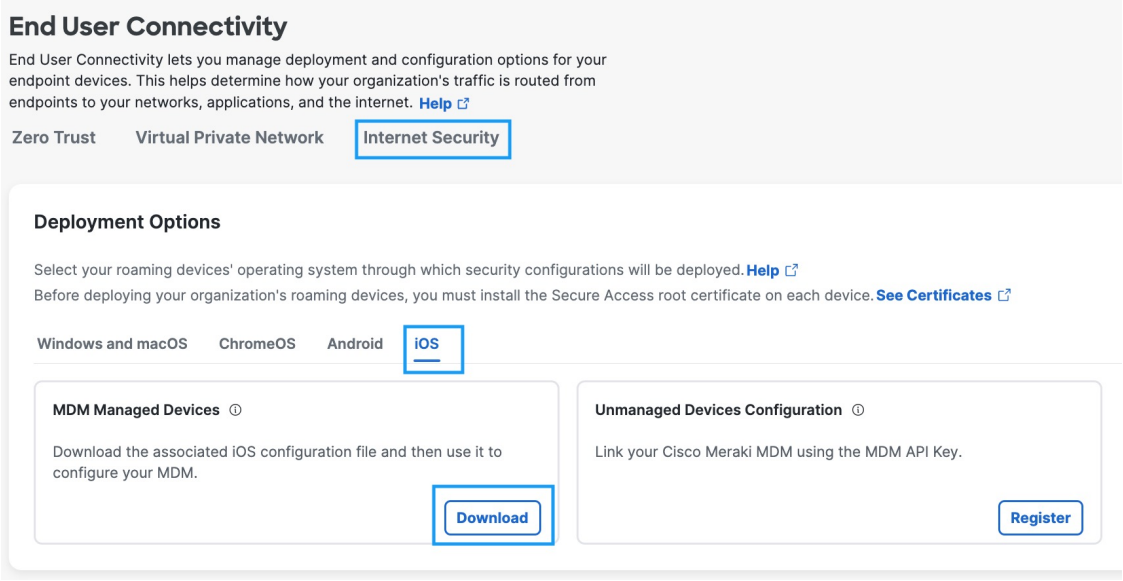
Procedure for Registering IBM MaaS360 MDM Solution

Provides instructions for completing the Procedure for Registering IBM MaaS360 MDM Solution workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

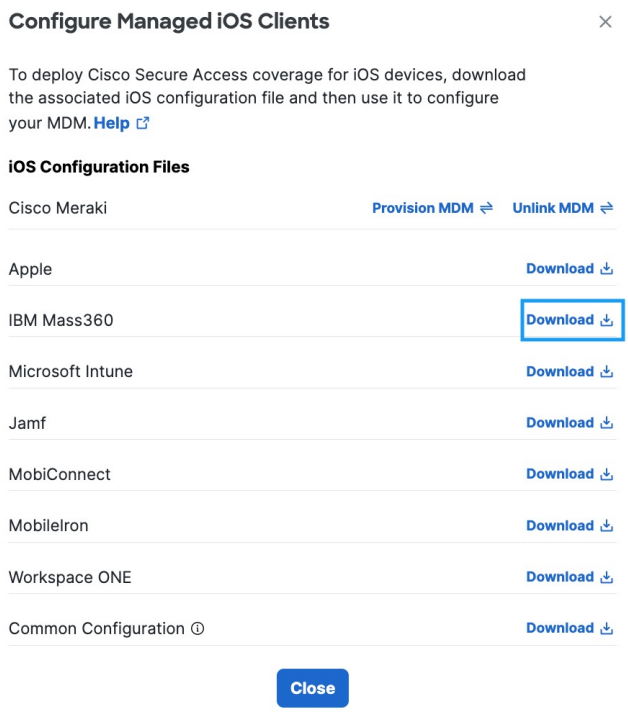
> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

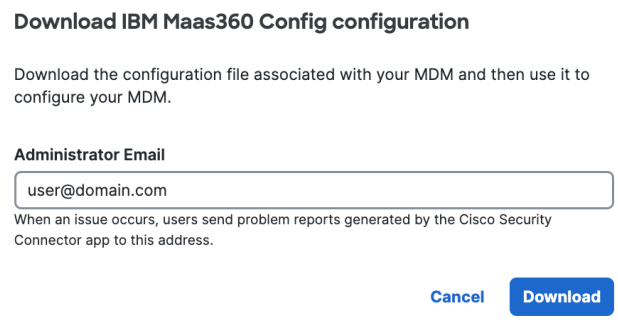


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.



5. To anonymize devices, add the following lines to the downloaded XML file, at the same level as the other CSC configuration parameters.

```
<key>anonymizationLevel</key>
<integer>1</integer>
```

> **Note**
>
> 1 turns anonymization on. 0 turns anonymization off.

Example:

```
...
   <key>serialNumber</key>
```

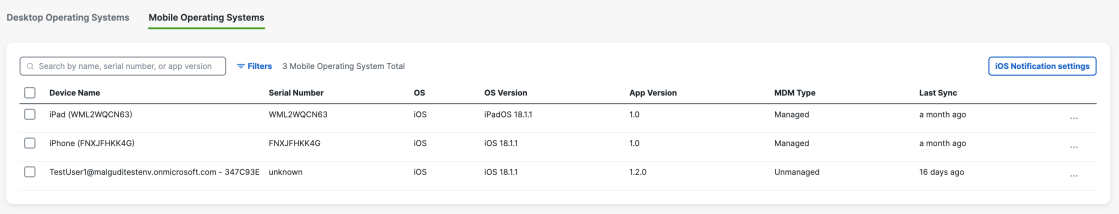
```
    <string>$DEVICE_SN$</string>
    <key>anonymizationLevel</key>
    <integer>1</integer>
</dict>
```

6. Use the contents of the edited XML file to create a new .mobileconfig file, then upload that file to your MDM profile.

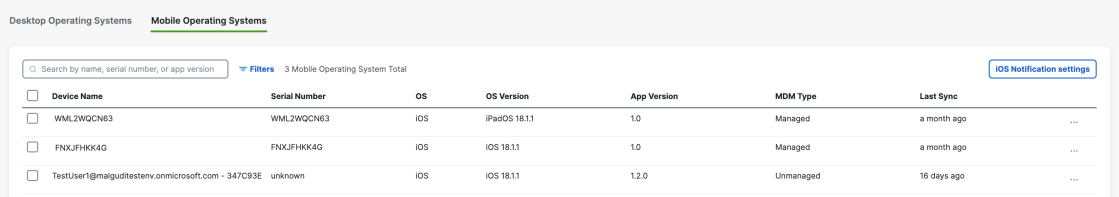
   For details about configuring your specific MDM system, see your MDM system's documentation.

What to do next

Your mobile device registers with Secure Access and is listed at **Resources** > **Roaming DevicesMobile Operating Systems**. The CSC app on your mobile device updates to connect to Secure Access. Your mobile device is now protected.



If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



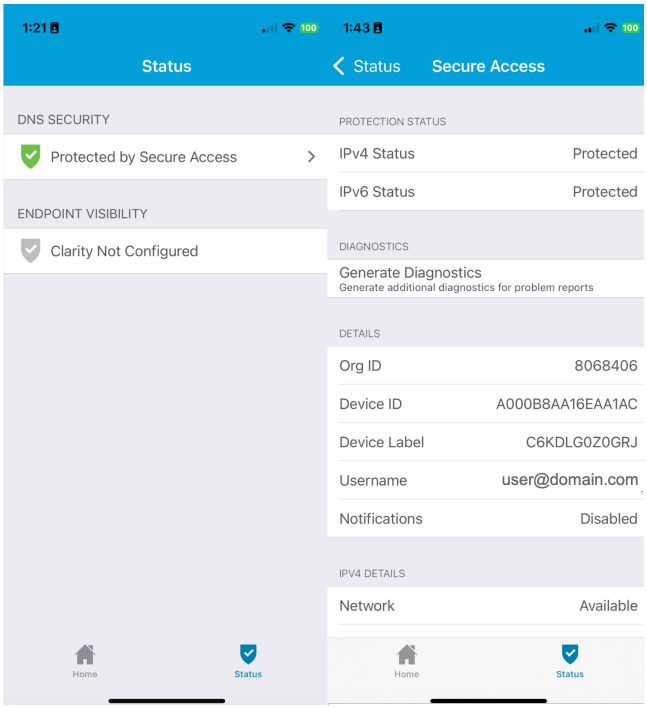
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS Device

Provides instructions for completing the Verify Secure Access on Your iOS Device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Intune Registration

Describes Intune Registration in Cisco Secure Access. By downloading an XML file from Secure Access and then uploading it to your Intune system, Intune is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access.

By downloading an XML file from Secure Access and then uploading it to your Intune system, Intune is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring Intune, see Intune's documentation.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Prerequisites

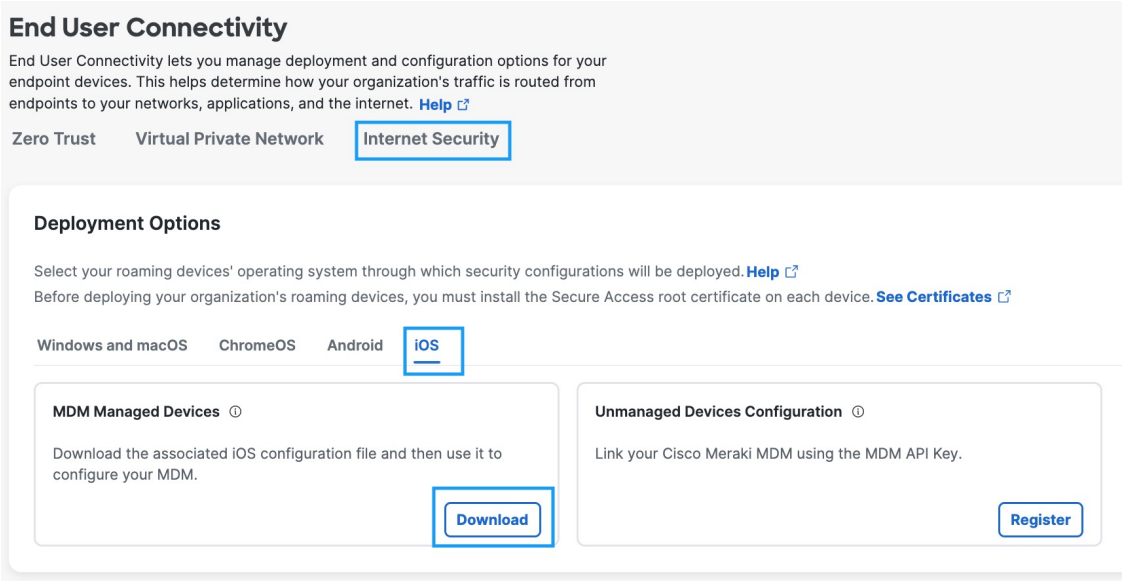
- The Cisco Security Connector requirements
- You must first configure your Intune MDM system. Configure Intune as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring Intune, see Intune documentation. For support, contact Intune support.

Procedure for Registering Intune MDM Solution

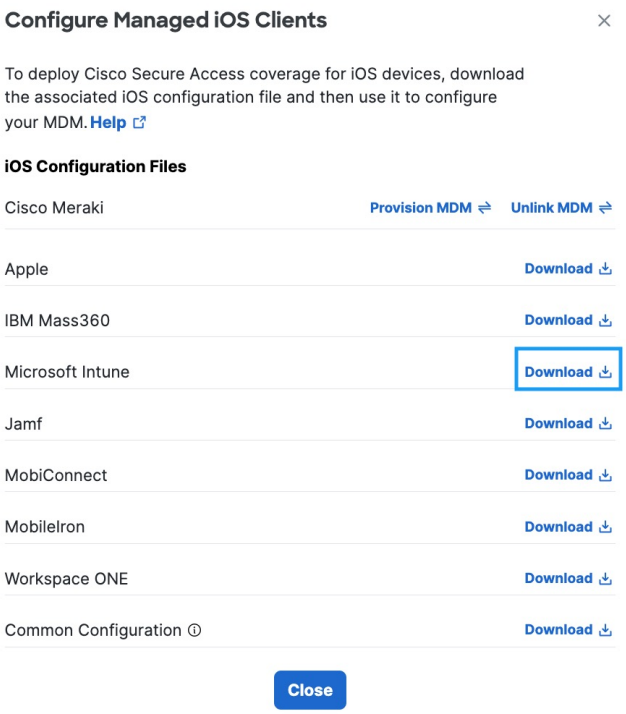
Describes Procedure for Registering Intune MDM Solution in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.



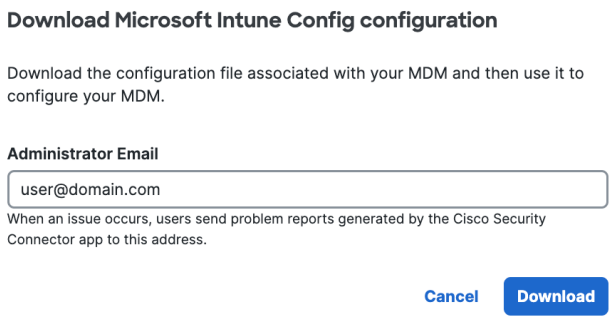
2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

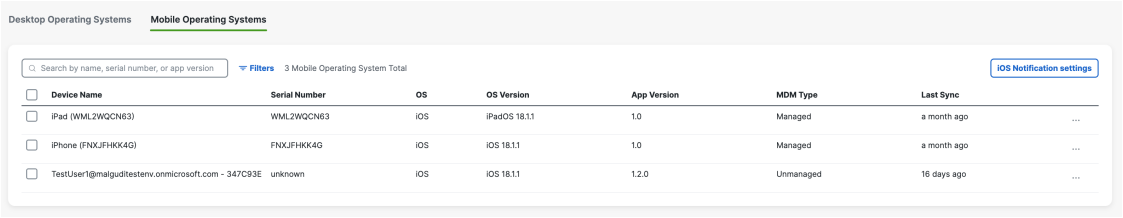
Your browser downloads a `mobileconfigMicrosoft Intune.xml` file to your computer.

This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.

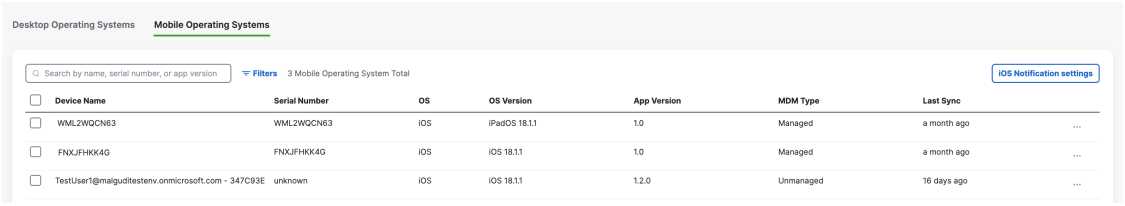


5. In Intune, create your profile. When prompted for a profile type, choose **Custom** and upload the `mobileconfigMicrosoft Intune.xml` file downloaded from Secure Access.

   If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



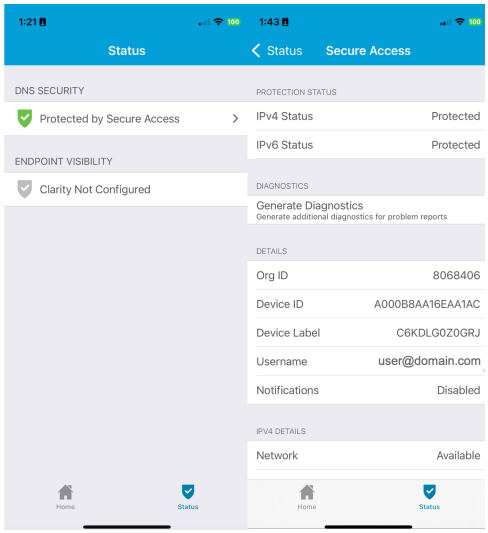
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS Device

Provides instructions for completing the Verify Secure Access on Your iOS Device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Jamf Registration

Describes Jamf Registration in Cisco Secure Access and explains Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting part of its contents into your Jamf system, Jamf is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring Jamf, see Jamf's documentation.

Prerequisites

- The Cisco Security Connector requirements
- Jamf Pro 10.2.0 or higher.
- You must first configure your Jamf MDM system. Configure Jamf as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring Jamf, see Jamf documentation. For support, contact Jamf support.

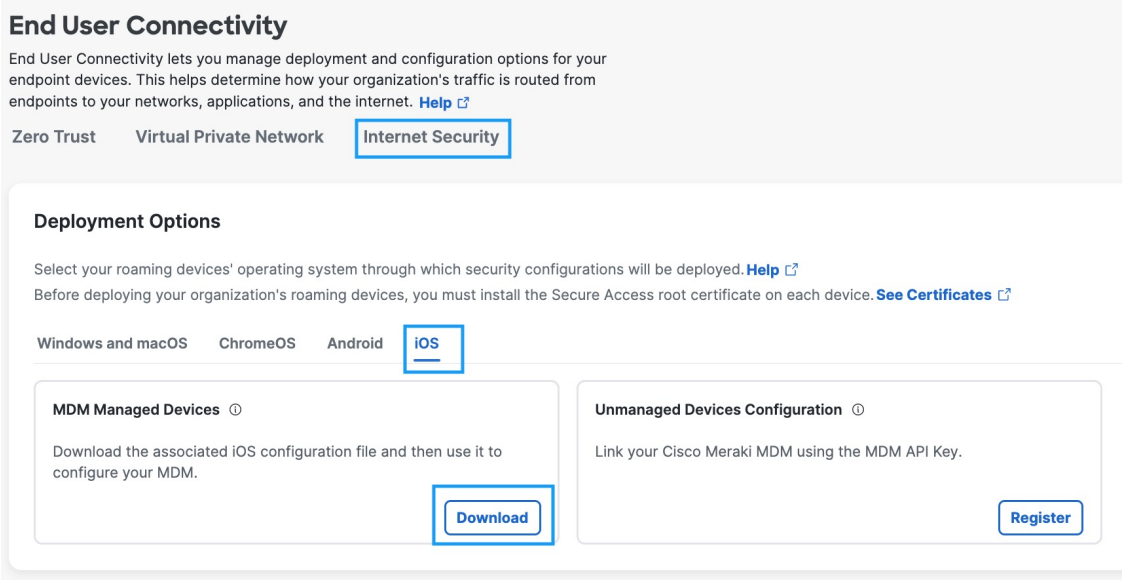
Procedure for Registering Jamf MDM Solution

Provides instructions for completing the Procedure for Registering Jamf MDM Solution workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

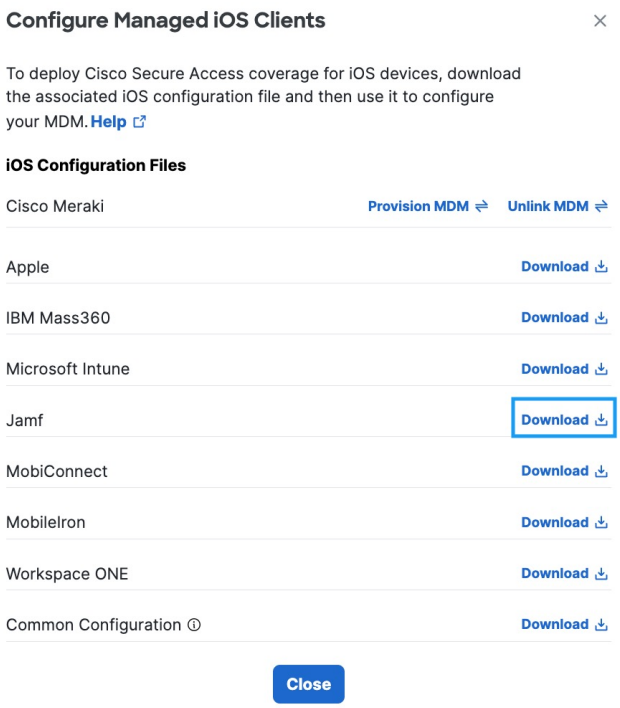
> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

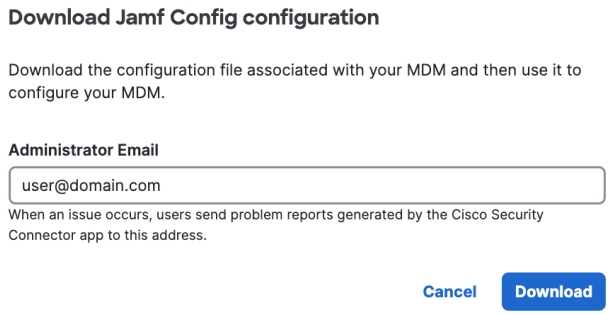


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **!** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.



5. Copy and paste the XML code between the **

   ** comments into your MDM profile.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
<!-- Jamf - copy from here to paste into the Jamf UI to provision a DNS proxy
 -->
        <dict>
                ...
        </dict>
<!-- Jamf - end copy -->
```

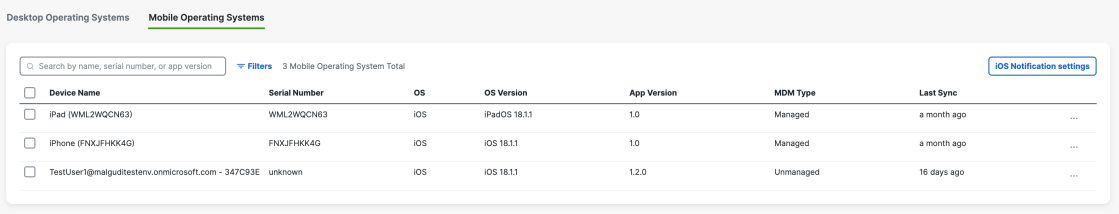
> **Note**
>
> If you are using Jamf School, then update the XML code to:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>PayloadContent</key>
     <array>
<!-- Jamf - copy from here to paste into the Jamf School UI to provision a
DNS proxy -->
        <dict>
             <key>serialNumber</key>
             <string>%SerialNumber%</string>
        </dict>
<!-- Jamf - end copy -->
```

6. In your new profile, applied for the CSC group, choose **Custom Settings**, and then **Configure**. Paste the edited XML here.

What to do next

If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



Alternate Configuration

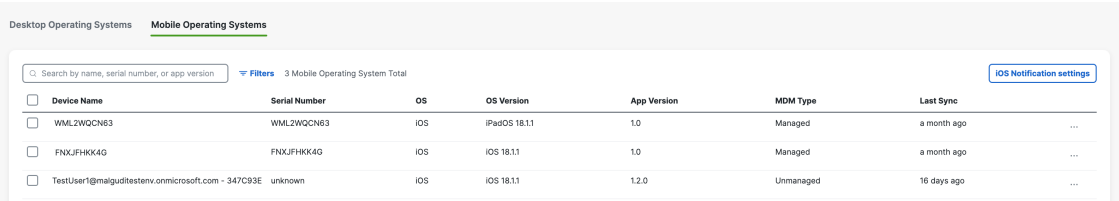
Alternatively, instead of copying and pasting the XML code (as in steps 4 and 5 above), you can upload the config file directly to JAMF. In JAMF, navigate to **Devices** > **Configuration Profiles** > **Upload** and upload the .mobileconfig file.

Anonymization

Describes Anonymization in Cisco Secure Access. Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes.

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Existing active devices anonymize with 24 hours. New devices anonymize immediately.



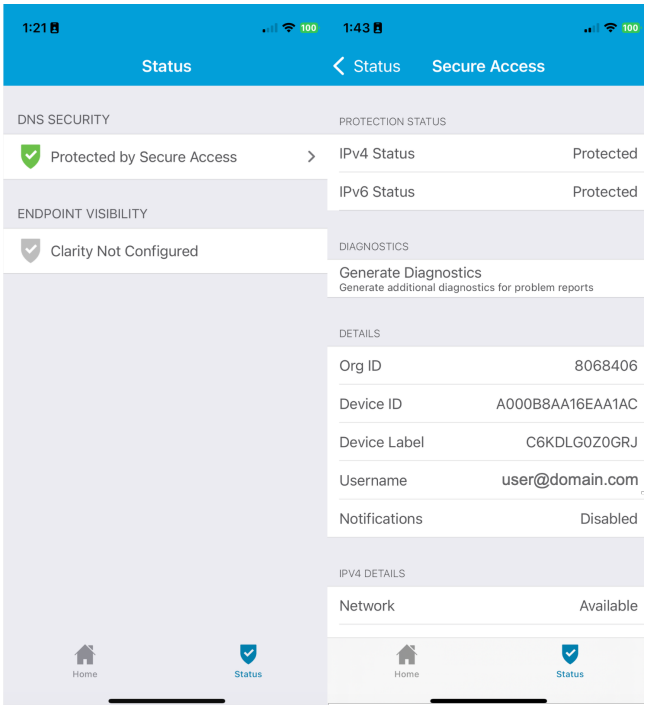
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS Device

Provides instructions for completing the Verify Secure Access on Your iOS Device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



MobileIron Registration

Describes MobileIron Registration in Cisco Secure Access and explains Prerequisites and Anonymization. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting its contents into your MobileIron system, MobileIron is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring your specific Mobile Device Management (MDM) system, see your MDM system's documentation.

> **Note**
>
> Secure Access supports MobileIron Enterprise Mobility Management (EMM) On-Prem and Cloud versions 9.4 or higher.

Prerequisites

- The Cisco Security Connector requirements
- MobileIron EMM On-Prem and Cloud versions 9.4 or higher.
- You must first configure your MobileIron MDM system. Configure your MobileIron system as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring MobileIron, see MobileIron documentation. For more information about adding the CSC to your MobileIron MDM, see MobileIron Configuration and MobileIron documentation. For support, contact MobileIron support.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

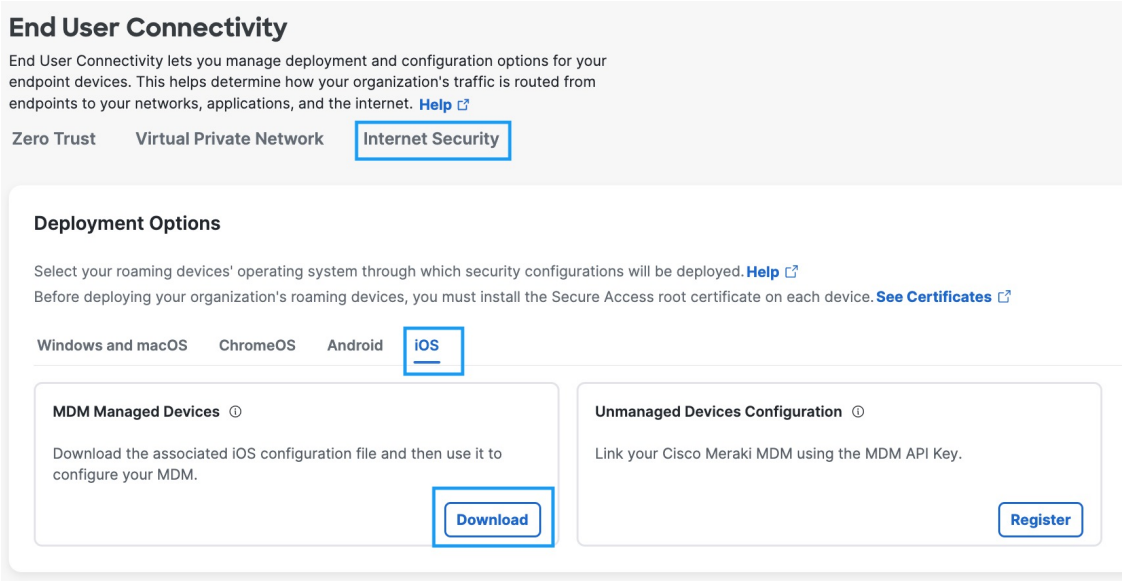
Procedure for Registering MobileIron MDM Solution

Provides instructions for completing the Procedure for Registering MobileIron MDM Solution workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

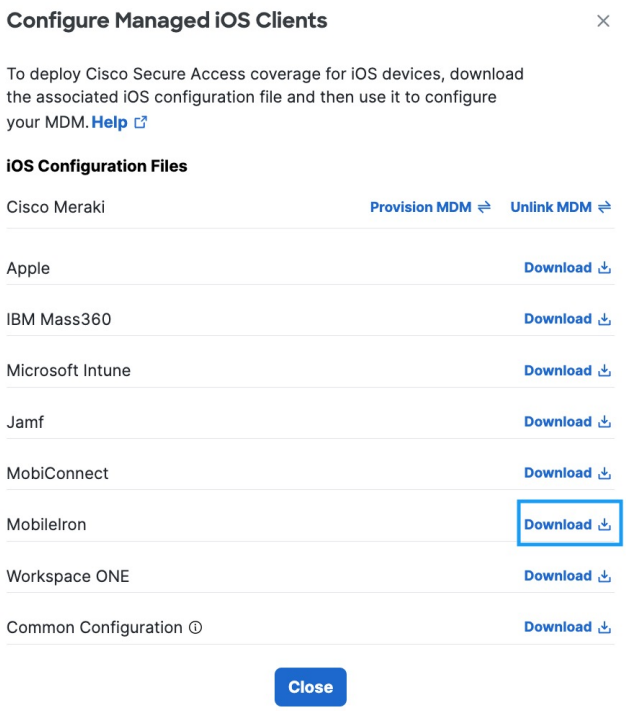
> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

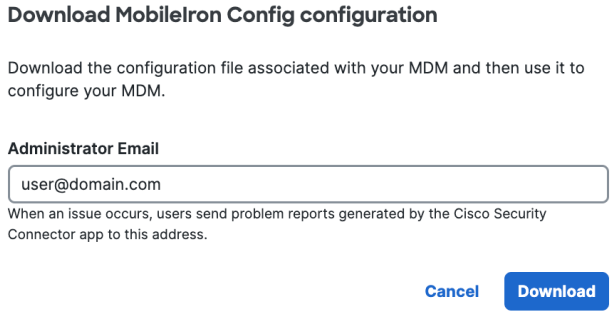


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **!** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.

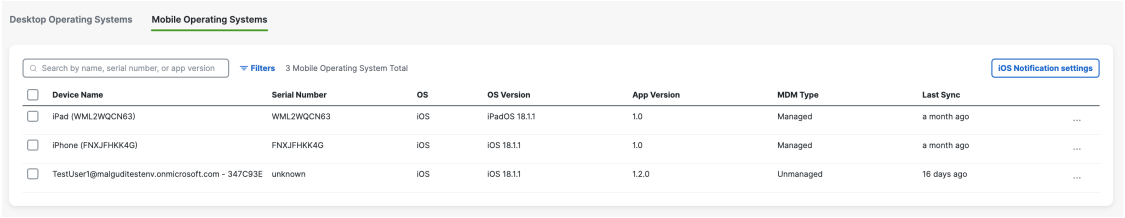


5. Copy the contents of the downloaded XML file and paste or upload it into your MDM profile (Policies & Configs > Configurations > iOS and MacOS > iOS Only). For information about configuring the MobileIron system, see MobileIron documentation.

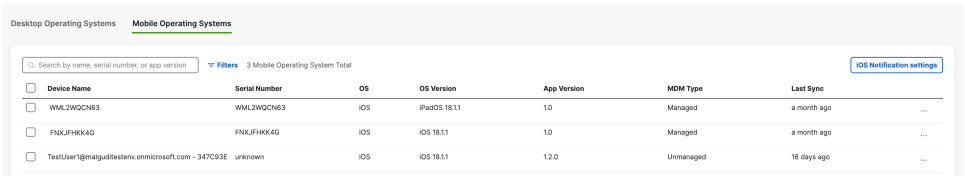
> **Note**
>
> For MobileIron cloud, "$DEVICE_SN$ may need to be replaced with "$".

What to do next

If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



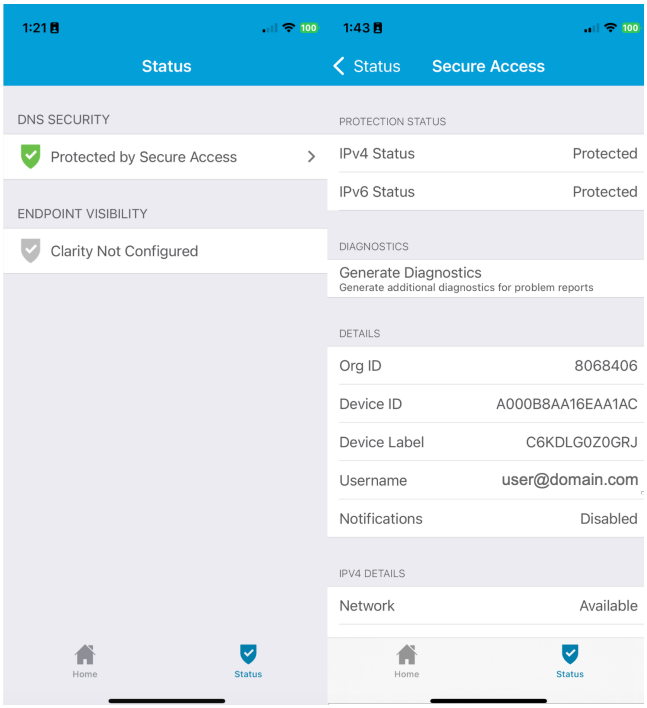
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS device

Provides instructions for completing the Verify Secure Access on Your iOS device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



MobileIron Configuration

Provides instructions for completing the MobileIron Configuration workflow in Cisco Secure Access. Before registering MobileIron with Secure Access, add the Cisco Security Connector (CSC) to your MobileIron MDM.

To download the Secure Access root certificate and deploy that to the mobile device for registration, follow these instructions.

From the **AMP** console:

Before you begin

Before registering MobileIron with Secure Access, add the Cisco Security Connector (CSC) to your MobileIron MDM.

Procedure

1. Navigate to **Accounts** > **Business**.
2. Under **Features**, click **MDM Integration**.
3. From the **MDM Type** drop-down list, select **MobileIron**.
4. Click **Save**.

MobileIron Cloud Configuration

Provides instructions for completing the MobileIron Cloud Configuration workflow in Cisco Secure Access. Currently, the MobileIron download on the dashboard supports the on-premise version only.

Currently, the MobileIron download on the dashboard supports the on-premise version only. The cloud version utilizes different device variables than the on-premise software. Deployment is very similar to on-premise, with several exceptions. To deploy to MobileIron Cloud:

Ensure your admin email address is added to the dashboard under the **Mobile Devices** page, **settings** option.

Procedure

1. Download the Mobile Iron profile from the Secure Access dashboard.
2. Replace the variable "$DEVICE_SN$" to $
3. Replace the variable "$DEVICE_MAC$" to $ (This is only used for the Clarity component of the CSC, not used for the Secure Access component. If you do not use Clarity, there will be no $DEVICE_MAC$ to replace.)

MobileIron On-Prem Configuration

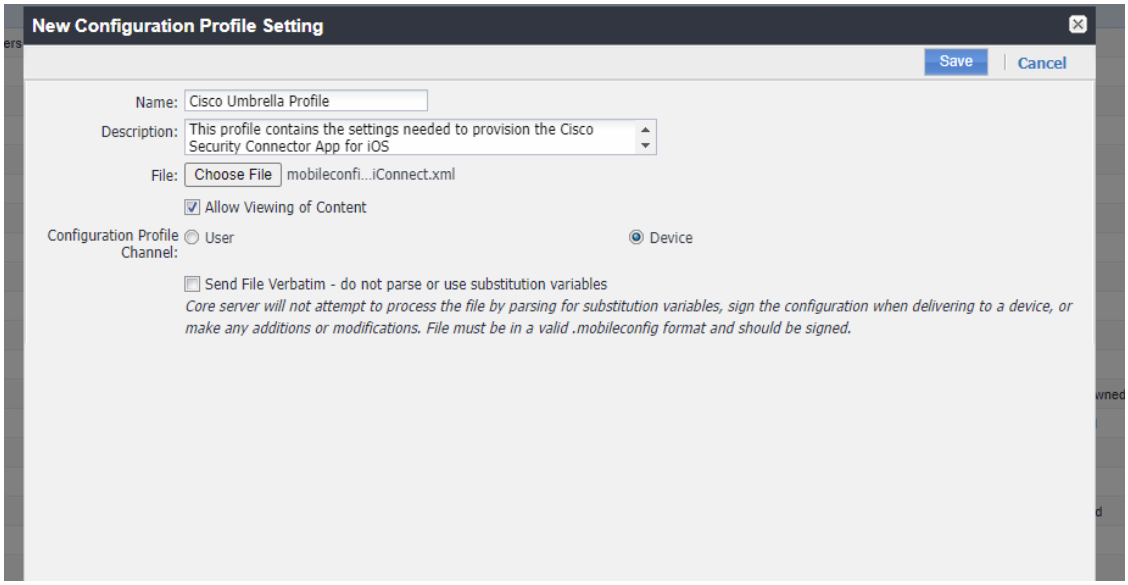
Provides instructions for completing the MobileIron On-Prem Configuration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

To deploy to On-Prem version:

Ensure your admin email address is added to the dashboard under the **Mobile Devices** page, **settings** option.

Procedure

1. Create a new label.
2. Download the Cisco Security Connector app from the iTunes store through MobileIron Core Console, and apply it to the label.
3. Obtain licenses through the Apple DEP webpage.
4. Create a certificate configuration with Cisco Umbrella Certificate uploaded, and then apply it to the label.
5. Create the **Configuration Profile** and upload the correct XML file, and then apply it to the label.



MobiConnect Registration

Describes MobiConnect Registration in Cisco Secure Access and explains Prerequisites and Anonymization. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting part of its contents into your MobiConnect system, MobiConnect is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring MobiConnect, see MobiConnect's documentation.

Prerequisites

- The Cisco Security Connector requirements
- MobiConnect version 30.1 or higher.
- You must first configure your MobiConnect MDM system. Configure MobiConnect as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring MobiConnect, see MobiConnect documentation. For support, contact MobiConnect support.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

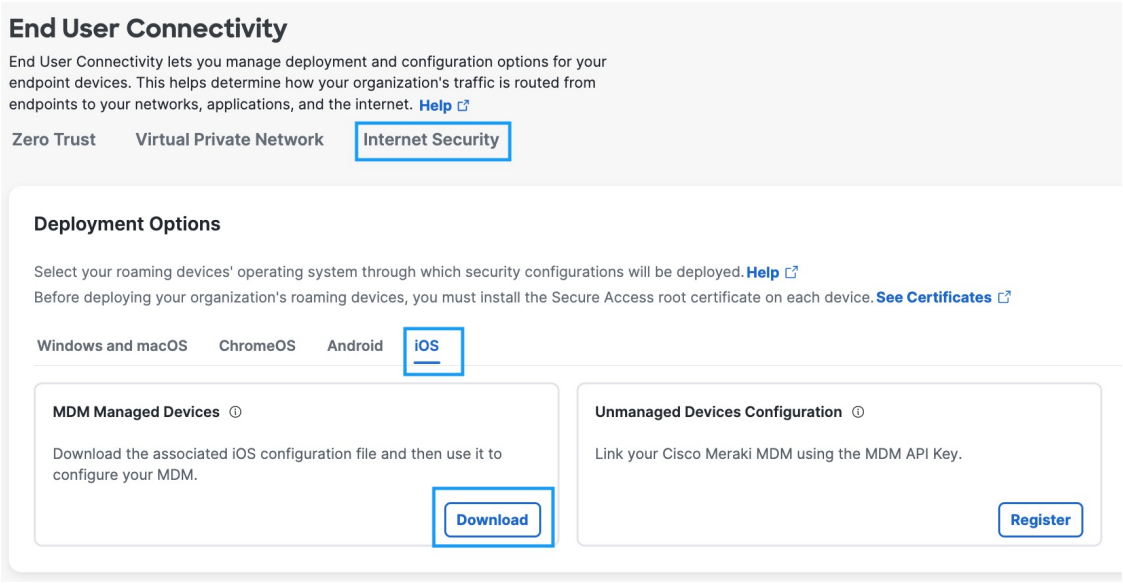
Procedure for Registering MobiConnect MDM Solution

Provides instructions for completing the Procedure for Registering MobiConnect MDM Solution workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

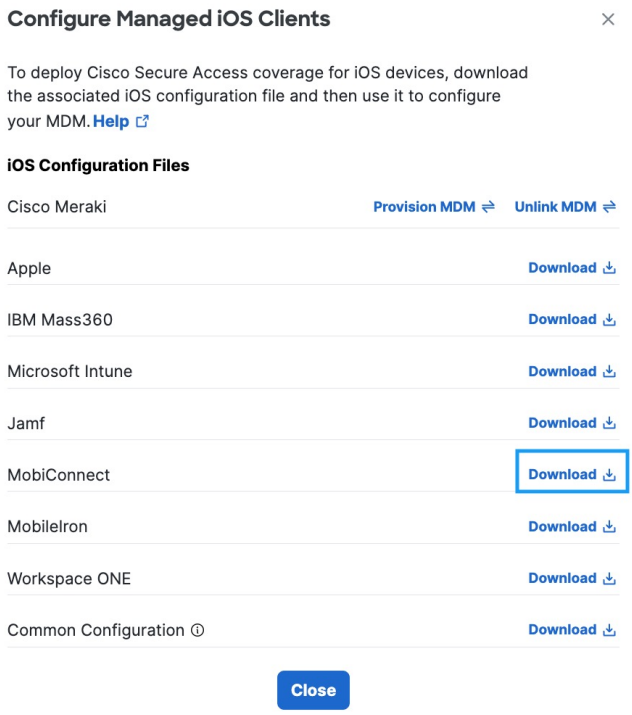
> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

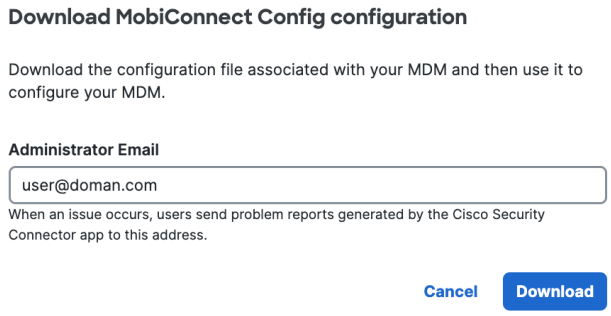


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **!** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.

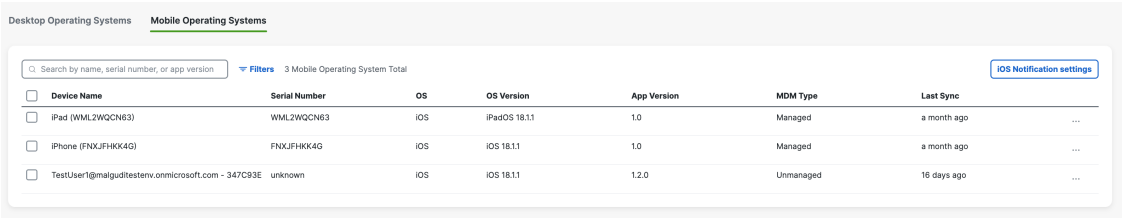


5. Copy and paste the XML code between the **<!-- MobiConnect... -->** comments into your MDM profile.

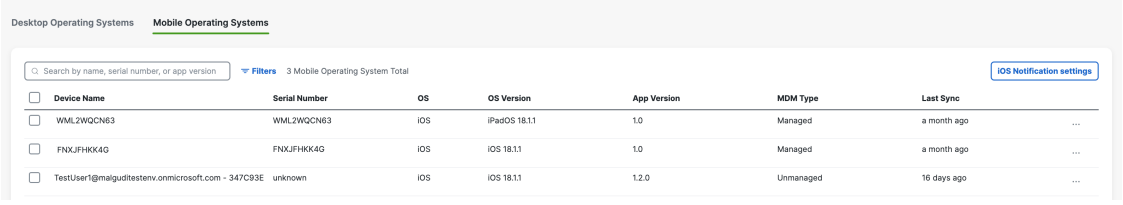
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
<!-- MobiConnect - copy from here to paste into the MobiConnect UI to provision
 a DNS proxy -->
            <dict>
              ...
            </dict>
<!-- MobiConnect - end copy -->
```

6. In your new profile, applied for the CSC group, choose **Custom Settings**, and then **Configure**. Paste the edited XML here.

   If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



   If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



What to do next

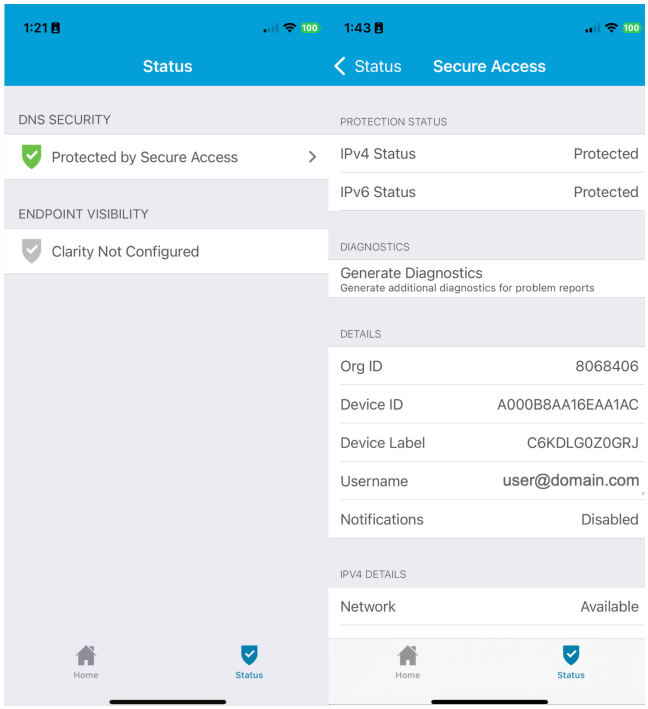
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS Device

Provides instructions for completing the Verify Secure Access on Your iOS Device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Workspace ONE Registration

Describes Workspace ONE Registration in Cisco Secure Access and explains Prerequisites and Anonymization. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting part of its contents into your Workspace ONE system, Workspace ONE is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring Workspace ONE, see Workspace ONE's documentation.

> **Note**
>
> **Version Information**
>
> Secure Access supports Workspace ONE Mobility Management On-Prem and Cloud versions 9.2 or higher. Workspace ONE was previously known as AirWatch.

Prerequisites

- The Cisco Security Connector requirements
- Workspace ONE Mobility Management On-Prem and Cloud versions 9.2 or higher.
- You must first configure your Workspace ONE MDM system. Configure Workspace ONE as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring Workspace ONE, see Workspace ONE documentation. For support, contact Workspace ONE support.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

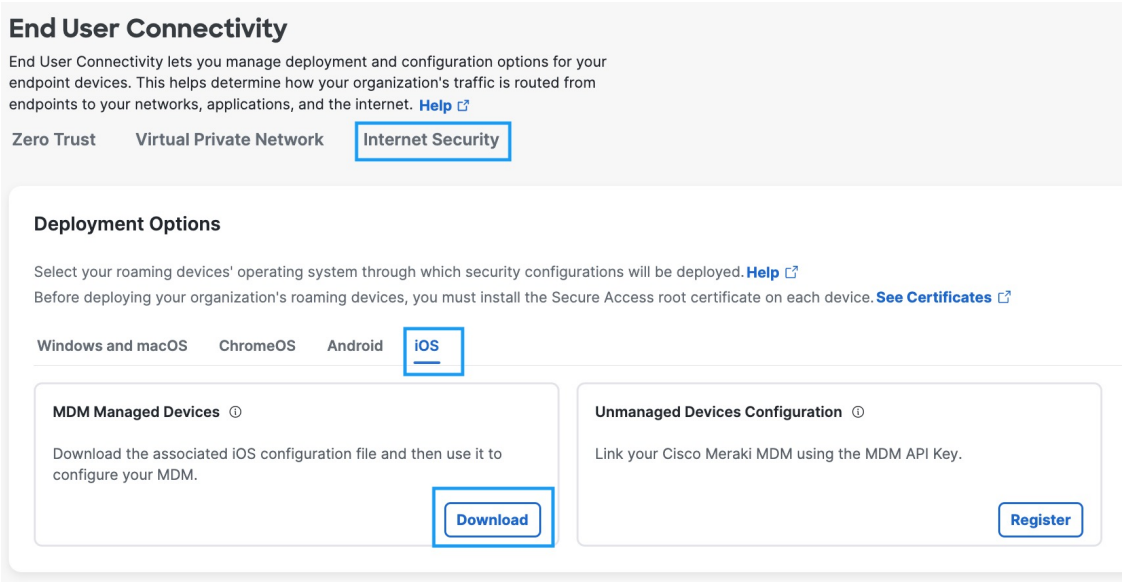
Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

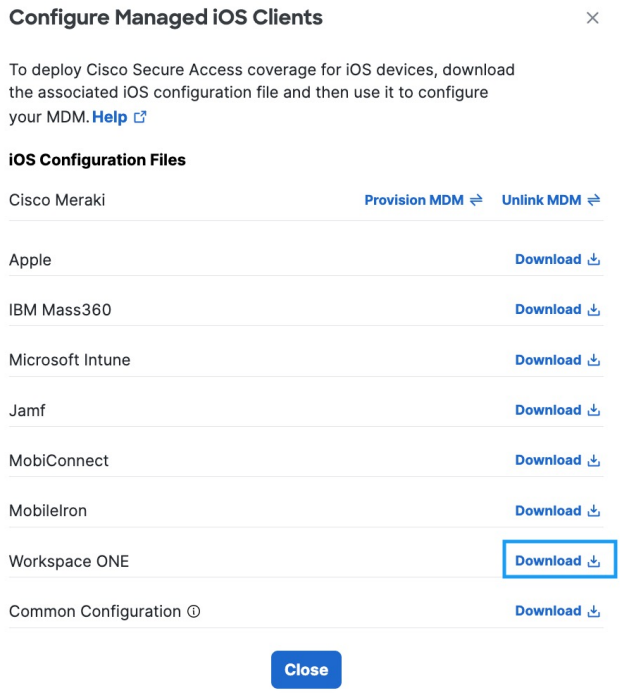
> **Note**
>
> You must log into your Secure Access dashboard as an administrator.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

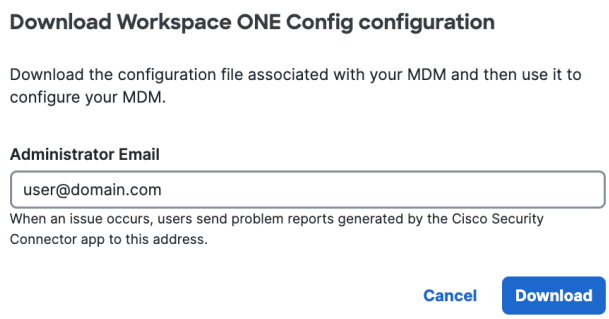


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.

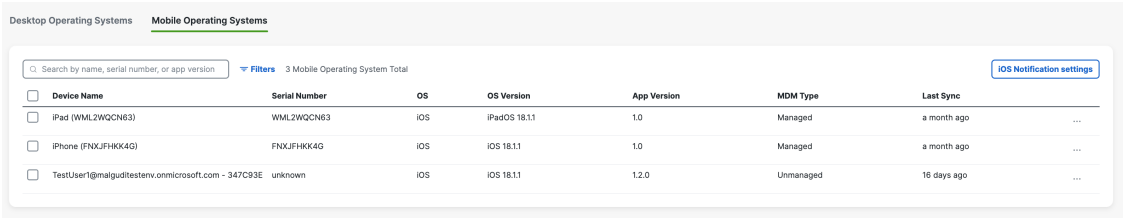


5. In your new profile, applied for the CSC group, choose **Custom Settings**, and then **Configure**. Paste the XML from the Dashboard download (above) here. It should start and end with <dict> and </dict>.

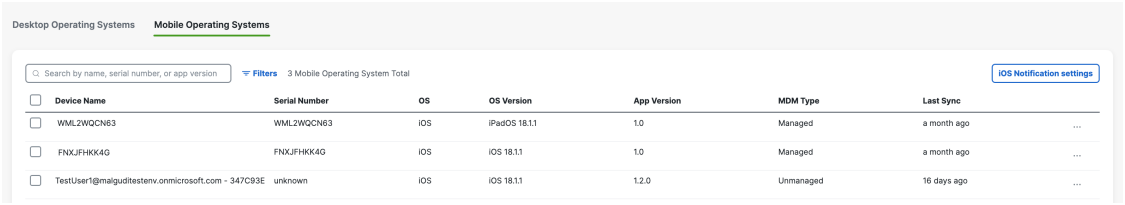
   If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.

What to do next

We recommend also deploying the Cisco Secure Access root certificate under the Certificates payload of your Workspace One profile. This certificate will allow HTTPS blocked and proxied pages to be certificate error-free.



If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



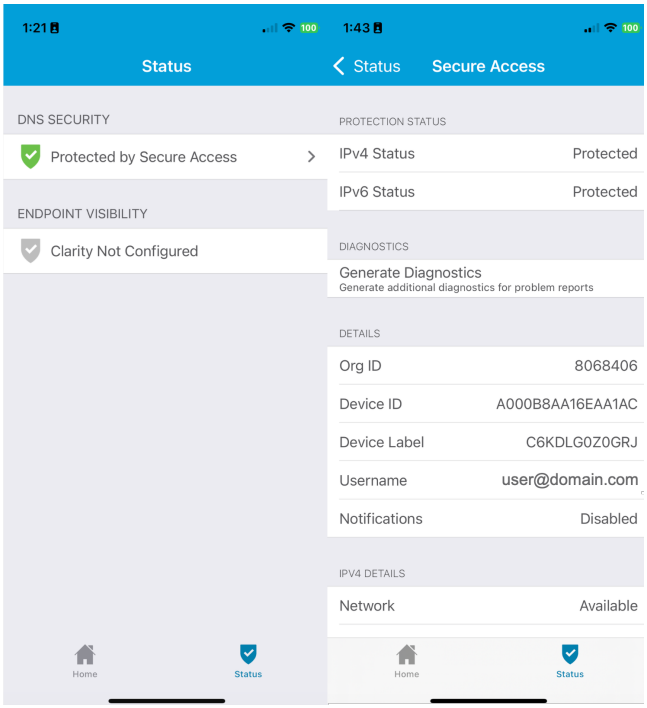
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify Secure Access on Your iOS Device

Provides instructions for completing the Verify Secure Access on Your iOS Device workflow in Cisco Secure Access. In the CSC app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

1. In the CSC app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Register an iOS Device Through a Generic MDM System

Describes Register an iOS Device Through a Generic MDM System in Cisco Secure Access and explains Anonymization and Prerequisites. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Note**
>
> "Generic" refers to any Mobile Device Management (MDM) system that is NOT Meraki, MobileIron, Airwatch, or Apple.

By downloading an XML file from Secure Access and updating it to support your iOS device's serial number, then adding this XML file to your "generic" MDM system, your MDM system is able to push configuration information to both Cisco Security Connector (CSC) and Secure Access so that your iOS device is registered with Secure Access. The result is that your iOS device is protected by Secure Access.

For information about configuring your specific MDM system, see your MDM system's documentation.

Anonymization

Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

Prerequisites

- The Cisco Security Connector requirements.

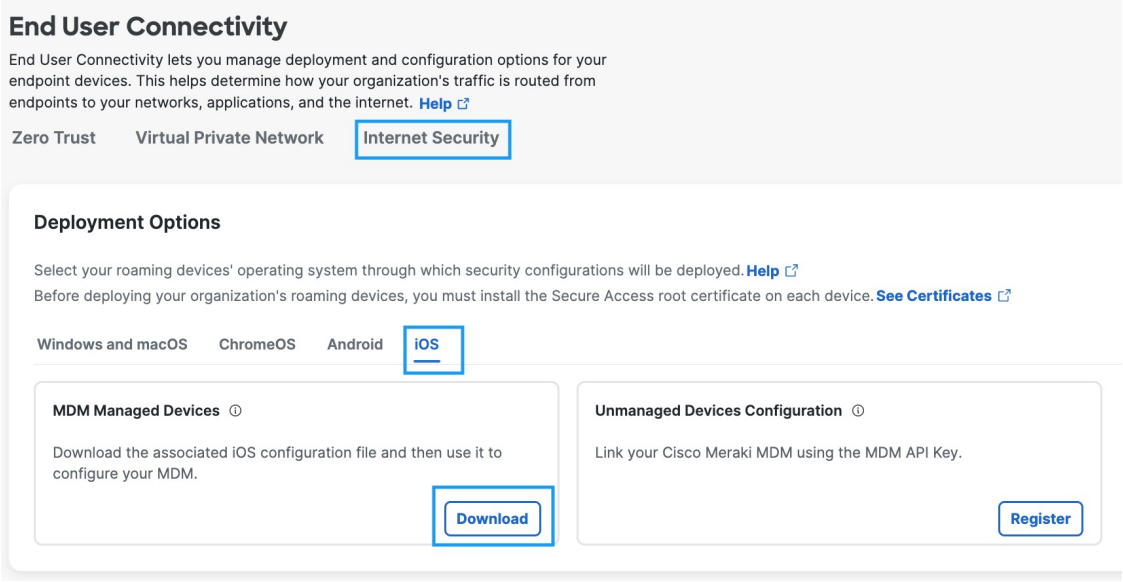
- Configure your MDM system as required so that it is able to push configuration information to both CSC and Secure Access. For information about configuring your specific MDM system, see your MDM documentation. For support, contact your MDM's support. For support, contact your MDM's support on deploying the Apple DNS Proxy Provider profile.
- Full admin access to the Secure Access dashboard. See Manage Accounts.

Register the iOS Device Through a Generic MDM System

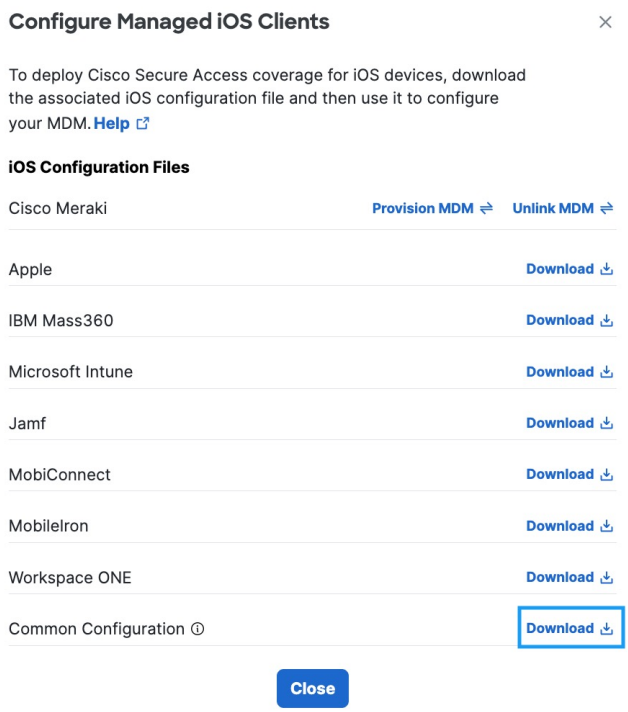
Provides instructions for completing the Register the iOS Device Through a Generic MDM System workflow in Cisco Secure Access. In Secure Access, navigate to Connect End User Connectivity and click Internet Security.

Procedure

1. In Secure Access, navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **iOS** tab.

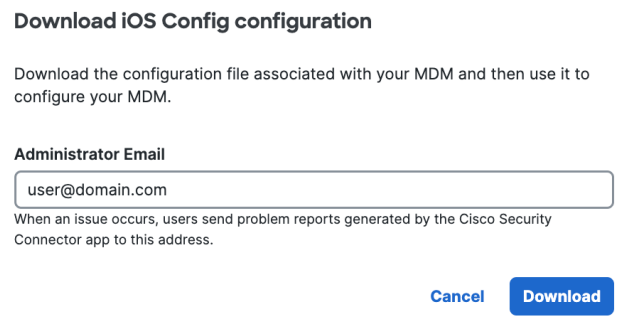


2. Under the **MDM Managed Devices** section, click **Download**.
3. In the **Configure Managed iOS Clients** window, click **Download**.



4. Add the administrator's email address to which the problem report will be sent when an issue occurs and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **!** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.



5. In the downloaded XML file, update the line {SERIAL_NUMBER} with the iOS device's serial number. This can be achieved in one of two ways:

   - **Automatically**–If your MDM system has its own variable and syntax for the variable {*SERIAL_NUMBER*}, replace this variable with your MDM's variable.
   - **Manually**–Open the downloaded XML file and update the line **{SERIAL_NUMBER}** with the device's serial number. For example, 1234567890.

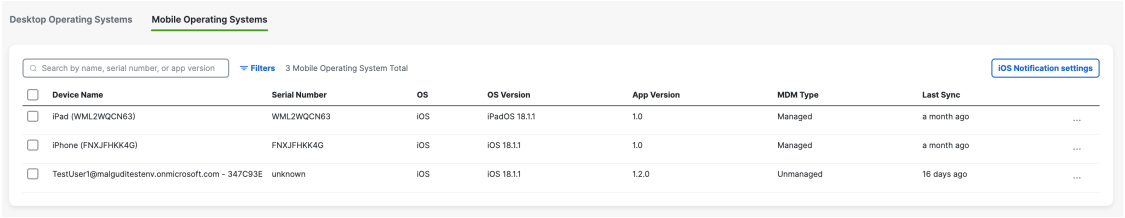
     Repeat this process for each iOS device–you must download and manually update an XML file for each device you want to register.

6. Add this updated XML file to your MDM.

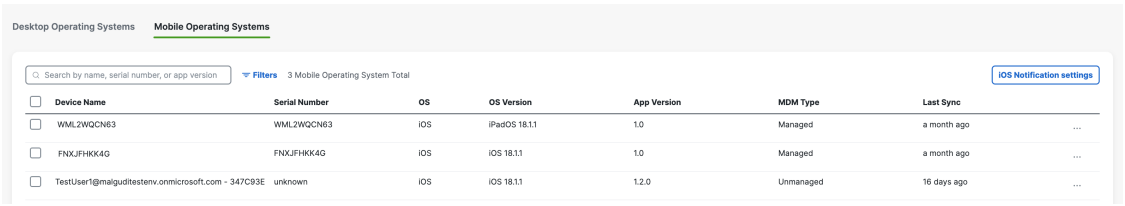
   For information about configuring your specific MDM system, see your MDM system's documentation.

What to do next

If successful, your mobile device registers with Secure Access and is listed at **Resources** > **Roaming Devices** > **Mobile Operating Systems**. CSC on your mobile device updates to connect to Secure Access so that your iOS device is protected by Secure Access.



If you have anonymized your device (see Anonymize Devices), Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



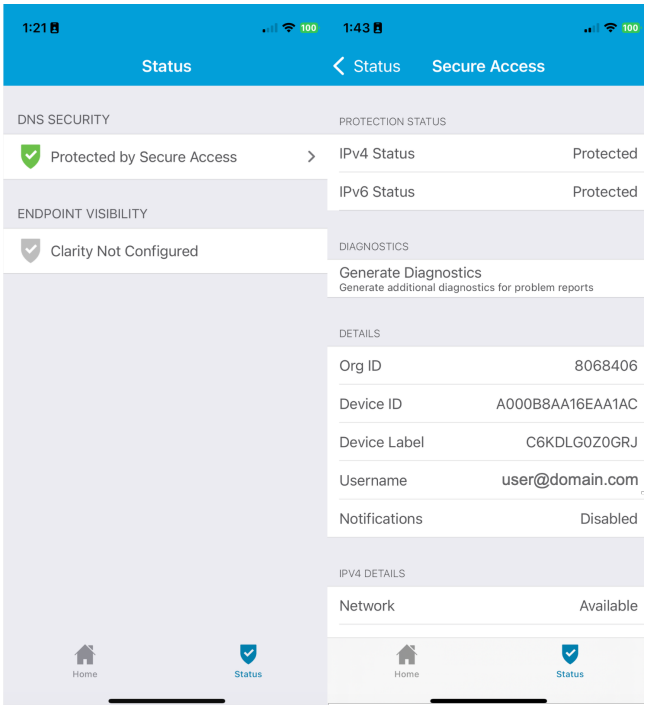
As no changes can be made in Secure Access to the actual provisioned device, these mobile devices are simply listed in Secure Access as identities; however, you can now use Secure Access to apply policies to these mobile device identities. For more information, see Apply a DNS Policy to Your Mobile Device.

Verify That Your Device is Protected by Secure Access

Provides instructions for completing the Verify That Your Device is Protected by Secure Access workflow in Cisco Secure Access. On your mobile device, in the Cisco Security Connector app, tap the Status icon and confirm that it shows Protected by Secure Access.

Procedure

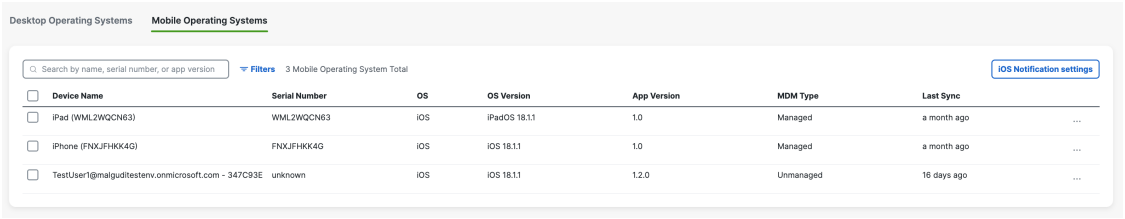
1. On your mobile device, in the Cisco Security Connector app, tap the **Status** icon and confirm that it shows **Protected by Secure Access**.
2. For protection details, tap **Protected by Secure Access**.



Apply an Access Policy to Your Mobile Device

Provides instructions for completing the Apply an Access Policy to Your Mobile Device workflow in Cisco Secure Access. Full admin access to the Secure Access dashboard.

Once your device is successfully configured and imported from the MDM dashboard, it is automatically synchronized with Secure Access. This ensures that the device's information, such as its identity and provisioning details, is made available in Secure Access. The imported device will then appear under **Resources** > **Roaming Devices** > **Mobile Operating Systems** in the Secure Access dashboard.



Since any changes to the actual provisioned device must be made through the MDM, these mobile devices are only listed in Secure Access. However, you can still apply access policies to these mobile device identities directly within Secure Access. To do this, navigate to **Secure** > **Policy** > **Access Policy** and configure the desired rules for mobile devices.

Access policies allow you to define the level of protection and logging, such as blocking specific types of sites or enabling additional security features like the Secure Access intelligent proxy.

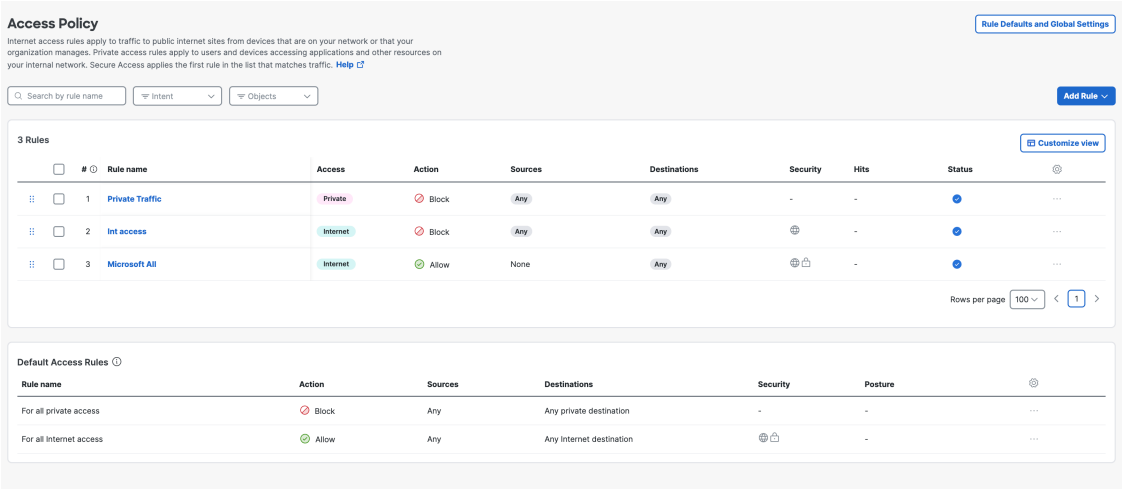
> **Note**
>
> Only one Access Policy can be applied to a device identity at any time.

Before you begin

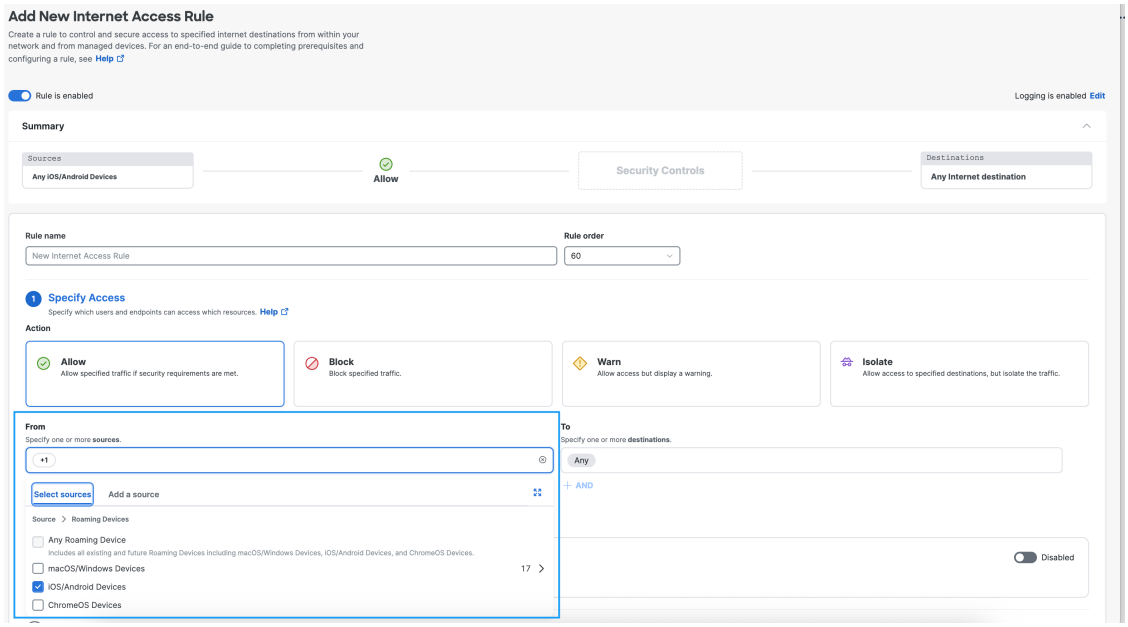
- Full admin access to the Secure Access dashboard. See Manage Accounts.

Procedure

1. Navigate to **Secure** > **Policy** > **Access Policy**.



2. Perform one of the following actions:
   a) To configure an existing policy, click the ellipsis at the far right side of a rule. Choose one of the following options based on your requirement: ui**Duplicate**, **View**, **Edit**, **Disable**, or **Copy Link**.
   b) To create a new Access Policy, click **Add Rule**. For more information, see Add an Internet Access Rule.
   c) While creating a new Access Policy, ensure that you select **Roaming Devices** > **iOS/Android Devices** as the source.



What to do next

When your device is imported into Secure Access, Secure Access automatically applies the default access rules to it. You can change which Access Policies are applied to your identity at any time. For more information about Access Policies, see Manage the Access Policies.

Add User Identity for Cisco Security Connector

Provides instructions for completing the Add User Identity for Cisco Security Connector workflow in Cisco Secure Access. You must provision the user identity and the iOS mobile device in Secure Access, and deploy an MDM system on the mobile device.

Add the user identity information in your MDM or EMM for the Cisco Security Connector. The Security Connector creates a hash from the value of the `userPrincipalName` key and adds the hash to DNS requests sent from the mobile device.

The Cisco Security Connector monitors DNS traffic from an iOS device and prevents connections to malicious sites. To increase the visibility of traffic from an iOS device, you can add user identity information to an iOS device for the Security Connector. In a Mobile Device Management (MDM) or Enterprise Mobile Management (EMM) configuration file, add an email address for a user identity. The Cisco Security Connector does not have direct access to user information on an iOS device, but can read the user identity information from an MDM or EMM.

Once you deploy the **mobileconfig** file on the iOS device, DNS queries sent from the device include a hash of the email address. When Secure Access receives a DNS request that includes the user identity information, Secure Access applies the internet access rules in the Access policy for the iOS device and the user identity. You can view the email address for the user identity and the iOS device in the Activity Search report.

Before you begin

You must provision the user identity and the iOS mobile device in Secure Access, and deploy an MDM system on the mobile device.

- Full Admin user role. For more information, see Manage Accounts.
- Cisco Security Connector for iOS–version 1.6.3 or later.

- Mobile Device Management (MDM) or Enterprise Mobile Management (EMM) system deployed on the managed or supervised iOS device.
- Provision user identities to Secure Access from an identity provider (IdP). For more information about identity integrations, see Manage Users, Groups, and Endpoint Devices .
- Deploy the Cisco Security Connector and set up a mobile configuration for the iOS device. For more information, see Quick Start.

Procedure

1. In the MDM or EMM, open the **mobileconfig** file for a device or an organization.
2. Add a `userPrincipalName` key and set the key to an email address for the user identity that you provisioned with Secure Access. You can set an email address for a single device or configure an MDM variable that applies to an organization.

   `EmailAddress` is an example of an MDM variable. For information about variables that are supported by your MDM, check your MDM's documentation.

   Note

   You must add the `userPrincipalName` key and value within the same `<dict> </dict>` scope that includes the `organizationId` key.

```
<plist version="1.0">
  <dict>
    <key></key>
    <array>
      ...
      <dict>
        ...
        <dict>
          ...
          <array>
            ...
          </array>
          ...
          <key>organizationId</key>
          <string>1234567</string>

          <key>userPrincipalName</key>
          <string>{{EmailAddress}}</string>
          ...
        </dict>
      </dict>
    </array>
    ...
  </dict>
</plist>
```

3. Save the **mobileconfig** file, and then deploy the file to the iOS devices with MDM or EMM.

Test Integration of User Identity With Cisco Security Connector

Describes Test Integration of User Identity With Cisco Security Connector in Cisco Secure Access. Check the deployment of the user identity information on your iOS device for the Security Connector.

Check the deployment of the user identity information on your iOS device for the Security Connector.

- **View your internet access rules in the Access policy and Activity Search report**–View the email address of the user identity and the name of the iOS device in your internet access rules and the Activity Search report.
- **Run a diagnostic tool**–Run a third-party network diagnostic app for iOS to generate a DNS query similar to:

```
Domain: erc.debug.opendns.com
Query Type: TXT
DNS Server: 208.67.222.222
```

A DNS response from Secure Access includes a line that begins with **alt uid** and contains the hashed value of the `userPrincipalName` key from the **mobileconfig**.

Anonymize Devices

Provides instructions for completing the Anonymize Devices workflow in Cisco Secure Access. Full admin access to the Secure Access dashboard.

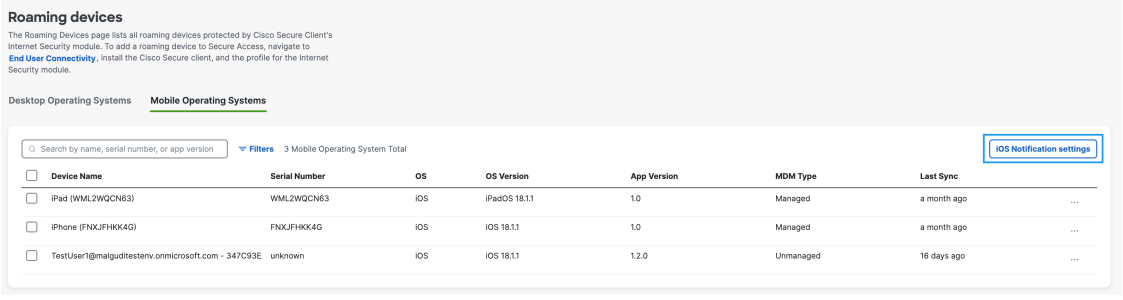
Secure Access provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Secure Access dashboard and in the Cisco Secure Connector (CSC) app UI. Before completing tasks to register your iOS devices, configure settings so that when you download configuration files these files will include settings to anonymize devices.

Before you begin

- Full admin access to the Secure Access dashboard. See Manage Accounts.

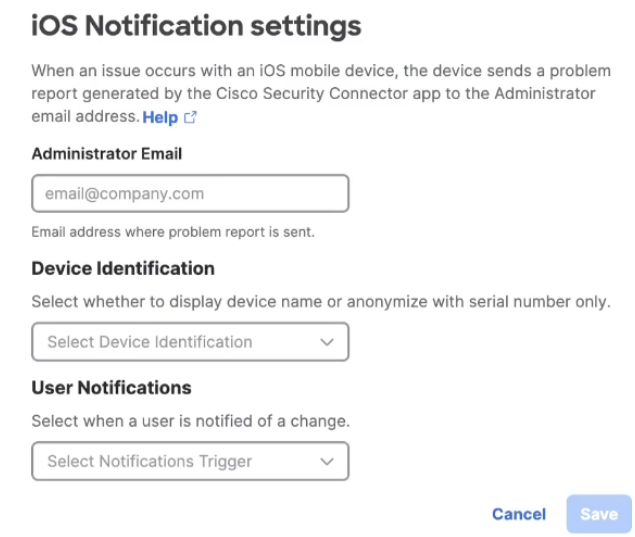
Procedure

1. Navigate to **Resources** > **Roaming Devices** > **Mobile Operating System** and click **iOS Notification settings**.

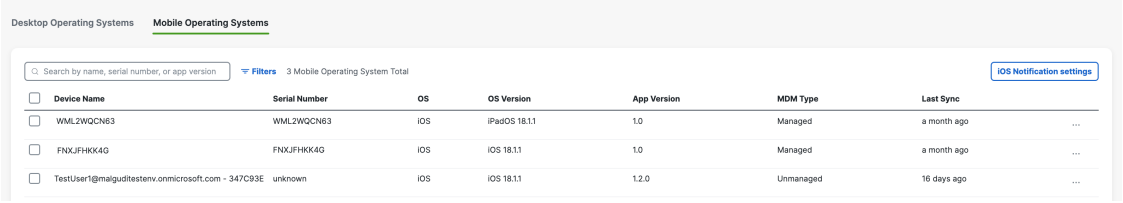


2. In the **iOS Notification settings** window, from the **Device Identification** drop-down list, choose **By Serial Number Only** and click **Save**.

   Your devices will now be anonymized when registered.



If you have anonymized your device, Secure Access hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



Export Device Data to CSV

Describes Export Device Data to CSV in Cisco Secure Access. The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria.

The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria. Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

The exported CSV file contains the following information for each device:

- originId
- label
- serialNumber
- appliedBundle
- dnsProtectionStatus
- swgProtectionStatus
- lastDnsProtectionStatus
- lastSync
- version

- osVersion
- osVersionName
- type

Here the **dnsProtectionStatus** field displays the DNS protection status of respective devices. For information about the various DNS protection statuses, refer to the View DNS Protection Status topic.

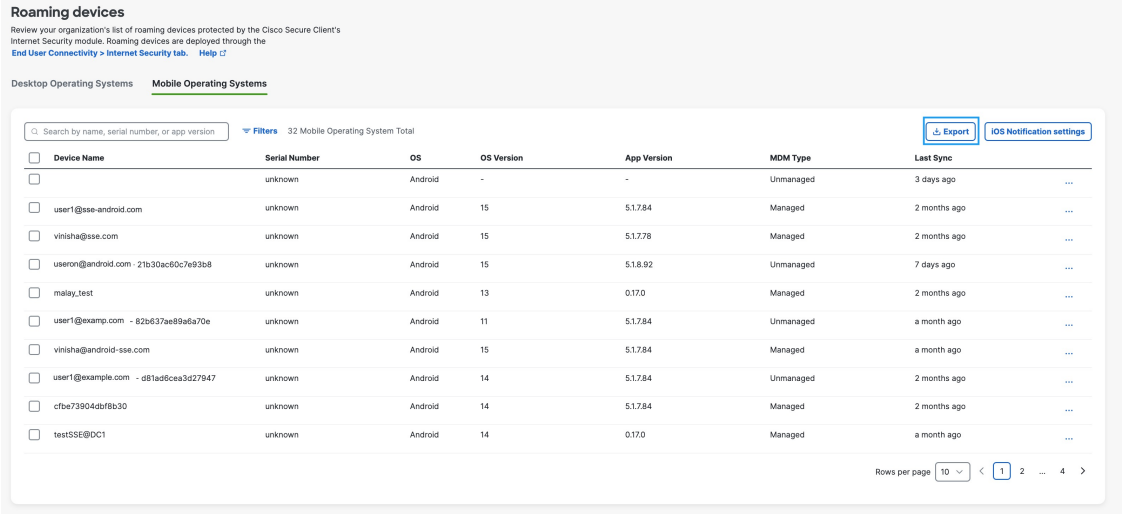
For information about the various SWG protection statuses, refer to the View SWG Protection Status topic.

Procedure

Provides instructions for exporting device data to a CSV It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Sources and destinations** > **Roaming Devices**.
2. For roaming devices running mobile operating systems, click **Mobile Operating Systems** or click **Desktop Operating Systems** for roaming devices running desktop operating systems.



3. Choose one of the following export options as per your requirement:
   - Export All Devices
     - Click **Export** at the top of the table to export all devices.
   - Export Selected Devices
     - Check the required number of devices and click **Export Selected** to export a specific number of devices.
   - Export Devices Based on Search Criteria
     - Search by name, serial number, or app version in the search bar. To further refine your search, click **Filter** and specify a search criteria to filter the devices accordingly.
     - Click **Export** to export all the devices meeting the search criteria. Check the required number of devices, and click **Export Selected** to export a specific number of devices that meet the search criteria.

What to do next

Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

DNS Protection Status in Exported Reports

Describes DNS Protection Status in Exported Reports in Cisco Secure Access. The dnsProtectionStatus column in Resources Roaming Devices exports uses these values.

The **dnsProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No DNS protection status is set or reported.	Not applicable
Open	The device is unprotected because Secure Access DNS resolvers are unreachable.	Unprotected (FailOpen)
Transparent	DNS protection is active and reporting, but DNS queries are not encrypted.	Protected
Encrypted	DNS protection is active and DNS queries are encrypted.	Encrypted
VA	DNS protection is provided through a Virtual Appliance.	BehindVA
Network	DNS protection is provided at the network level.	BehindNetwork
Disabled	DNS protection is disabled by configuration or policy.	Disabled
Uninstalled	The Cisco Secure Client Secure Access module is uninstalled.	Not applicable
TrustedCustomerNetwork	DNS protection is disabled on a customer-defined trusted network.	Trusted customer network
CiscoTrustedNetwork	DNS protection is disabled on a Cisco trusted network.	Cisco trusted network
DisabledDueToACVpnFullTunnel	DNS protection is disabled while a full-tunnel VPN connection is active.	DisabledDueToACVpn
Off	The device has not synchronized within the timeout period. Its last status is stale.	Not applicable

Note

`Off` is not applied when the raw status is `Uninstalled` or `-`.

To know more about the DNS protection status of the Cisco Secure Client, see View DNS Protection Status

SWG Protection Status in Exported Reports

Describes SWG Protection Status in Exported Reports in Cisco Secure Access. The swgProtectionStatus column in Resources Roaming Devices exports uses these values.

The **swgProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No SWG protection status is set or reported.	Not applicable
Protected	SWG protection is active.	Protected
Unprotected	SWG protection is inactive.	Unprotected
Disabled	SWG protection is disabled by configuration or policy.	Disabled
DisabledDueToVPN	SWG protection is disabled while a VPN full-tunnel connection is active.	Disabled (VPN connection)
DisabledDueToTrustedNetwork	SWG protection is disabled while the device is on a trusted network.	Disabled (trusted network)
ConfigError	SWG protection cannot be applied because of a configuration error.	Configuration Error
CloudServiceUnavailable	The SWG cloud service is unreachable from the device.	Cloud Service Unavailable
Offline	The device has not synchronized within the timeout period. Its last SWG status is stale.	Not applicable

To know more about the SWG protection status of the Cisco Secure Client, see View SWG Protection Status

Push the Cisco Root Certificate to Managed Devices

Provides instructions for completing the Push the Cisco Root Certificate to Managed Devices workflow in Cisco Secure Access. Full admin access to the Secure Access dashboard.

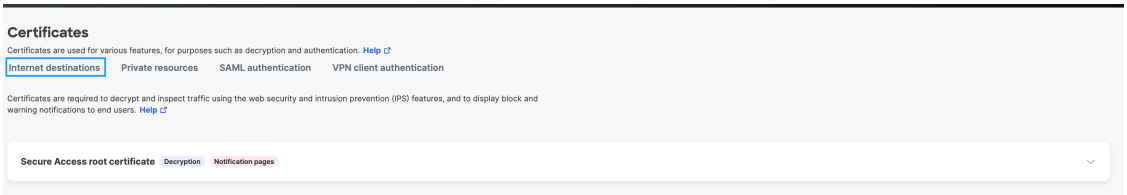
To support the display of block pages for HTTPS sites, HTTPS decryption if the Intelligent Proxy is used, and Trusted Network Detection if a VA is present, you must push the Secure Access certificate to each of your managed devices.

Before you begin

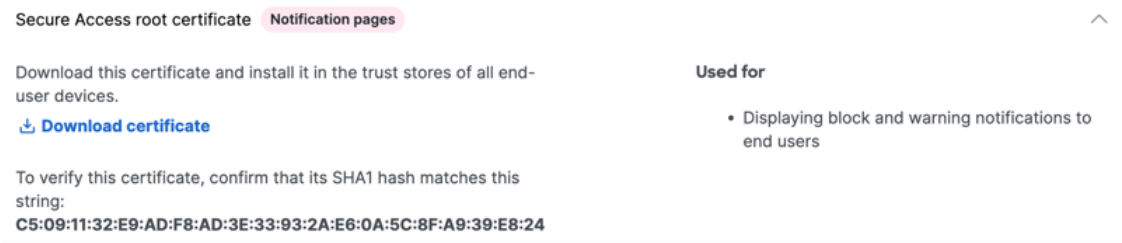
- Full admin access to the Secure Access dashboard. See Manage Accounts.

Procedure

1. Navigate to **Secure** > **Certificates** > **Internet destinations**, and then expand **Secure Access root certificate**.



2. Click **Download certificate** to download the `Cisco_Secure_Access_Root_CA.cer` file.



3. Push the root certificate to all your devices from the MDM admin panel so that block pages can be displayed.

   This allows block pages for HTTPS sites to appear correctly, enables HTTPS decryption if the Intelligent Proxy is used, and enables Trusted Network Detection if a VA is present.

> **Note**
>
> If there is an Secure Access VA in your network and you want to use Trusted Network Detection, configure the VA as detailed in Umbrella Virtual Appliance: Receiving user-IP mappings over a secure channel.

Configure Cellular and Wifi Domains

Provides instructions for completing the Configure Cellular and Wifi Domains workflow in Cisco Secure Access. Cisco Security Connector (CSC) for iOS version 1.6 or higher on iOS 14 or higher.

By default, iOS will appropriately prioritize DNS to the expected interface. However, in some cases you may need to inform iOS of the desired target interface.

For example:

- Always send a domain over WiFi, never cellular. This can ensure that local corporate domains are never sent over the cellular network.
- Always send a domain over cellular, never WiFi. This can aid in compatibility issues, such as voicemail domains only functioning over cellular DNS.

Before you begin

- Cisco Security Connector (CSC) for iOS version 1.6 or higher on iOS 14 or higher.

Procedure

1. Open the iOS configuration profile in your preferred code editor. Your profile may already have wifiDomains and celluarDomains keys as shown. If not, add them.

For example:

```
<key>anonymizationLevel</key>
<integer>1</integer>
<key>disabled</key>
<false/>
  <key>cellularDomains</key>
  <array>
    <string>sendtocellularconnection.com</string>
  </array>
  <key>wifiDomains</key>
  <array>
    <string>sendoverwifi.com</string>
</array>
  <key>internalDomains</key>
```

2. Configure the wifiDomains or cellularDomains keys as desired using the example provided. Each domain is encapsulated by a string tags. Some configuration profiles may require the addition of these keys. Keys should be added immediately preceding the *internalDomains* key.

   For example:

```
<dict>
 <key>anonymizationLevel</key>
 <integer>1</integer>
 <key>disabled</key>
 <false/>
 <key>cellularDomains</key>
 <array>
   <string>sendtocellularconnection.com</string>
 </array>
 <key>wifiDomains</key>
 <array>
   <string>sendoverwifi.com</string>
  </array>
<key>internalDomains</key>
```

Configuring DNS Suffix Allow List

Provides instructions for completing the Configuring DNS Suffix Allow List workflow in Cisco Secure Access. For devices running iOS 16 or later, you must install the Cisco Security Connector for iOS version 1.7 or higher.

When the **noAutoSuffix** setting in the configuration file is set to NO, all entries in the DNS Search Domains are added to the allow list. This makes it difficult for the system to differentiate between user-added and iOS-added suffixes. To address this issue, the **IgnoreDomains** key in the configuration file can be used to selectively approve the necessary suffixes, even when **noAutoSuffix** is set to NO.

For example: The local Wi-Fi network router adds the sample_suffix.com at the router level, which is necessary for the proper operation of all devices using your Wi-Fi network. However, if someone places a domain that is otherwise "blocked" in this DNS suffix list, it allows the domain to be bypassed, resulting in undesired behavior.

Before you begin

- For devices running iOS 16 or later, you must install the Cisco Security Connector for iOS version 1.7 or higher.

Procedure

1. Open the iOS configuration profile in your preferred code editor.

```
<key>ignoreDomains</key>
<array>
<string>sample_suffix.com</string>
<string>contoso.network.local</string>
</array>
```

2. Add domain names as multiple string entries in the array.

> **Note**
>
> After you save the changes, the iOS configuration profile deploys automatically to the iOS device.

Troubleshooting

Describes Troubleshooting in Cisco Secure Access. The Cisco Security Connector (CSC) app deployed on an iOS device can generate various Secure Access reports.

The Cisco Security Connector (CSC) app deployed on an iOS device can generate various Secure Access reports. The Secure Access reports provide diagnostic information about the device's DNS traffic, which is protected by Secure Access.

If you configured your Secure Access administrator's email address in the Cisco Security Connector, send the Secure Access diagnostic reports to the administrator. For more information, see Generate Diagnostics and Email the Secure Access Report.

If your Secure Access administrator's email address is not configured in the Cisco Security Connector, share the Secure Access reports with a Secure Access administrator through a supported cloud application. For more information, see Generate Diagnostics and Share the Secure Access Report.

Prerequisites

- Confirm that you meet all requirements for the deployment of the Cisco Security Connector on iOS devices. For more information, see Cisco Security Connector Secure Access Setup Guide.

Generate Diagnostics and Email the Secure Access Reports

Provides instructions for completing the Generate Diagnostics and Email the Secure Access Reports workflow in Cisco Secure Access. Before you begin, add an Secure Access administrator's email address to the Cisco Security Connector.

Before you begin, add an Secure Access administrator's email address to the Cisco Security Connector. For more information, see Add an administrator email address.

Procedure

1. On your iOS device, in the Cisco Security Connector app, navigate to **Umbrella details** > **Diagnostics** > **Generate Diagnostics**.
2. Tap **Start**. The diagnostic report starts generating.

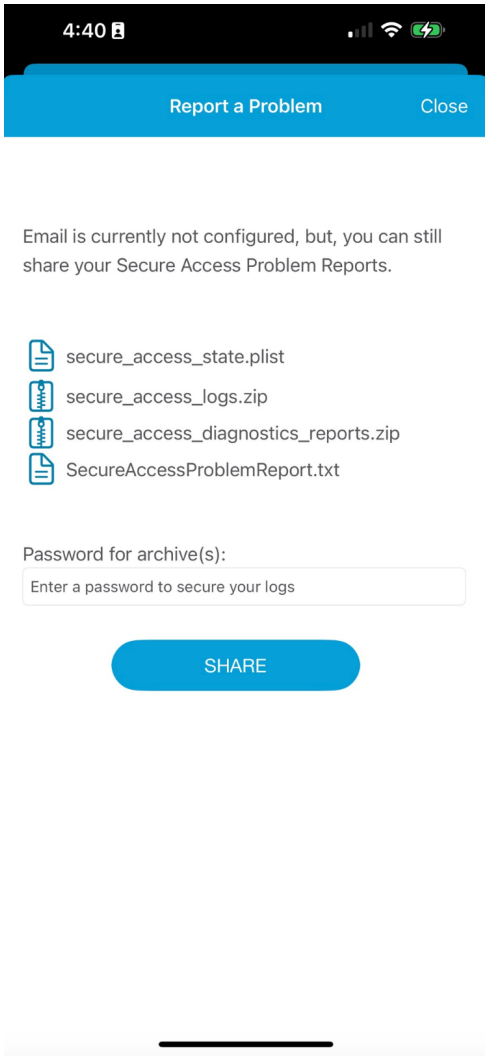
3. When the diagnostic report is complete, navigate to **About** > **Report a Problem...**.
4. Enter a problem description, then tap **Next**. A preview of the problem report email appears, which you can edit, or add more recipients to the message. The Secure Access diagnostic report files are attached.
5. Tap **Send**.

Generate Diagnostics and Share the Secure Access Reports

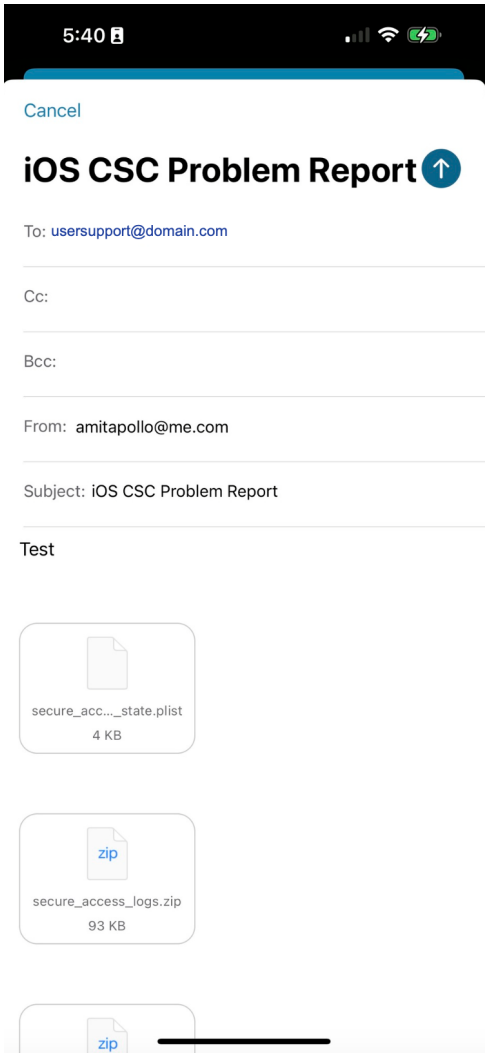
Provides instructions for completing the Generate Diagnostics and Share the Secure Access Reports workflow in Cisco Secure Access. On your iOS device, in the Cisco Security Connector app, navigate to Umbrella details Diagnostics Generate Diagnostics .

Procedure

1. On your iOS device, in the Cisco Security Connector app, navigate to **Umbrella details** > **Diagnostics** > **Generate Diagnostics**.
2. Tap **Start**. The diagnostic report starts generating.
3. When the diagnostic report is complete, navigate to **About** > **Report a Problem...**.
4. Enter a problem description, then tap **Next**.
5. When prompted, enter a password, and then click **Share**.



> **Note**
>
> If email is configured, the diagnostics report can be shared through email.



6. Share the Secure Access diagnostic report files through iCloud, Airdrop, Webex, iMessage, or other apps.

> **Note**
>
> You may not share the Secure Access diagnostic report with the following apps natively: Facebook, Twitter, Weibo, Flickr, and Tencent Weibo.

65 Managed Android

Topics:

- Secure Access Module for Cisco Secure Client (Android OS)
- Deploy the Android Client
- Manage Identities
- Export Device Data to CSV
- Troubleshooting
- Frequently Asked Questions about Managed Android

Provides an overview of Managed Android in Cisco Secure Access, including Secure Access Module for Cisco Secure Client (Android OS), Deploy the Android Client, and Manage Identities. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Secure Access Module for Cisco Secure Client (Android OS)

Describes Secure Access Module for Cisco Secure Client (Android OS). It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

> **Note**
>
> **DNS Policies Only**
>
> Android Mobile Security is only supported in Secure Access for Access policies.

Mobile device threats are prevalent on any network. The Cisco Secure Access Module in Cisco Secure Client for Android OS is a roaming client for managed Android devices that offers protection from these threats at the DNS layer. This protection extends to both apps and browser-based traffic to the entire protected scope of the Android device.

A mobile device management system (MDM) is required to deploy this client to mobile devices and to push the Secure Access configuration to the mobile devices.

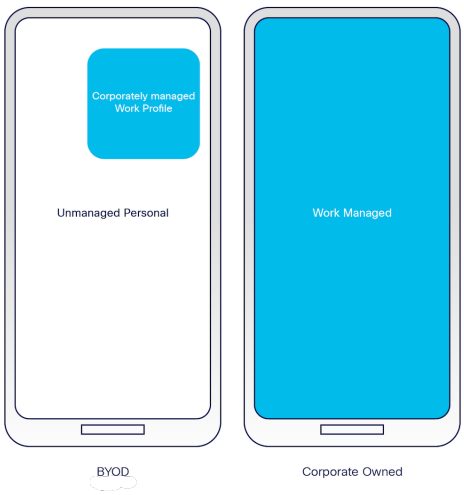
Device Security

Describes Device Security in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

There are two deployment modes for the Secure Access module for Cisco Secure Client:

- Personal "bring your own device" (BYOD)
- Organization-owned device

Secure Access coverage applies exclusively to the work profile of the Android device. For fully managed (organizational owned) devices, the entire device is covered. For employee-owned devices with a work profile, only the work profile is covered by Secure Access for Android. Please refer to the diagram below, where blue indicates Secure Access coverage:



Prerequisites

Describes Prerequisites in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

- An Android Enterprise compatible device deployment. The legacy Device Admin (DA) system is not supported at this time.
- Private DNS must be turned off for DNS interception to function properly.
- Android mobile devices running Android OS version 6.0.1 and above. Devices examples are Samsung, Google, and Motorola. FireOS devices and other Android forks are not supported.
- An MDM for deploying the software. The following MDMs have been tested, and you should be able to use any MDM:
  - MobileIron
  - Meraki
  - VMWare WorkspaceOne (Airwatch)
  - Microsoft InTune
  - Samsung Knox
  - Google Admin Console (Google Workspace)
- Access to a Secure Access subscription, including mobile device coverage
- A network meeting access requirements
  - For IPv4 or Dual Stack networks, ensure that UDP ports 53, 5353, and 443 are accessible to the IP address 208.67.222.64.
  - For IPv6 or Dual Stack networks, ensure that UDP ports 53, 5353, and 443 are accessible to the IP address 2620:119:53::64.

  > **Note**
  >
  > For IPv6-only networks, the NAT64 and DNS64 or 464XLAT gateways are required.

  > **Note**
  >
  > ***DNS64** (RFC 6147) is meant for single-stack IPv6 networks. This is to help with IPv4 to IPv6 transitions. If you are using Umbrella DNS on devices without IPv4 access, these resolvers will synthesize records that can reach those destinations through a NAT64 gateway using the Well-Known Prefix. More details available in DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers.

- For on-network scenarios, Trusted Network Detection (TND) may also be used to disable the client on network and pass traffic to a Virtual Appliance. The following prerequisites apply:
  - All VAs in use are defined by FQDN (IPs entered will not allow the client to go into trusted network mode) in the umbrella_va_fqdns configuration property.
    - The format for this field is comma separated, for example, (va1.domain.com, va2.domain.com)
  - VAs must be registered to the same Secure Access organization as the Android devices
  - HTTPS mode for user events enabled on the Virtual Appliance

- If the VA's FQDN is not publicly signed, the self-signed root certificate for the VA domain used for HTTPS mode on the VA must also be pushed to the Android device to sign the connection.
- VA certificates should contain Subject Alternate Name (SAN) matching the VA's configured domain to successfully communicate with the VA over HTTPS mode
- For more information on how to configure HTTPS mode on the VA, see Umbrella Virtual Appliance: Receiving User-IP mappings Over a Secure Channel.

Deploy the Android Client

Describes Deploy the Android Client in Cisco Secure Access and explains Download Configuration, MDM Configurations, and Secure Access Certificate. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The process of deploying the Android client consists of three tasks:

- Download the Android Configuration
- Configure the mobile device manager (MDM) you use
- Push the Secure Access certificate

> **Note**
>
> **DNS Policies Only**
>
> Android Mobile Security is only supported in Secure Access for DNS policies.

Download Configuration

Android Configuration Download

MDM Configurations

- Cisco Meraki MDM
- MobileIron MDM
- VMware Workspace ONE
- Microsoft Intune MDM
- Samsung Knox MDM

Secure Access Certificate

Push the Secure Access Certificate to Devices

Android Configuration Download

Describes Android Configuration Download in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access and adding this file to your MDM system, your MDM system is able to push configuration information to both Cisco Security Connector (CSC) and Secure Access so that your Android device is registered with Secure Access. The result is that your Android device is protected by Secure Access.

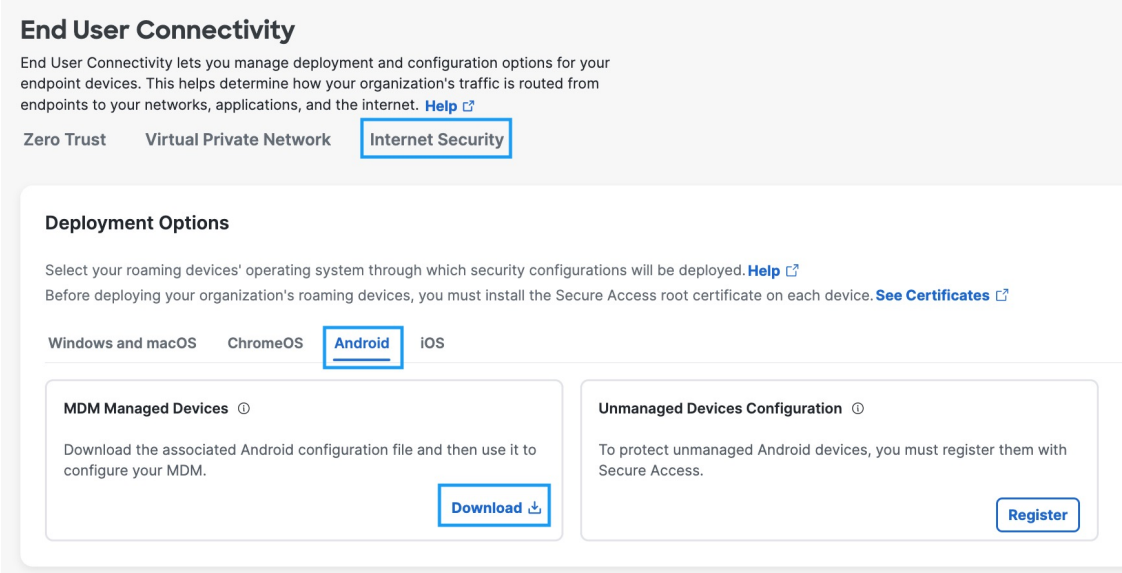
For information about configuring your specific MDM system, see your MDM system's documentation.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. Navigate to Connect End User Connectivity and click Internet Security.

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **Android** tab.



2. Under the **MDM Managed Devices** section, click **Download**.

   The downloaded configuration file contains details that are required to enable Secure Access security on your Android device. For example, it includes the organization ID and unique registration token associated with your Secure Access organization.

```
{"organizationInfo":{"Value":{"organizationId":<orgid>,"productId":<product
id>"regToken":"<reg token>"}}}
```

   If the deployment key is enabled, the configuration file includes the deployment key, deployment key name, and MDM ID in addition to other attributes. For more information on the deployment key, see Manage Device Deployment.

```
{"organizationInfo":{"Value":{"deploymentKey":"<deploymentkey>","deploymentKeyName":"<deployment
 key name>","mdmId":"<mdm id>, "organizationId":<ordgid>,"productId":<product
 id>,"regToken":"<reg token>"}}}
```

   Only one administrator is required to download the config file.

3. Save the file securely; you will use it in deploying your mobile device manager (MDM).

   Follow the link matching your MDM:

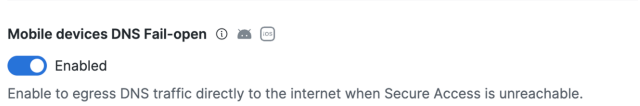
   - Cisco Meraki MDM
   - MobileIron MDM

- VMware Workspace ONE
- Microsoft Intune MDM
- Samsung Knox MDM

Fail Close/Open Scenario

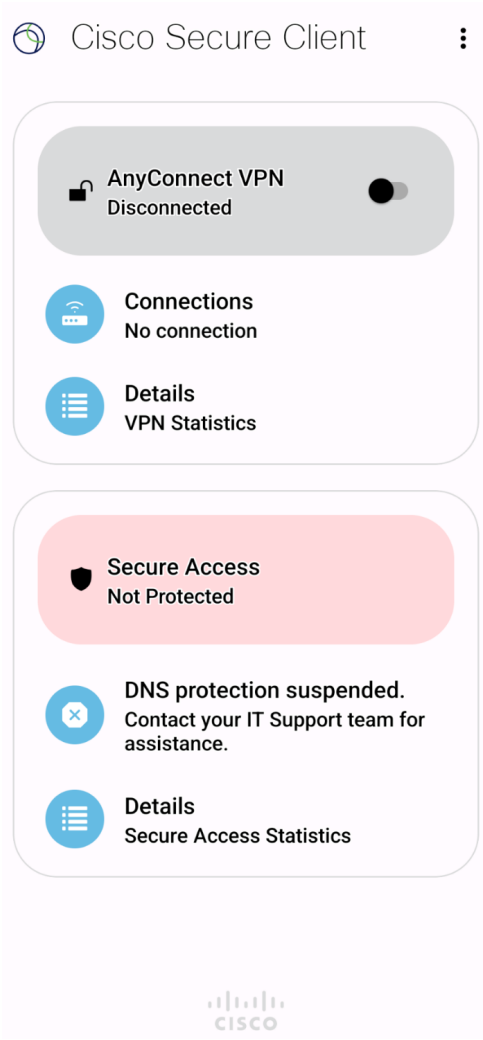
Describes Fail Close/Open Scenario in Cisco Secure Access. Navigate to Cisco Secure Client settings Advanced , and enable the Mobile devices DNS Fail-open field to egress DNS traffic directly to the internet when Secure Access is unreachable.

Navigate to **Cisco Secure Client settings** > **Advanced**, and enable the **Mobile devices DNS Fail-open** field to egress DNS traffic directly to the internet when Secure Access is unreachable.



> **Note**
>
> The Mobile Device Settings are the only settings applicable for Android devices under the Secure Access Security Settings.

In case of internal errors, such as the Secure Access Resolver is not reachable or the DNSCrypt Certificate is not available, the Secure Access UI displays the following:



Manage Device Deployment

Describes Manage Device Deployment in Cisco Secure Access. The Deployment Key feature provides an effective way to manage device registration within organizations while mitigating unauthorized access.

The **Deployment Key** feature provides an effective way to manage device registration within organizations while mitigating unauthorized access. This feature introduces the concept of a **deployment key** that can be activated, deactivated, and revoked. By utilizing deployment keys, administrators gain control over the credentials used by devices during registration for Secure Access protection. A deployment key is a field in the Android configuration file (mobileconfigAndroid.txt), which is used when registering devices to your organization's network. This feature ensures that only authorized devices are enrolled by requiring an active deployment key for registration.

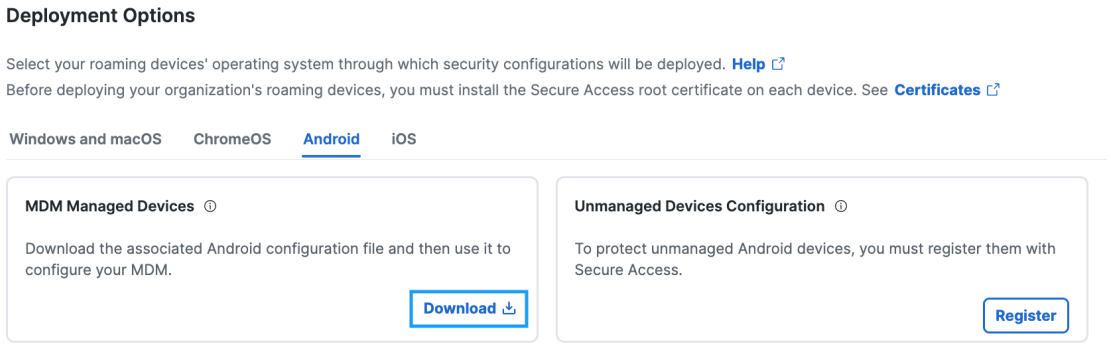
Note

Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, provided the deployment key in their mobileconfigAndroid.txt file is active.

This feature facilitates seamless device registration and ongoing validation while offering the flexibility to deactivate keys when necessary. If any unauthorized devices try to connect, administrators can swiftly deactivate the current deployment key and delete the suspected devices from the dashboard, ensuring a secure and efficient network environment. The

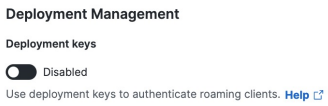
devices will not be able to reregister with the now-deactivated deployment key. Administrators can then activate a new deployment key. This allows IT teams to maintain operational continuity while safeguarding against unauthorized access.

If your Secure Access deployment requires a deployment key, or if your organization has already enabled them, the Android configuration file can only be downloaded when there is an active deployment key (see image below). Then, register your supervised Android device through your Mobile Device Manager (MDM) to Secure Access. For more information, see Android Configuration Download.



Prerequisites for Device Deployment Management

- For the Global deployment, the Deployment key feature is optional. Enable the Deployment Keys feature (**Connect > End User Connectivity > Internet Security**) if it is disabled.

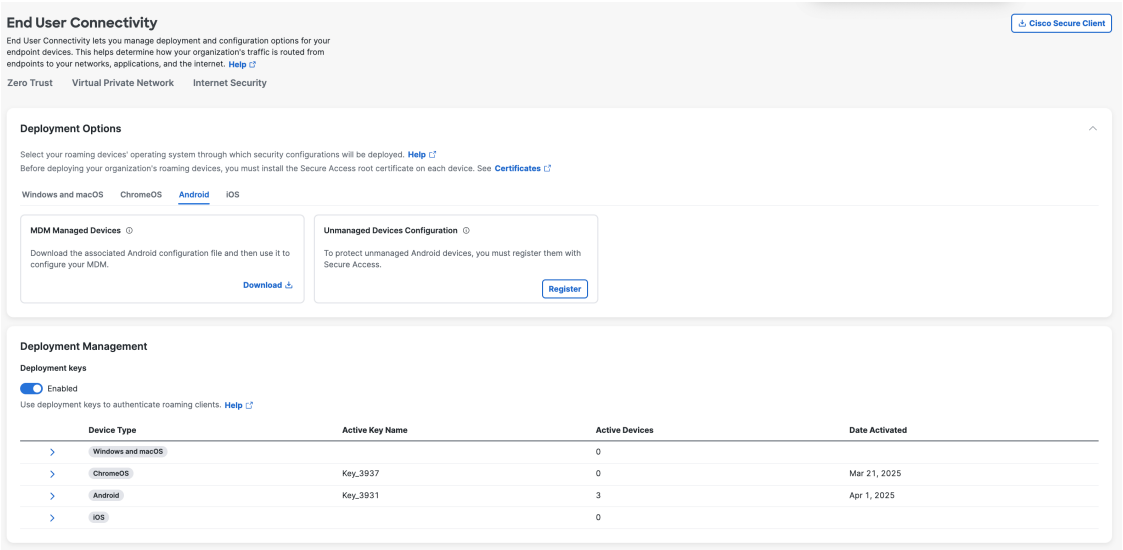


Add and Activate Deployment Key

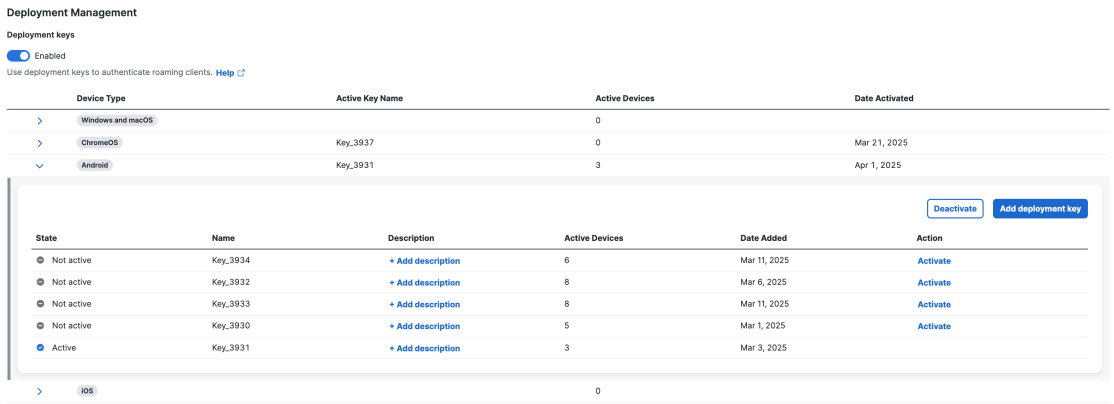
Provides instructions for completing the Add and Activate Deployment Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

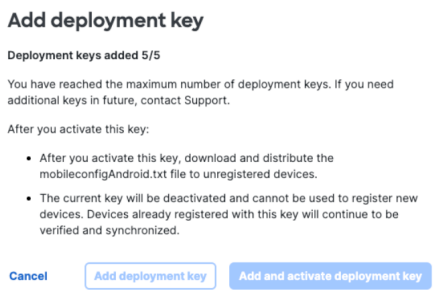
1. Navigate to **Connect** > **End User Connectivity**.
2. Click **Internet Security**.



3. In the **Deployment Management** section, expand the device type (Android).



4. Click **Add deployment key**.
5. In the **Add deployment key** window, click **Add & activate deployment key** to create and activate a deployment key for inclusion in your organization's Android configuration file.



What to do next

You can choose to add the deployment key immediately, but activate it later. In such a scenario, click **Add deployment key**. The deployment key is added to the table. When you are ready to activate the deployment key, click **Activate** in the **Action** column.

Important

- Only one deployment key can be active at a time for each device type.
- You can add up to five deployment keys per device type. To remove a key, contact Cisco support or your Account Manager.
- The deployment key name includes a random number to ensure its uniqueness.

Manage Deployment Key Compromise

Provides instructions for completing the Manage Deployment Key Compromise workflow in Cisco Secure Access. If you determine that a key has been compromised, take action to protect your network's integrity and security.

If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

This section outlines the necessary actions to be taken to ensure network security and continuity, including deactivating compromised keys, understanding the effects on existing clients, and steps for activating and distributing a new key for secure device registration.

Procedure

1. **Deactivate the Compromised Key**: Deactivate the compromised key. This action prevents any further device registrations using the deactivated key, ensuring that your network remains secure.

   To deactivate a deployment key, perform the following steps:

   a. Navigate to **Connect** > **End User Connectivity**.

   b. Click **Internet Security**.

   c. In the **Deployment Management** section, expand the device type.

   d. Click **Deactivate** in the **Action** column. Upon deactivating the compromised deployment key, it is important to consider its implications on both existing clients and the registration of new devices:

   - **Effect on existing clients**: It's important to note that deactivating a key will not disrupt the operation of clients already using it. These clients will continue to function normally, minimizing any potential impact on your current network operations.
   - **Limitations for new devices**: However, deactivated keys cannot be used for registering new devices. This means that any device attempting to register itself with the deactivated key will be unable to do so.

   > **Note**
   >
   > Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, provided the deployment key in their mobileconfigAndroid.txt file is active.

2. **Activate the new deployment key**: To facilitate the registration of new devices, you must activate a different deployment key. This new key will replace the compromised one and will be used for future device registrations.
3. **Download a new profile**: After the new key is activated, download a new profile, specifically the Android configuration file. This file contains the updated information, including the new active deployment key.

4. **Distribute the new profile to new devices**: Distribute the updated Android configuration profile to any new devices that need to connect to your network. This ensures that they have the correct and secure credentials to register and operate within your network environment.
5. **Update the Android configuration file for registered Devices**: Devices that are already registered and require an update to the Android configuration file will automatically receive changes once the configuration is updated in the mobile device manager (MDM).

Delete a Deployment Key

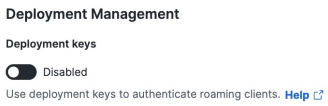
Describes Delete a Deployment Key in Cisco Secure Access. To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

Reverting to Using Legacy Deployment Implementation

Describes Reverting to Using Legacy Deployment Implementation in Cisco Secure Access. If needed, you can revert to the legacy registration mechanism by disabling the Deployment Keys feature (Connect End User Connectivity Internet Security).

If needed, you can revert to the legacy registration mechanism by disabling the **Deployment Keys** feature (**Connect** > **End User Connectivity** > **Internet Security**).



- After disabling the Deployment Keys feature, devices that are currently using the last activated deployment key will continue to be protected by Secure Access. However, new devices will not be able to register with the deactivated deployment key.
- To revert to the legacy registration mechanism, download the updated Android configuration file (mobileconfigAndroid.txt), which will no longer include the deployment key. New devices can now register using the legacy method.

Backward Compatibility

Describes Backward Compatibility in Cisco Secure Access. This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

For example, on Android:

- Cisco Secure Client for Android Release 5.1.9.114 or earlier will continue to use the legacy User ID and fingerprint for registration purposes, regardless of whether a deployment key is present.
- Cisco Secure Client for Android Release 5.1.9.115 or later will use the deployment key for registration, regardless of whether the User ID and fingerprint are present. If the deployment key is unavailable, the legacy User ID and fingerprint will be used for registration instead.

Cisco Meraki MDM

Describes Cisco Meraki MDM in Cisco Secure Access. For Meraki administrators, once you have deployed the Cisco Security Connector (CSC), use the Meraki dashboard to deploy the app to devices.

For Meraki administrators, once you have deployed the Cisco Security Connector (CSC), use the Meraki dashboard to deploy the app to devices. When your endpoints have registered with Secure Access, they will appear in the dashboard. For information about how to configure and enroll an Android device, see Meraki documentation.

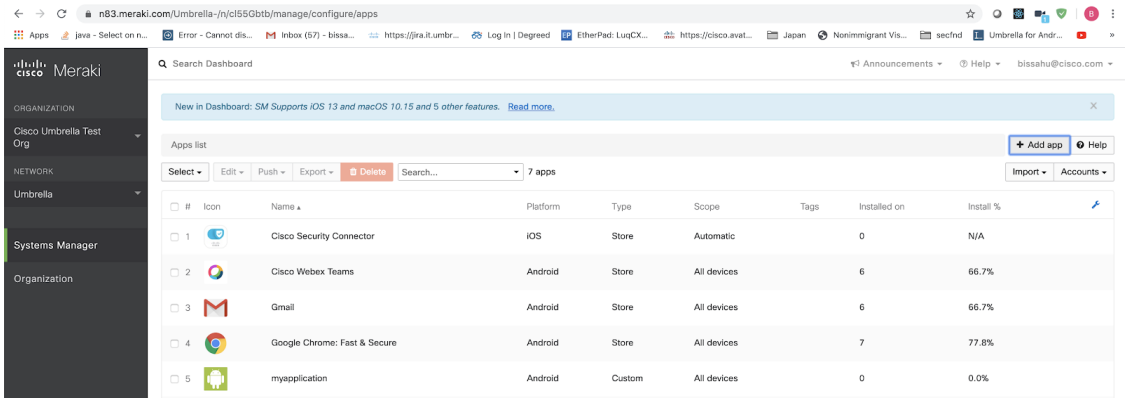
Add App to Cisco Meraki

Provides instructions for completing the Add App to Cisco Meraki workflow in Cisco Secure Access. This process needs to be done only once.

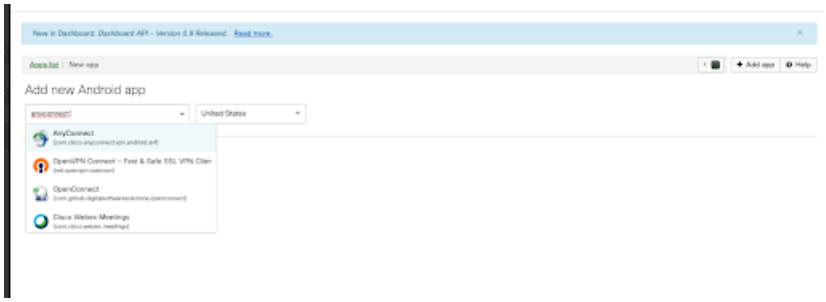
This process needs to be done only once.

Procedure

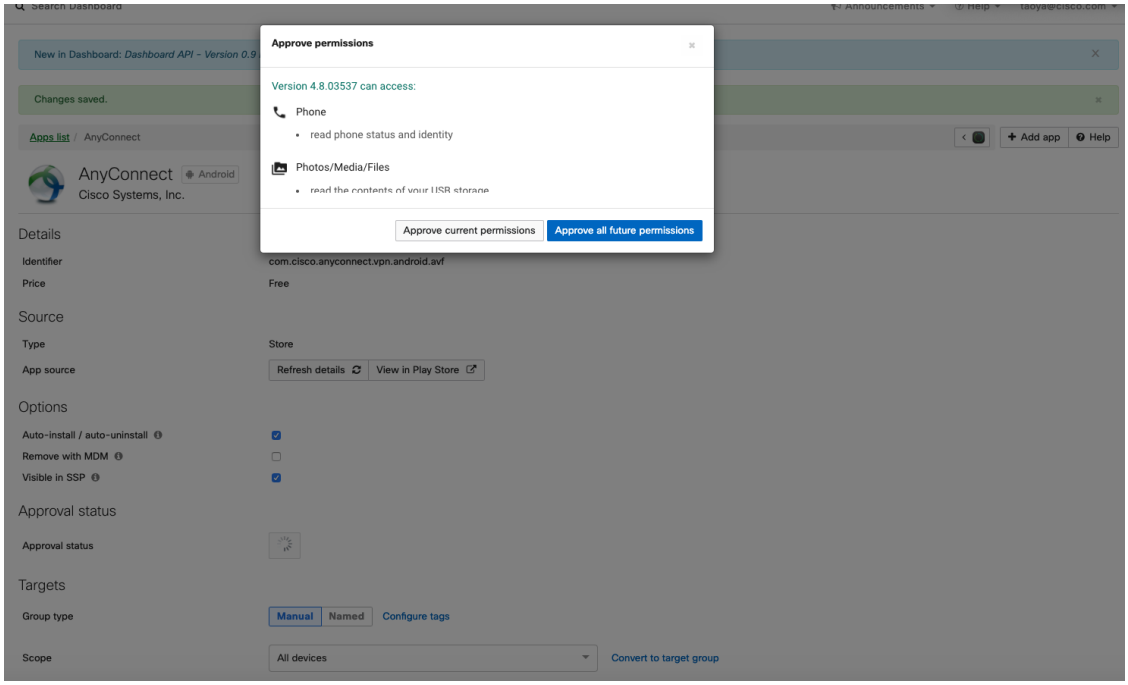
1. In Meraki, navigate to **System Manager** > **Apps** > **Add Apps** > **Add New Android App**.



2. Search for **Cisco Secure Client - AnyConnect** or for the bundle id **com.cisco.anyconnect.vpn.android.avf**.



3. Select the app and approve the permissions, then click **Approve**. If the app has been previously approved, simply re-approve it.

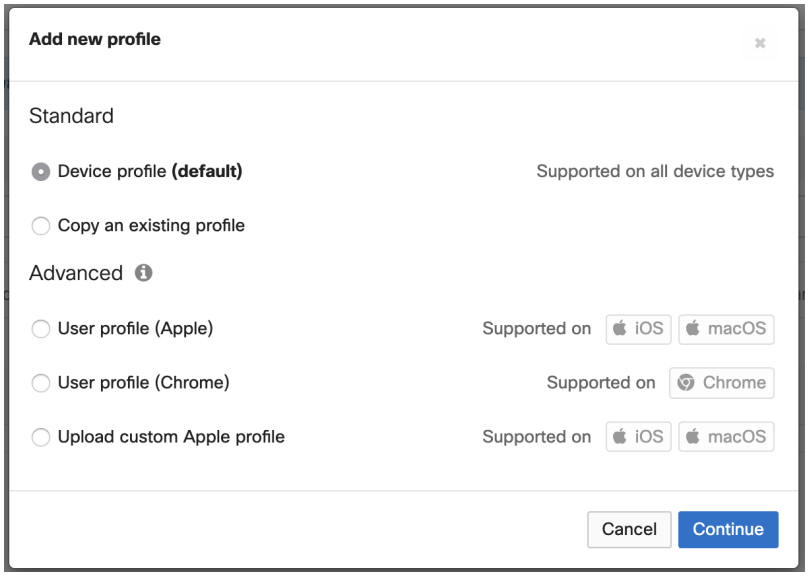


Add Configuration for App

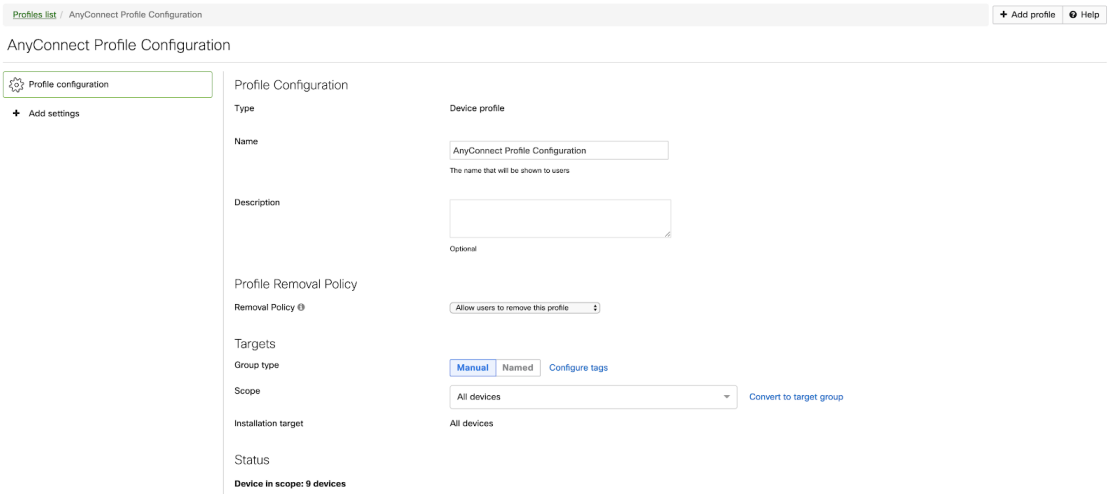
Provides instructions for completing the Add Configuration for App workflow in Cisco Secure Access. Navigate to System Manager Settings and click Add Profile.

Procedure

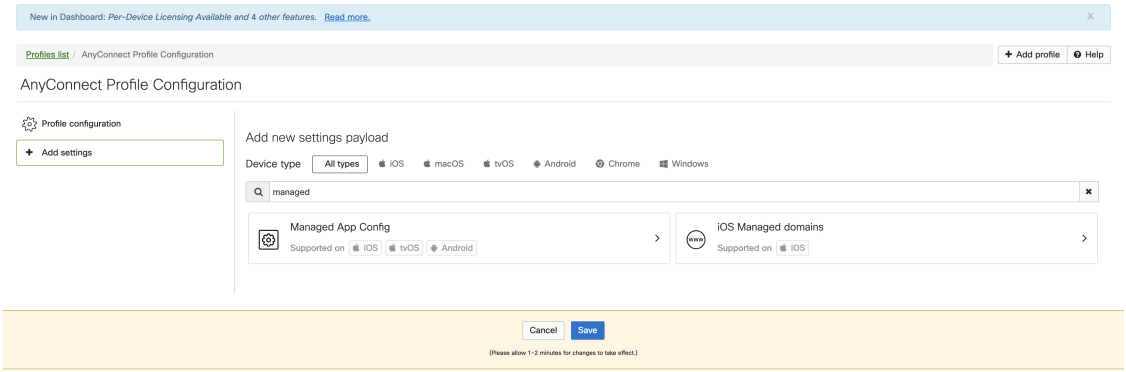
1. Navigate to **System Manager** > **Settings** and click **Add Profile**.
2. Select **Device Profile (default)** from the pop-up, then click **Continue**.



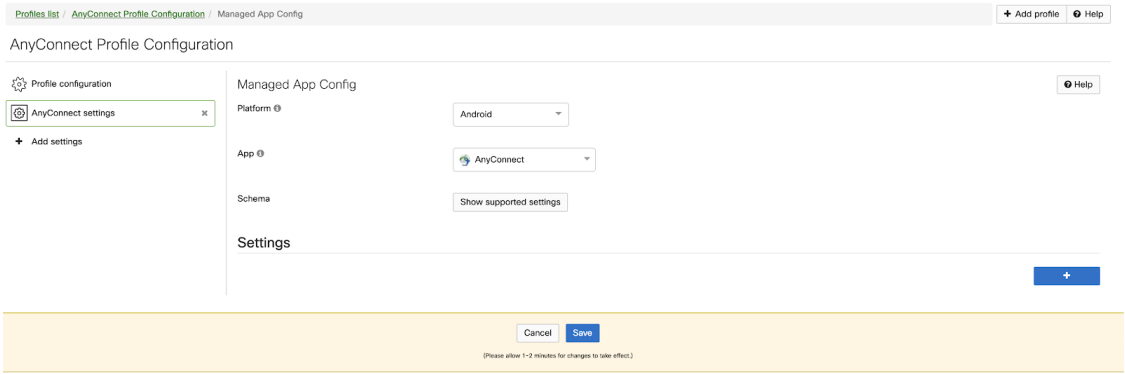
3. Name the profile.



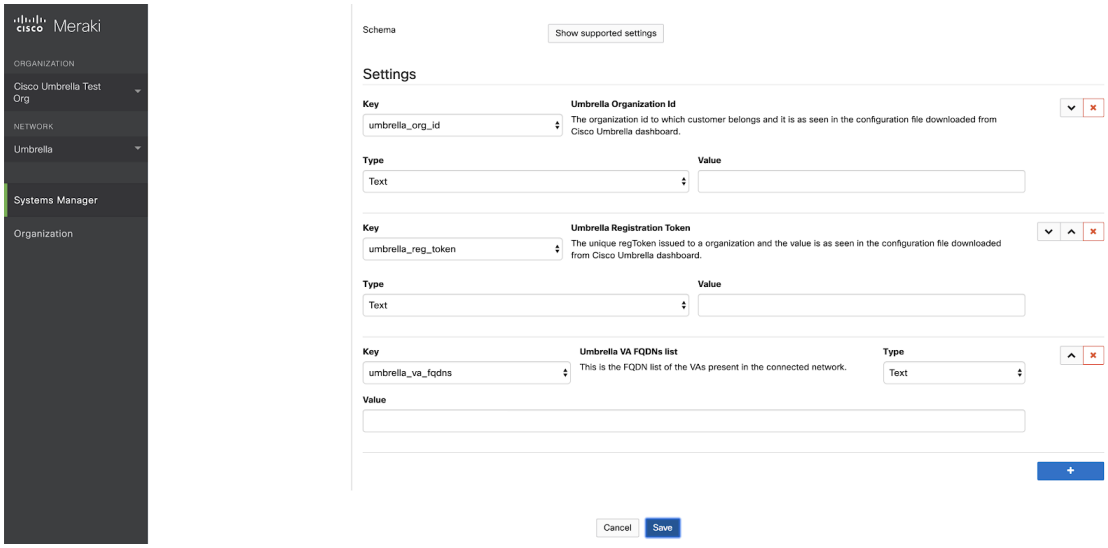
4. Click **Add Settings**.
5. Select the **Android** device type, then search for **Managed App Config**.



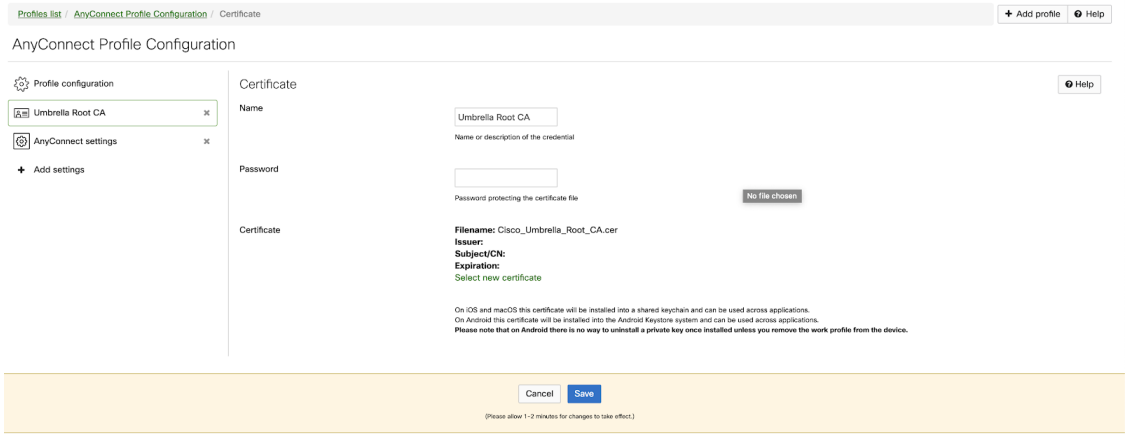
6. Choose **Android** from the **Platform** menu, then choose **Cisco Secure Client - AnyConnect** from the **App** menu.
7. Click **+**.



8. Choose **umbrella_org_id** from the menu, and enter your org ID value. (Refer to the **orgId** property in the mobileconfigAndroid.json file.)
9. Click **+**. Choose **umbrella_reg_token** from the menu and enter the value. (Refer to the **regToken** property in the mobileconfigAndroid.json file.)
10. Click **+**. Choose **umbrella_va_fqdns** from the menu and enter the value. For example, `va1.yourdomain.com`.



11. Click **Add Settings**, then search for *Certificate*. Click to select the result.
12. Name the certificate, then click **Choose File**.



13. In the popup window, select the Secure Access root CA file you downloaded from the Secure Access dashboard. For example, `https://dashboard.sse.cisco.com/o/YOUR-ORG-ID/#/deployments/configuration/rootcertificate`.
14. Click **Save**.
15. Upload the CA certificate, then click **Save**.
16. Navigate to **Profile Configuration** and deploy the configuration to one or more Android devices.
17. Click **Save**.

Push the App to Devices

Provides instructions for completing the Push the App to Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

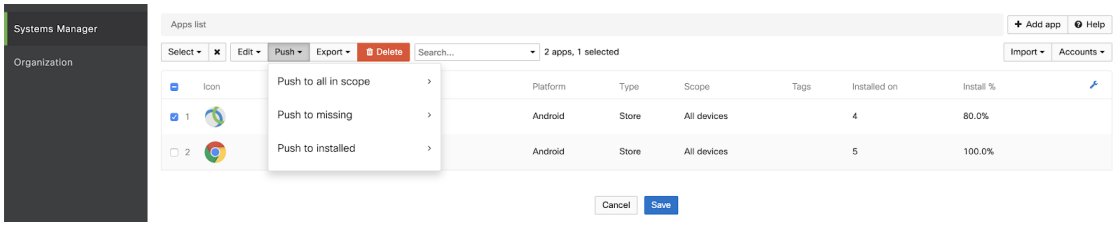
Multiple Device Push

Procedure

---

1. Open **Systems Manager** > **Apps**.
2. Select **Cisco Secure Client- AnyConnect** > **Push**, then push the app to the desired devices.

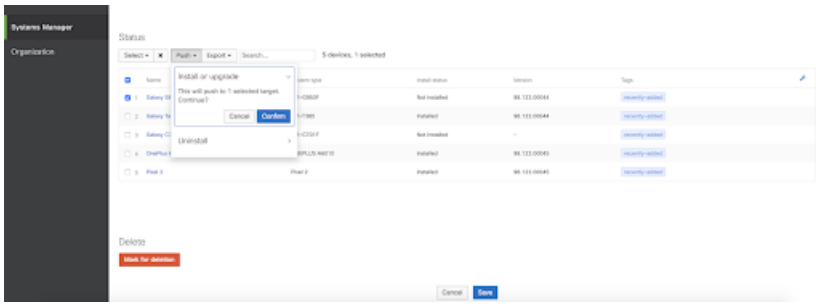
3. Click **Save**.



What to do next

Single Device Push

1. Open **Systems Manager** > **Apps**.
2. Select **Cisco Secure Client - AnyConnect**, then scroll to the device list.
3. Select a specific device, then click **Push**.
4. Click **Save**.



Push the Cisco Root Certificate

Describes Push the Cisco Root Certificate in Cisco Secure Access. For information, see Push the Cisco Root Certificate to Devices.

For information, see Push the Cisco Root Certificate to Devices.

MobileIron MDM

Describes MobileIron MDM in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access, optionally updating it, and then pasting its contents into your MobileIron system, MobileIron is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your Android device is registered with Secure Access. The result is that your Android device is protected by Secure Access.

Note

MobileIron Details

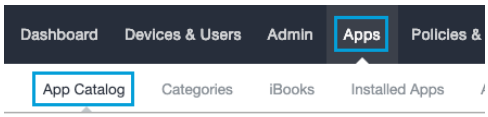
For more information about using the Cisco Secure Access module with the MobileIron Mobile Device Manager, refer to MobileIron documentation, which is available online at MobileIron's website.

Configure the App

Provides instructions for completing the Configure the App workflow in Cisco Secure Access. In your MobileIron admin dashboard, add a label.

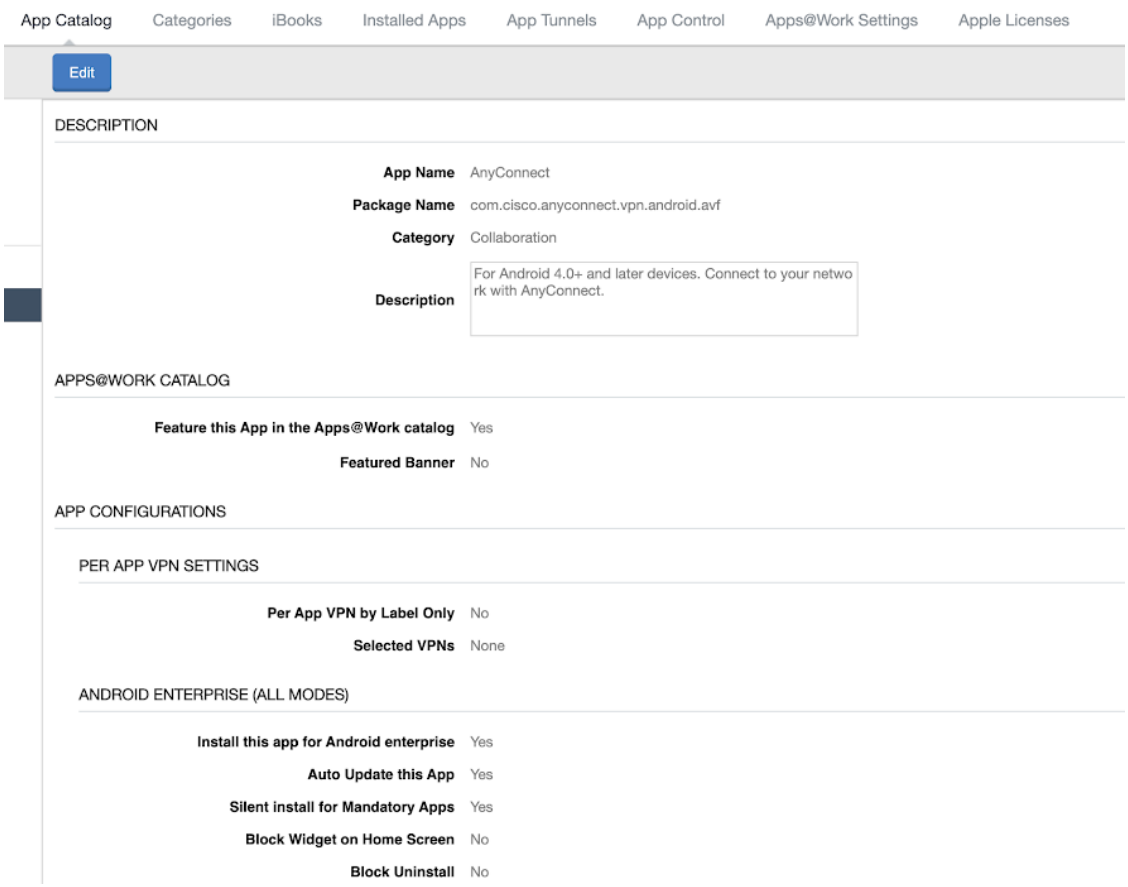
Procedure

1. In your MobileIron admin dashboard, add a label.
2. In your MobileIron dashboard, navigate to **Apps** > **App Catalog**.



3. Search for the app by name: `Cisco Secure Client - AnyConnect` or by bundle id: `com.cisco.anyconnect.vpn.android.avf`
4. Click **Cisco Secure Client- AnyConnect** and open its **Description page**.

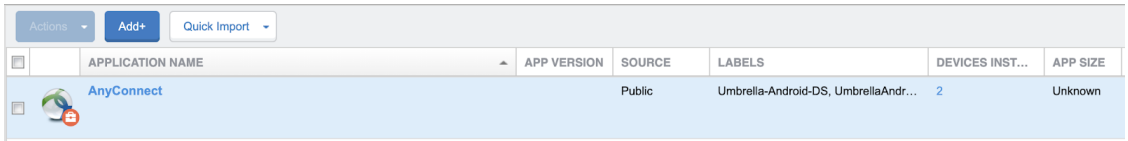




5. Click **Edit** and expand **Default Configuration for AnyConnect**.
6. Scroll to **Umbrella Organization Id**, **Umbrella Registration Token**, and **Umbrella VA FQDN**.



7. Open the file you saved in the section Android Configuration Download. Copy and paste the `organizationid` and `regToken` values from the file into **Umbrella Organization Id** and **Umbrella Registration Token**.
8. Add the Secure Access VA FQDN IPs if there is a VA in the network.
9. Click **Save**.
10. Apply the label you created to the Android app. This label enables the administrator to push the app to managed Android devices.
11. Upload the VA certificate to the MDM and push it to all users.
12. Apply the label you created to the Android app.



The label enables you to push the app to specific users.

Push the App

Provides instructions for completing the Push the App workflow in Cisco Secure Access. In your MobileIron dashboard, navigate to Devices and Users Devices .

Procedure

1. In your MobileIron dashboard, navigate to **Devices & Users** > **Devices**.
2. Select a registered device from the Devices List.
3. Apply the label to the device.
4. Select **Force Device Check-In** from the **Actions** menu to push the app to the selected device.

Push User Identities

Describes Push User Identities in Cisco Secure Access. When user identities are pushed to Secure Access, you can identify and search users and devices.

When user identities are pushed to Secure Access, you can identify and search users and devices. For more information, see Manage Identities.

Push the Cisco Root Certificate

Describes Push the Cisco Root Certificate in Cisco Secure Access. For more information, see Push the Cisco Root Certificate to Devices.

For more information, see Push the Cisco Root Certificate to Devices.

VMware Workspace ONE

Describes VMware Workspace ONE in Cisco Secure Access. This section explains how to deploy the Umbrella module on Android devices using zero-touch deployment.

This section explains how to deploy the Umbrella module on Android devices using zero-touch deployment. This method ensures seamless protection by enabling Always On VPN through the Mobile Device Manager (MDM) Workspace One, without manual intervention.

The Umbrella module in Cisco Secure Client provides robust protection against threats by securing both applications and internet-based traffic at the DNS layer on Android devices.

Note

Workspace ONE Details

For more information about using the Cisco Umbrella Anyconnect module with the Workspace ONE MDM, refer to the Workspace ONE documentation available online on VMWare's documentation website.

Important

Install the Cisco Secure Client only after you have published and installed the Always On VPN profile in Workspace One Intelligent Hub.

Prerequisites for Deployment

- Complete the Android EMM (Enterprise Mobility Management) registration, device enrollment, and a work profile creation.

- Ensure that the MDM app Hub is visible within the work profile.

Create Always On VPN Profile

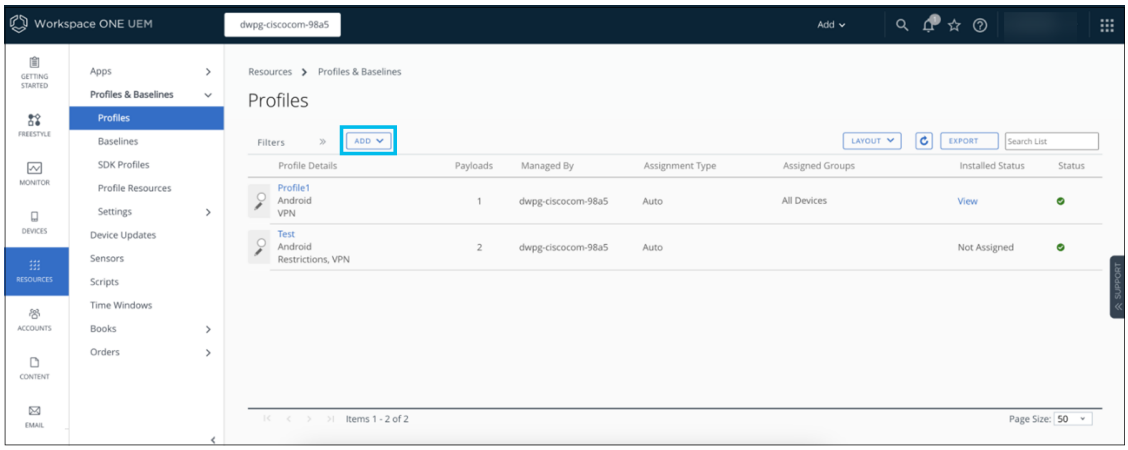
Provides instructions for completing the Create Always On VPN Profile workflow in Cisco Secure Access. In the Workspace ONE UEM console, navigate to Resources Profiles and Baselines Profiles .

Before you begin

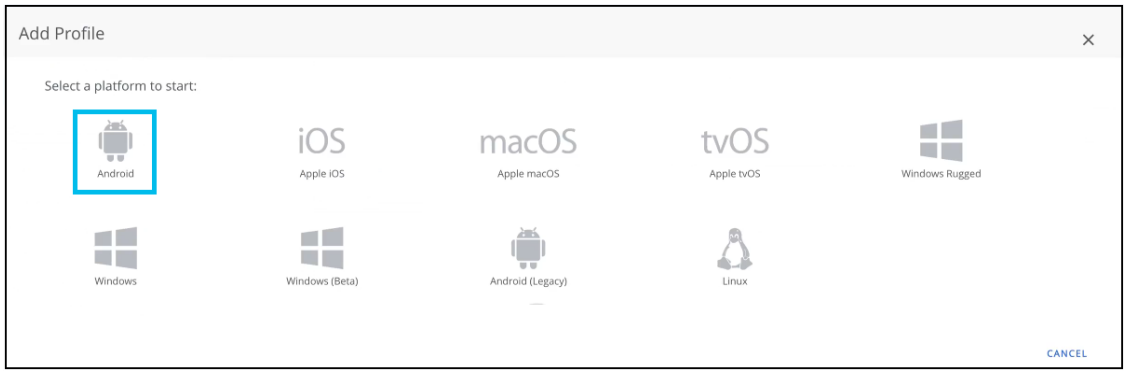
Before you create an Always On profile, we **strongly** recommend ensuring both your Windows operating system is up to date with sustem-provided updates and your Windows Defender account is **not** out of date. Insufficient versioning and noncompliance causes policy failure.

Procedure

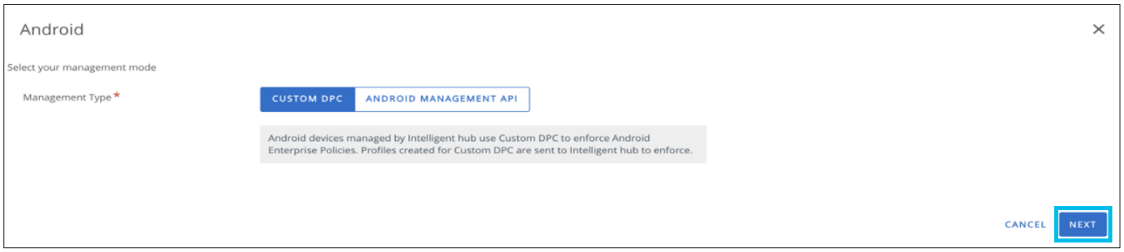
1. In the Workspace ONE UEM console, navigate to **Resources** > **Profiles & Baselines** > **Profiles**.
2. Click **Add** and choose **Add Profile** from the drop-down list.



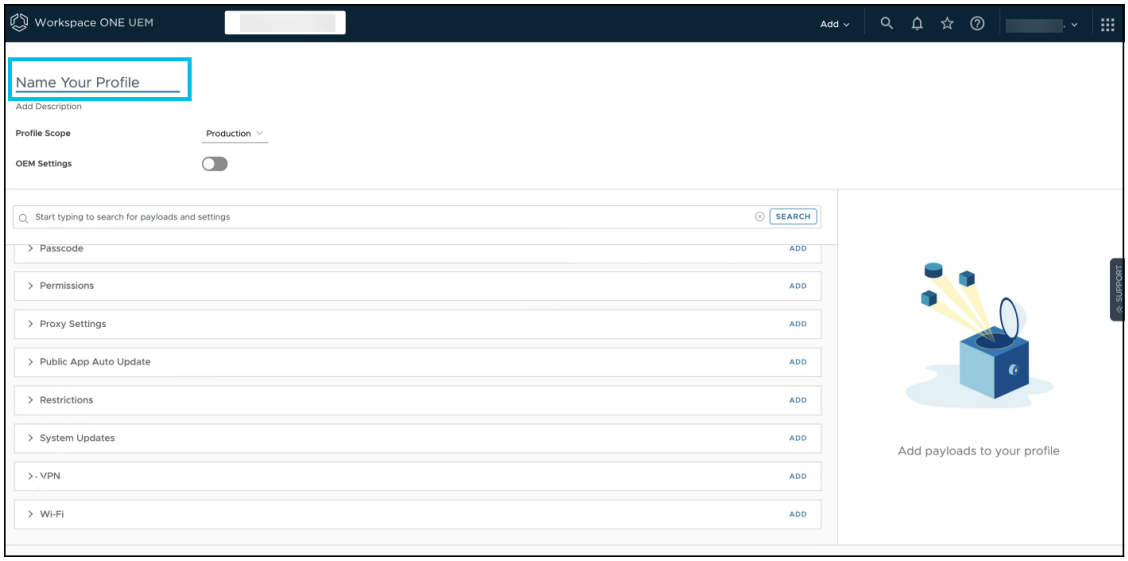
3. Select **Android** as the platform.



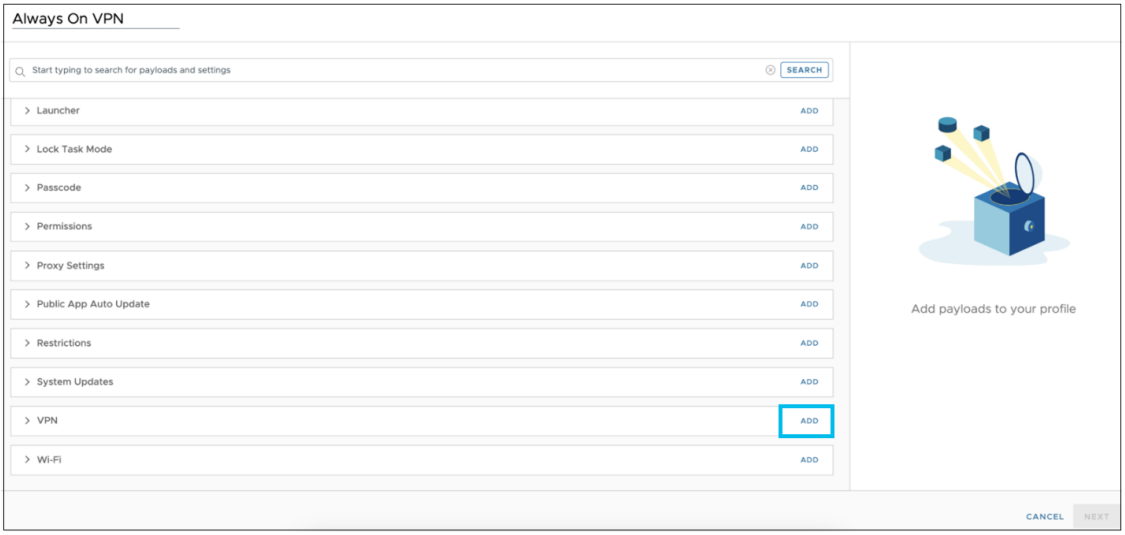
4. Choose **CUSTOM DPC** or **ANDROID MANAGEMENT API** as the **Management Type** and click **Next**.



5. Enter a name for your profile. For example, *Always On VPN*.

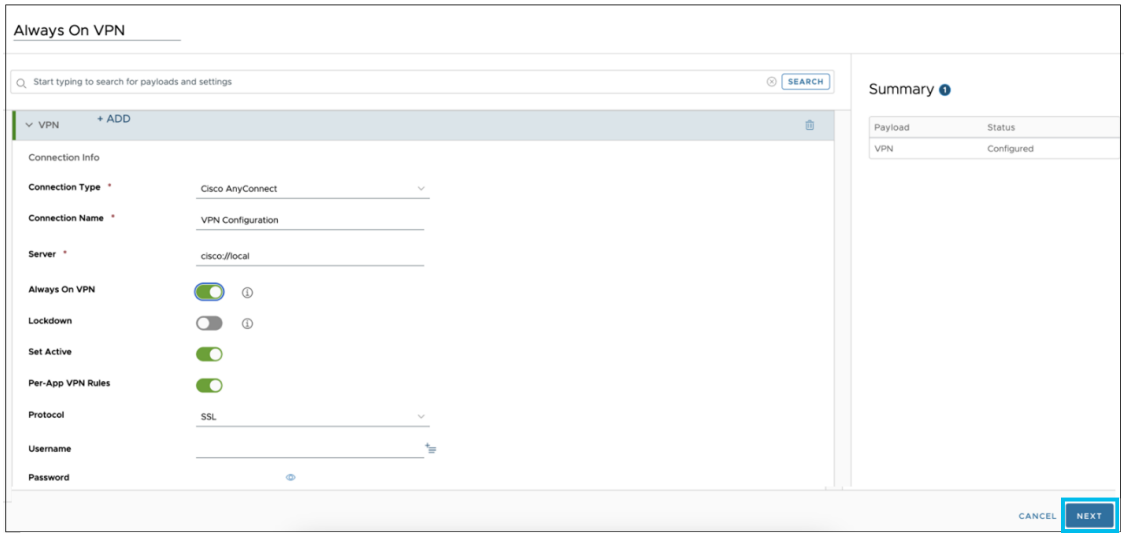


6. Navigate to the **VPN** section and click **Add**.

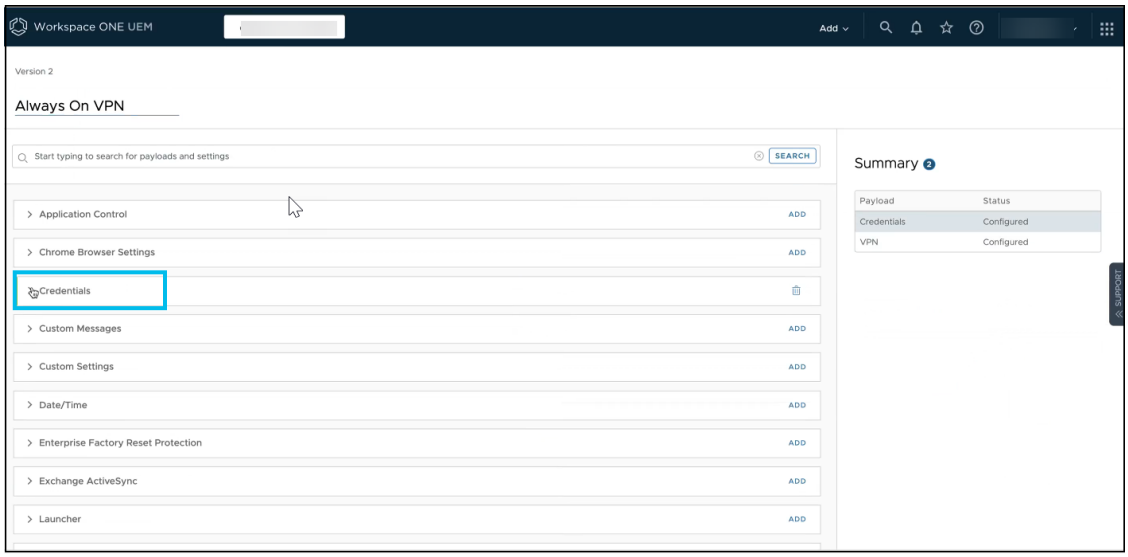


7. In the VPN setting configuration section, complete the fields, including the following:
   - From the **Connection Type** drop-down list, choose **Cisco AnyConnect**.
   - In the **Server** field, enter *cisco://local*.
   - In the **Connection Name**, enter the name.
   - Enable the **Always on VPN** button.
   - Enable the **Set Active** button.
   - Enable the **Per-App VPN Rules** button.

8. Click **Next**.



9. Search or navigate to the **Credentials** section, and click **Add**.

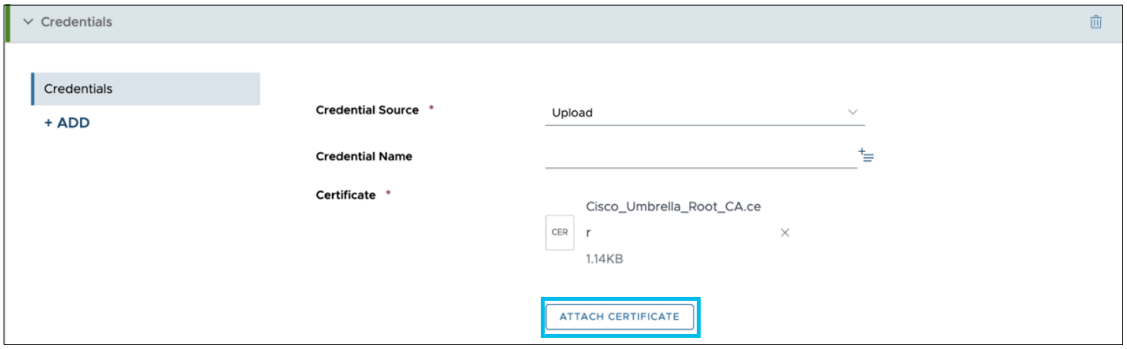


10. In the Credential section, do the following:

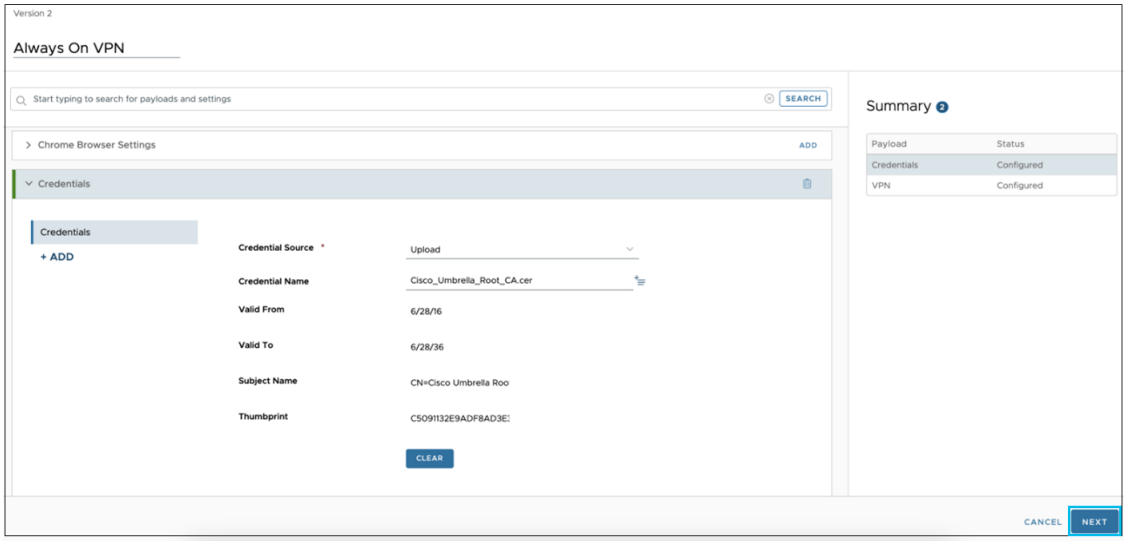
- From the **Credential Source** drop-down list, choose **Upload**.
- Click **Choose File** to browse and select the **Cisco_Umbrella_Root_CA Certificate** downloaded from Umbrella.

> **Note**
>
> In Umbrella, navigate to **Deployments** > **Configuration** > **Root Certificate**, expand **Cisco Root Certificate Authority**, and download the Cisco Umbrella root certificate, see Push the Umbrella Certificate to Managed Devices

- Click **ATTACH CERTIFICATE**.



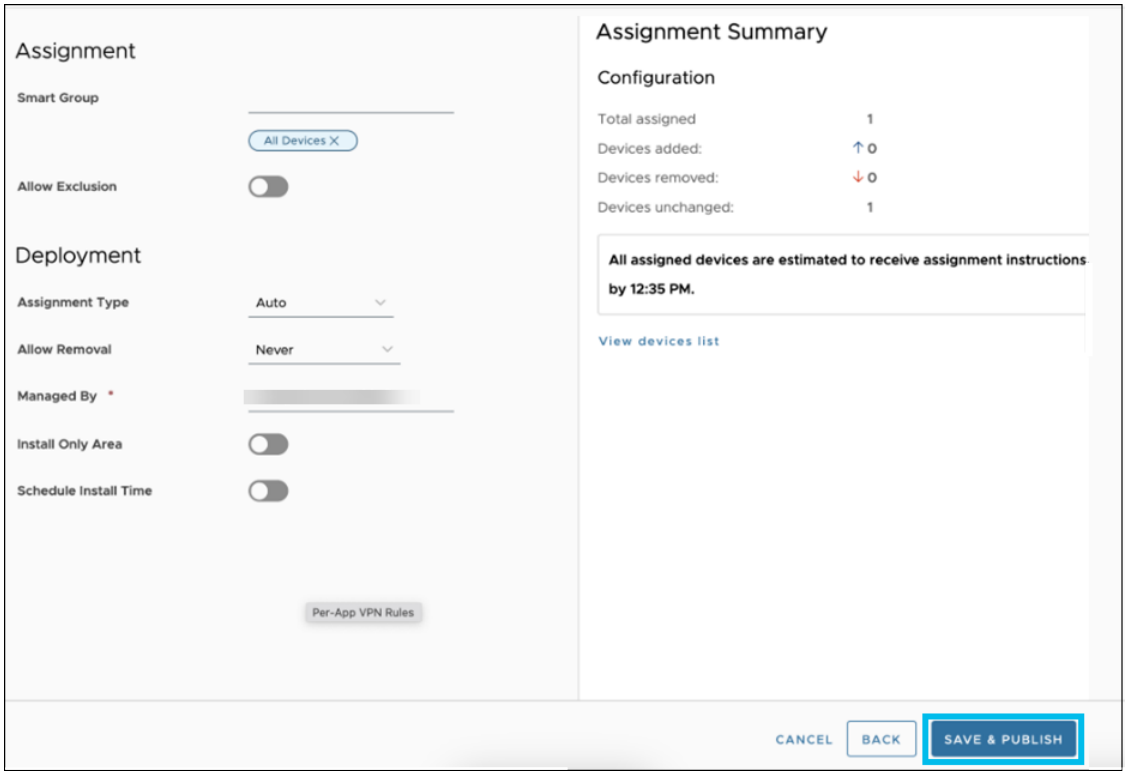
11. After successful upload of the certificate, the **Credential Name** would be added automatically and then click **Next**.



12. In the Assignment and Deployment profile settings screen, complete the fields, including the following:

- In the **Smart Group** field, choose the group of devices to which the Always On VPN profile is to be assigned.
- Select the appropriate deployment values. Choose **Auto** from the **Assignment Type** drop-down list, to deploy the profile to all device automatically.

13. Click **Save & Publish**.

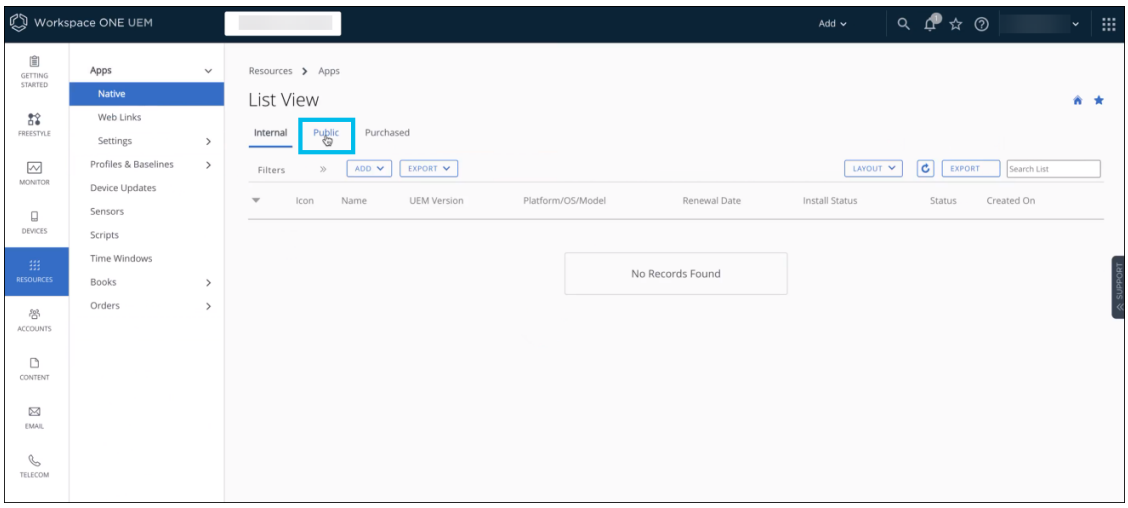


Add and Publish the Cisco Secure Client Application

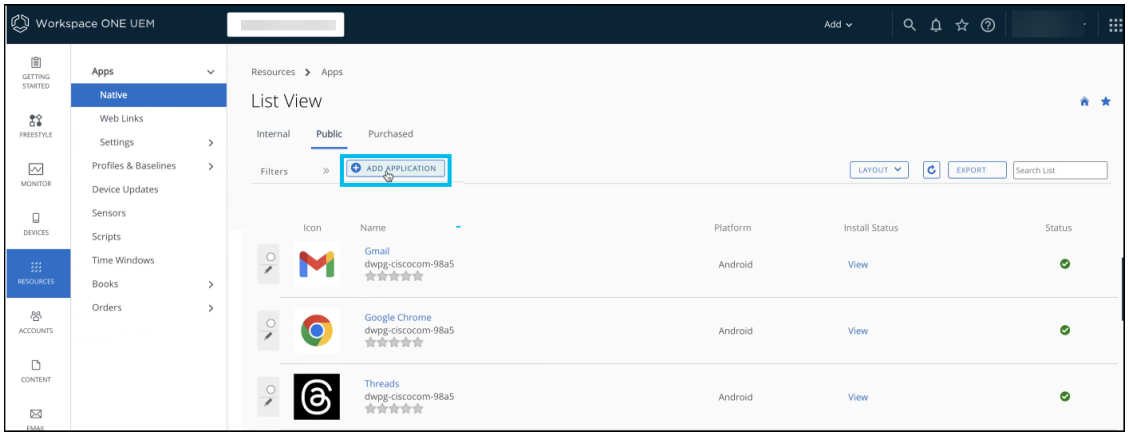
Provides instructions for completing the Add and Publish the Cisco Secure Client Application workflow in Cisco Secure Access. In the Workspace ONE UEM console, navigate to ResourcesNativePublic.

Procedure

1. In the **Workspace ONE UEM** console, navigate to **Resources** > **Native** > **Public**.

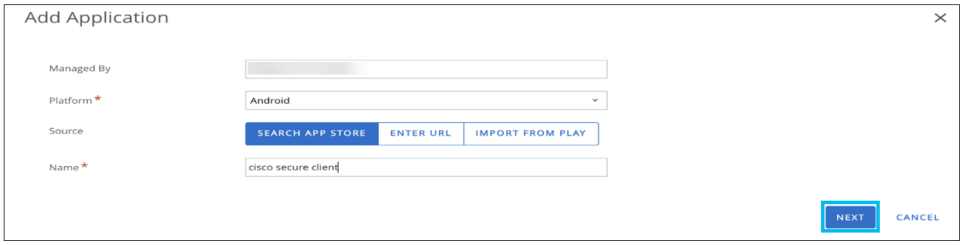


2. Click **Add Application**.

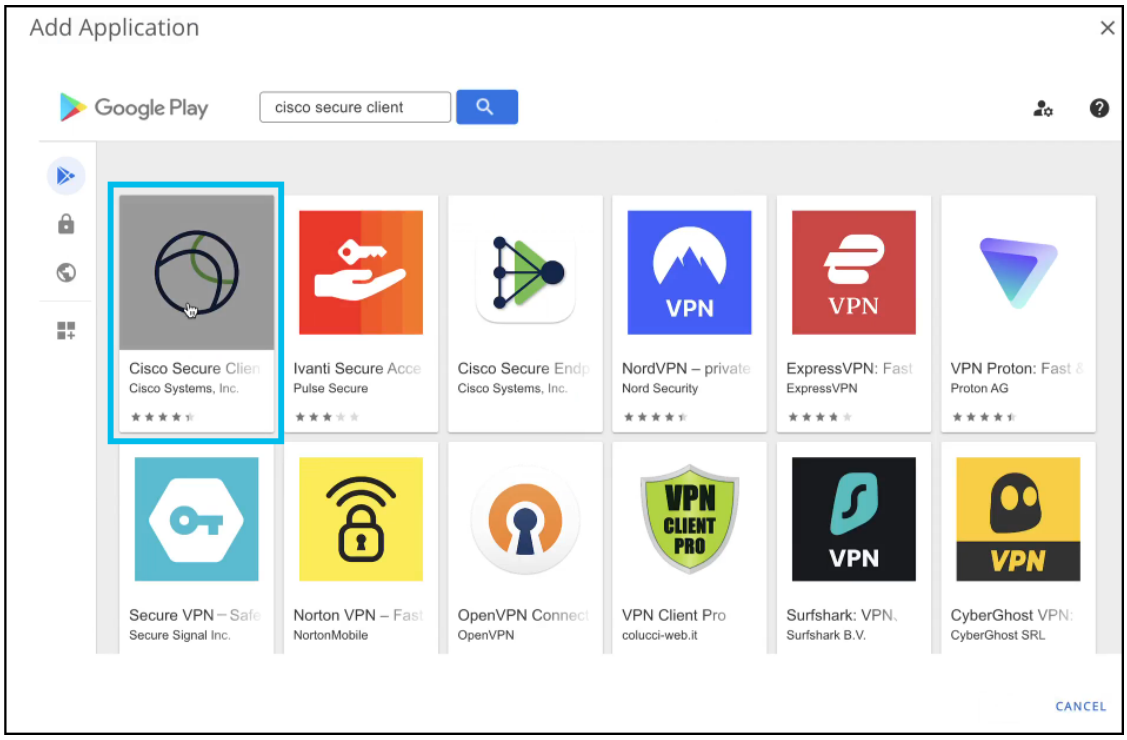


a. To add the **Cisco Secure Client** application, add the following details:

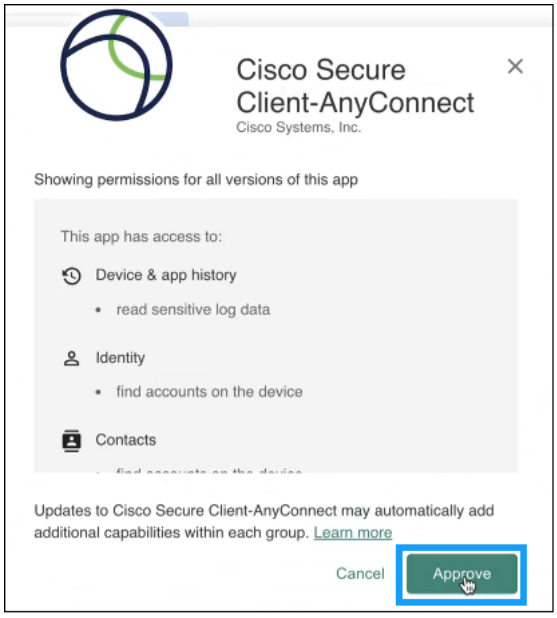
1. Enter **Managed By** field, choose the Organization Group that you set up to manage applications.
2. From the **Platform** drop-down list, choose **Android**.
3. In the **Source** field, select **SEARCH APP STORE** to search for the application in the app store.
4. In the **Name** field, enter *Cisco Secure Client* and click **Next**. Google Play launches within the console.



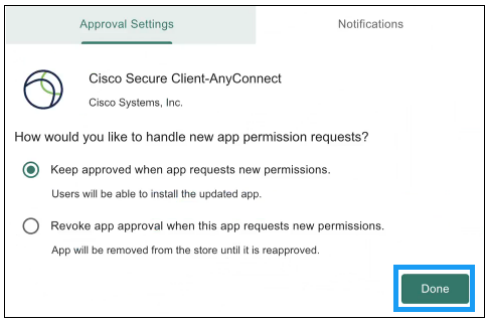
3. In the Google Play store, click the **Cisco Secure Client AnyConnect** application.



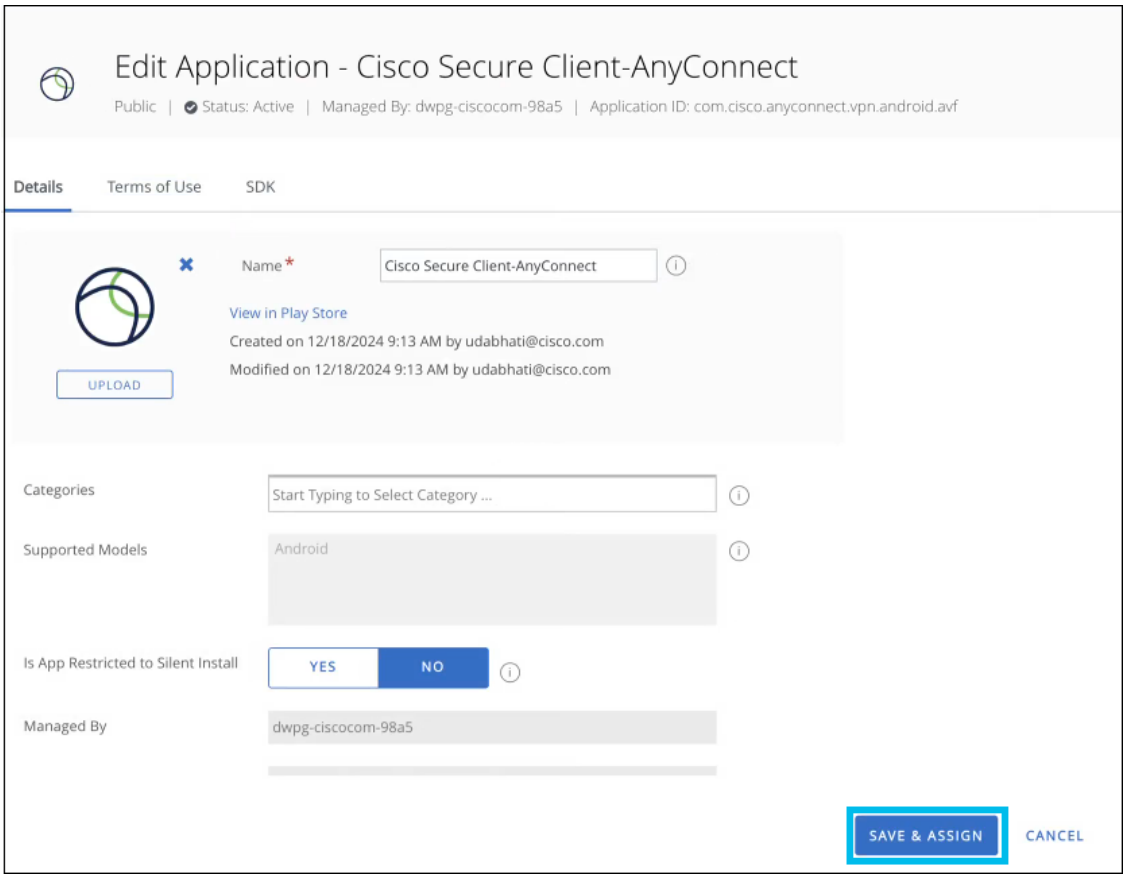
4. Click **Approve** to accept the permission for all versions of the application.



5. Click **Done** to handle the new app permission requests.

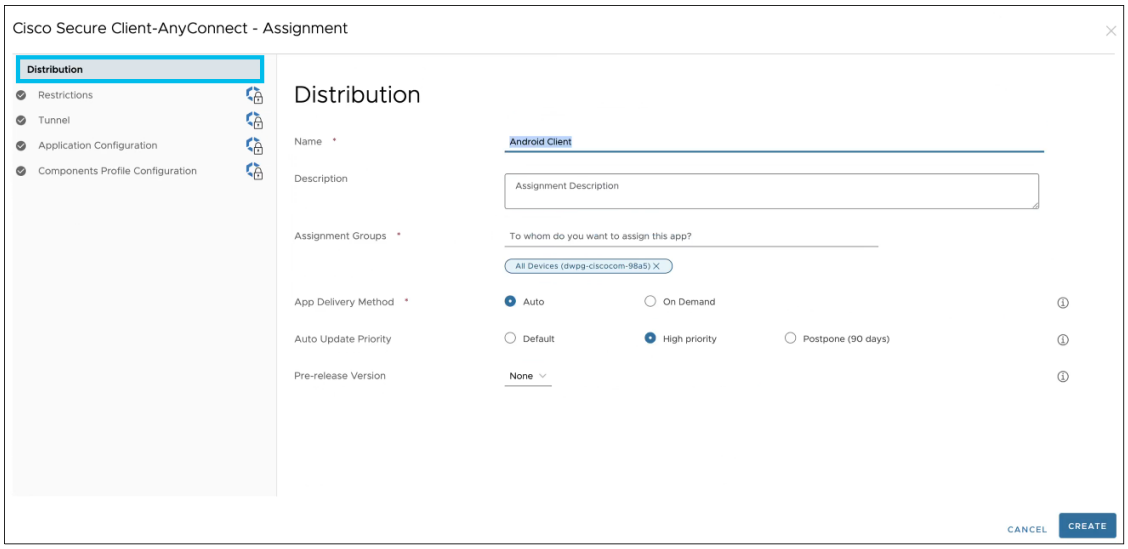


6. Now, click **Save & Assign**.

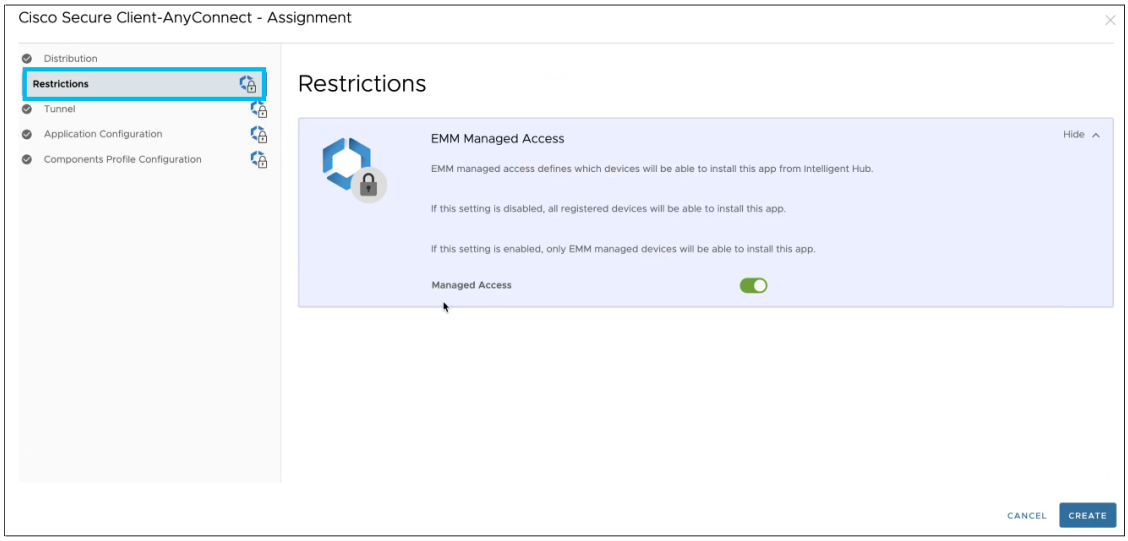


The Cisco Secure Client-AnyConnect Assignment Wizard appears:

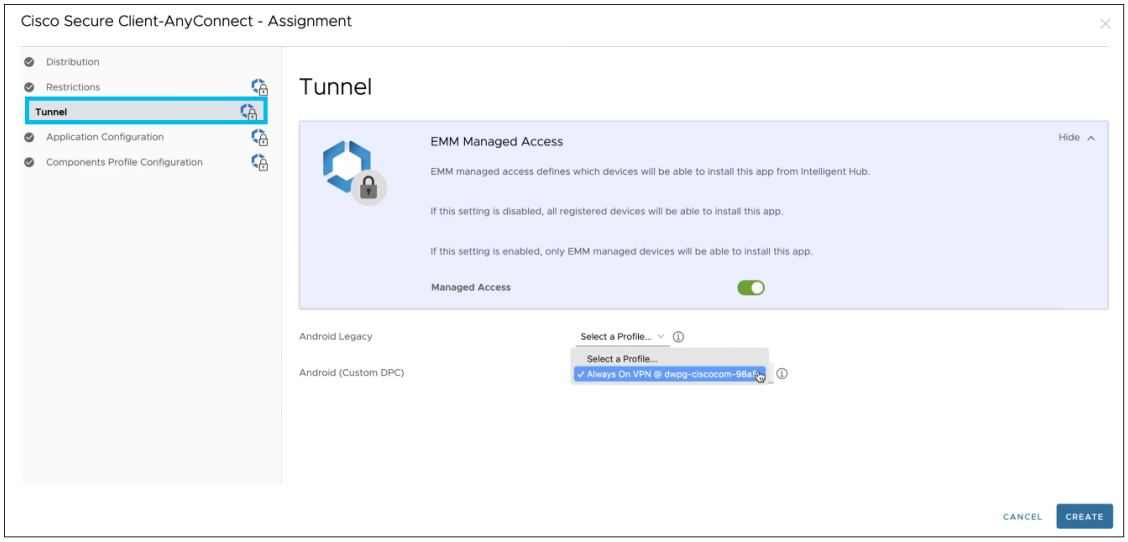
7. On the **Distribution** page, enter the necessary details to define how the application will be distributed. Click **Restrictions**.



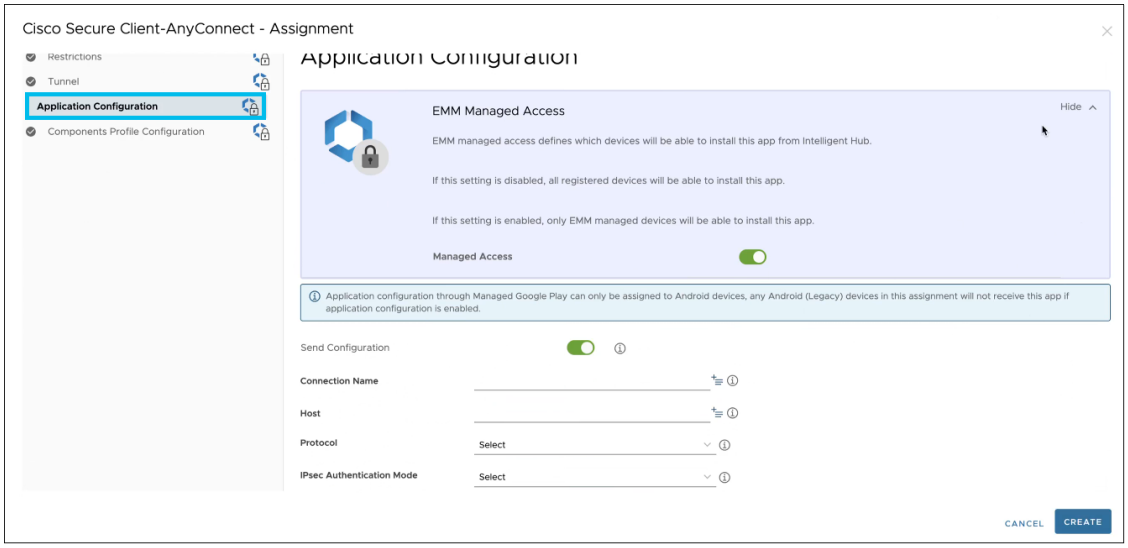
8. On the **Restrictions** page, enable the **Managed Access** button to allow only EMM managed devices to install the application. Click **Tunnel**.



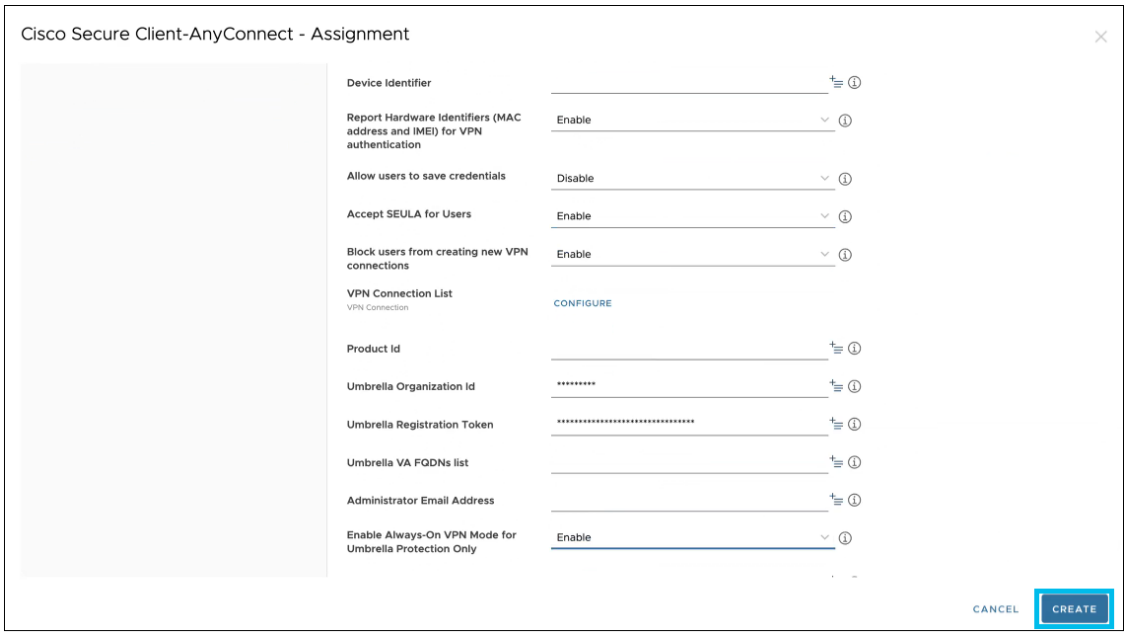
9. On the **Tunnel** page, from the **Android (Custom DPC)** drop-down list, choose the Always On VPN profile created in the Create Always On VPN Profile section. This enables the Always On VPN profile for the managed devices. Click **Application Configuration**.



The Application Configuration page appears.



10. On the **Application Configuration** page, complete the fields, including the following:
    - Leave the **Host** field empty, as the server details are taken from the profile.
    - From the **Accept SEULA For Users** drop-down list, choose **Enable** to prevent users from manually accepting the SEULA banner.
    - From the **Enable Always On VPN Mode for Secure Access Protection Only** drop-down list, choose **Enable** to allow the Cisco Secure Client application to automatically manage protection and seamlessly accept VPN connection requests when Secure Access protection is activated.
    - From the **Block users from creating new VPN connections** drop-down list, choose **Enable**.
    - Enter the application configuration details, such as, Secure Access Organization Id and Registration Token, by referring the **Android Config File** downloaded from the dashboard. For more information on how to download Android Config File, see Android Configuration Download.

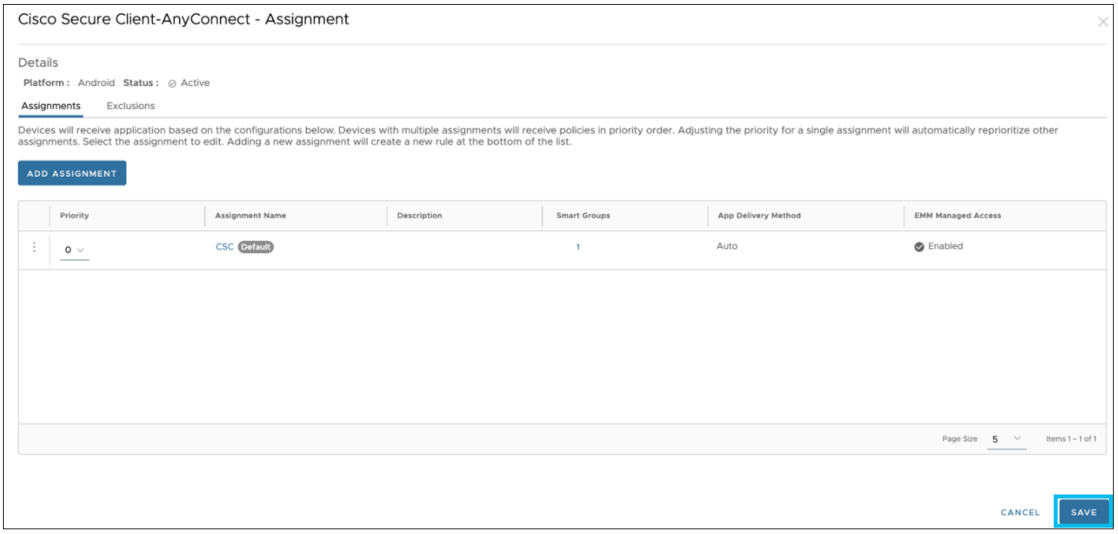


11. Click **Components Profile Configuration**.
12. Click **Create**.

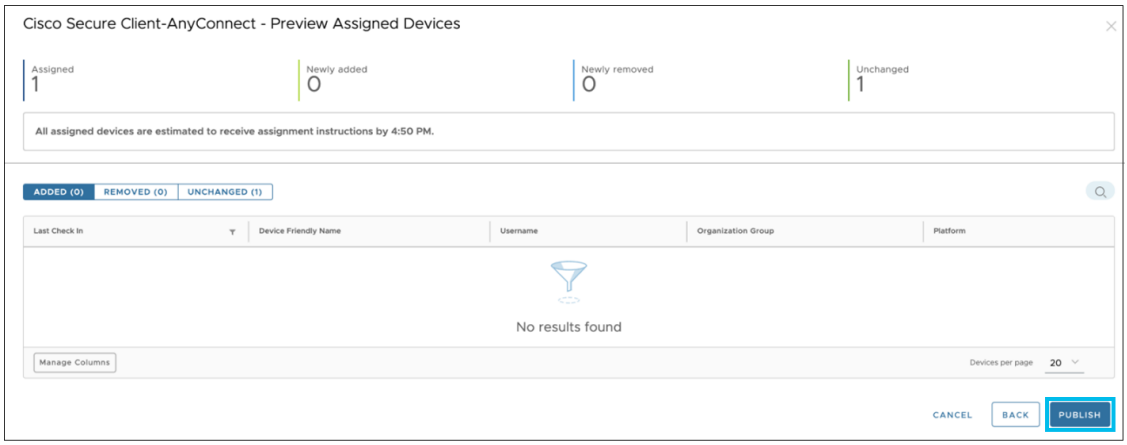


The Cisco Secure Client-AnyConnect app assignment is created.

13. Click **Save**.



14. Click **Publish** to publish the Cisco Secure Client Application.



What to do next

As the app delivery method is set to auto on the Distribution page the application gets installed automatically on the device and is displayed in both the console and your device.

Microsoft Intune MDM

Describes Microsoft Intune MDM in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access and then uploading it to your Intune system, Intune is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your Android device is registered with Secure Access. The result is that your Android device is protected by Secure Access.

For information about configuring Intune, see Intune's documentation.

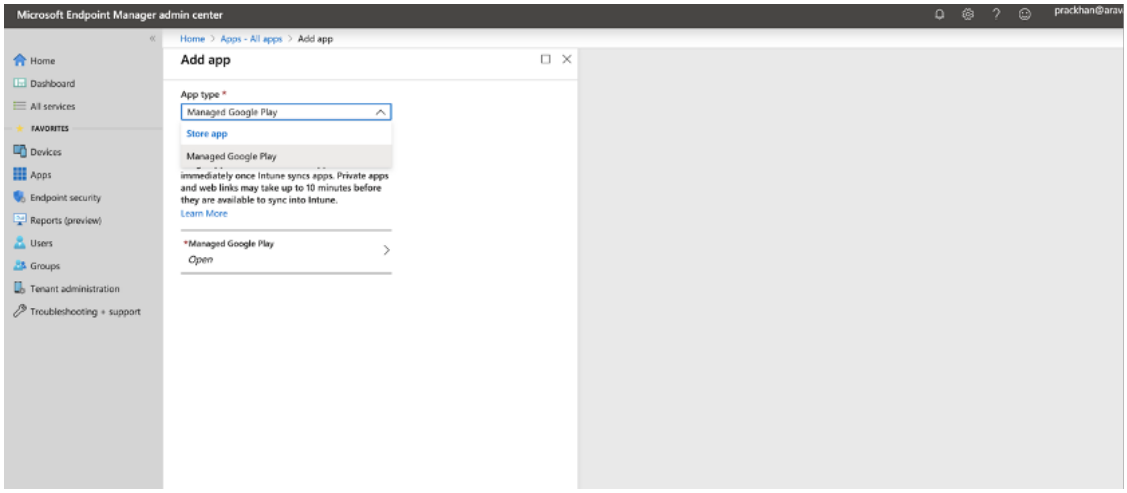
> **Note**
>
> **Microsoft InTune Details**
>
> For more information about using the Cisco Secure Access module with the InTune Mobile Device Manager, see InTune documentation, available online at Microsoft's documentation website.

Publish the Cisco Secure Client - AnyConnect App to Managed Android Devices

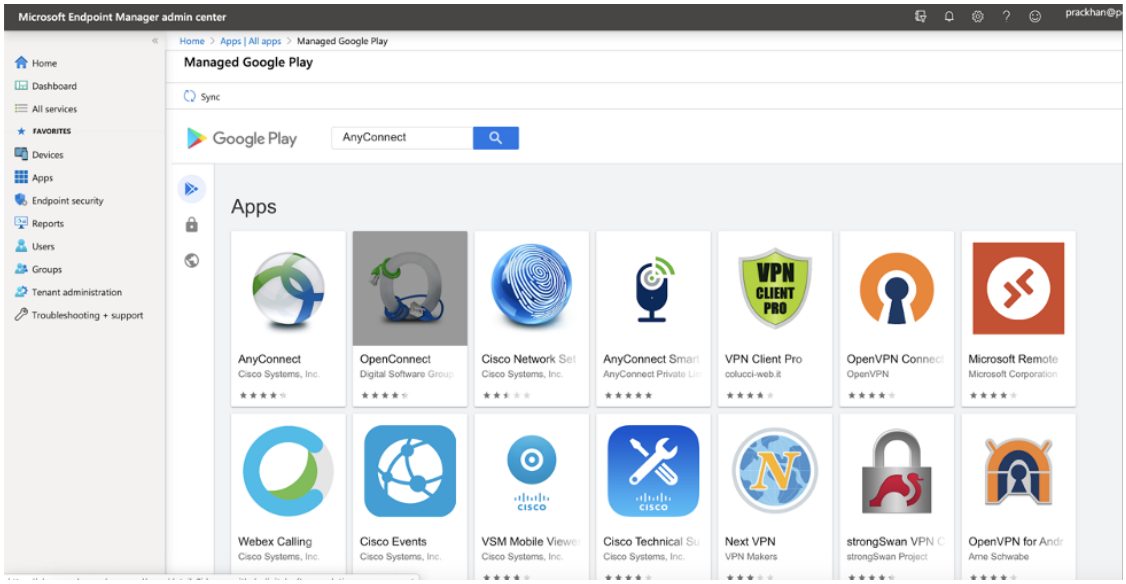
Provides instructions for completing the Publish the Cisco Secure Client - AnyConnect App to Managed Android Devices workflow in Cisco Secure Access. In your InTune dashboard, navigate to Apps All Apps Add Application .

Procedure

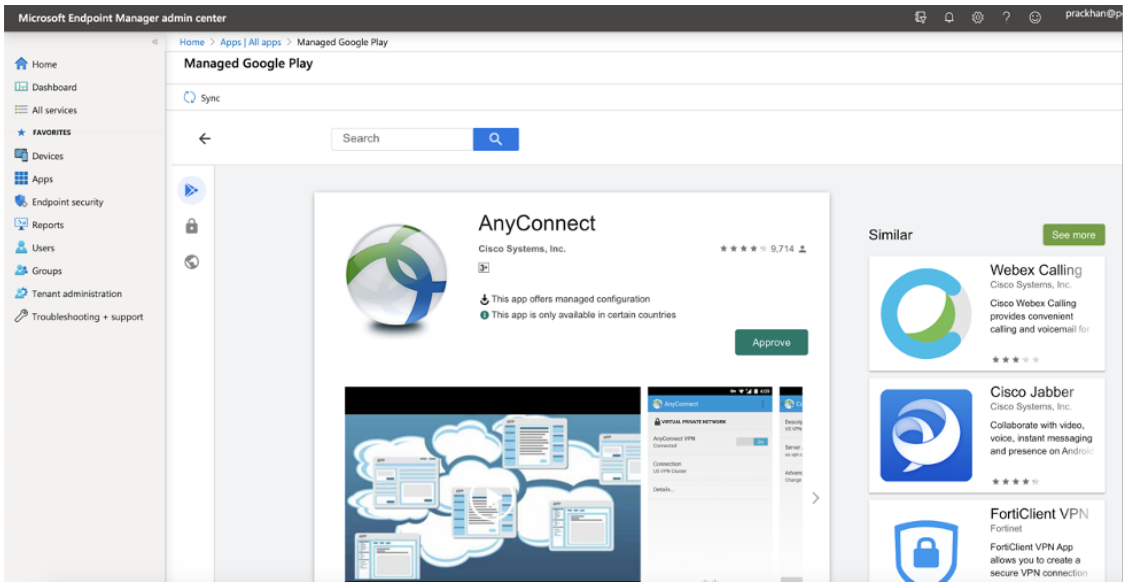
1. In your InTune dashboard, navigate to **Apps** > **All Apps** > **Add Application**.
2. From the **App Type** pull-down, choose **Managed Google Play**.



3. In the Play store, search for `Cisco Secure Client - AnyConnect` (or the bundle id: `com.cisco.anyconnect.vpn.android.avf`).



4. Approve the app and then click **Select**.
5. Click *Sync*. The app appears in the App List after syncing.



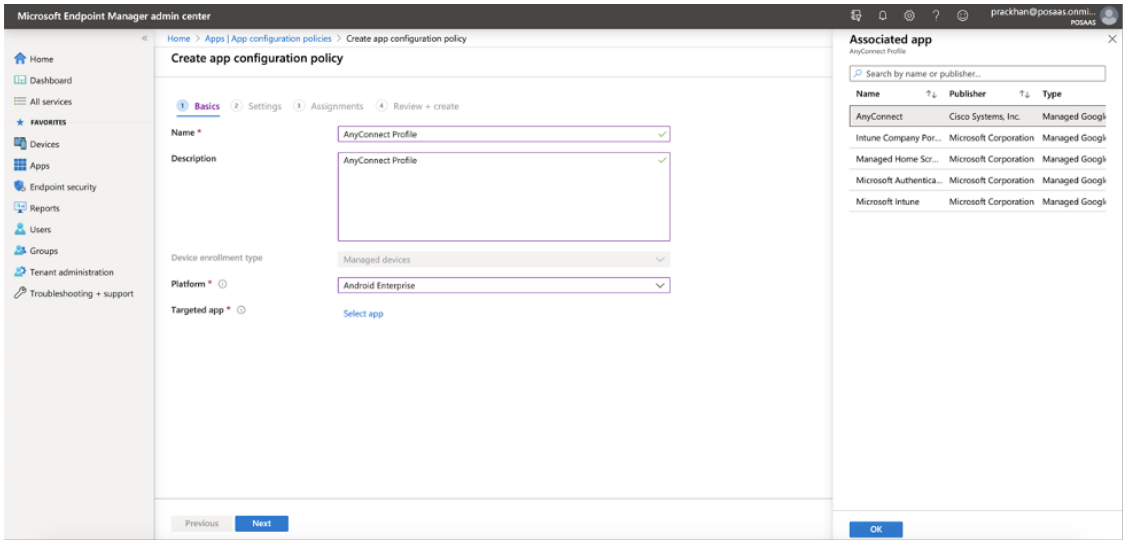
Configure Secure Access

Provides instructions for completing the Configure Secure Access workflow in Cisco Secure Access. In your InTune dashboard, navigate to Apps Configuration Policy .

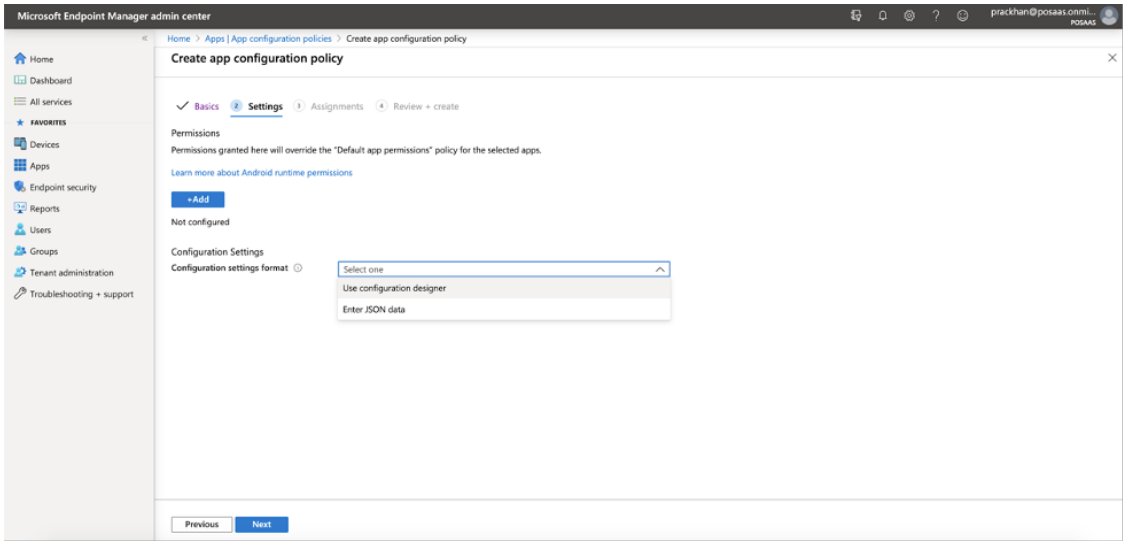
Procedure

---

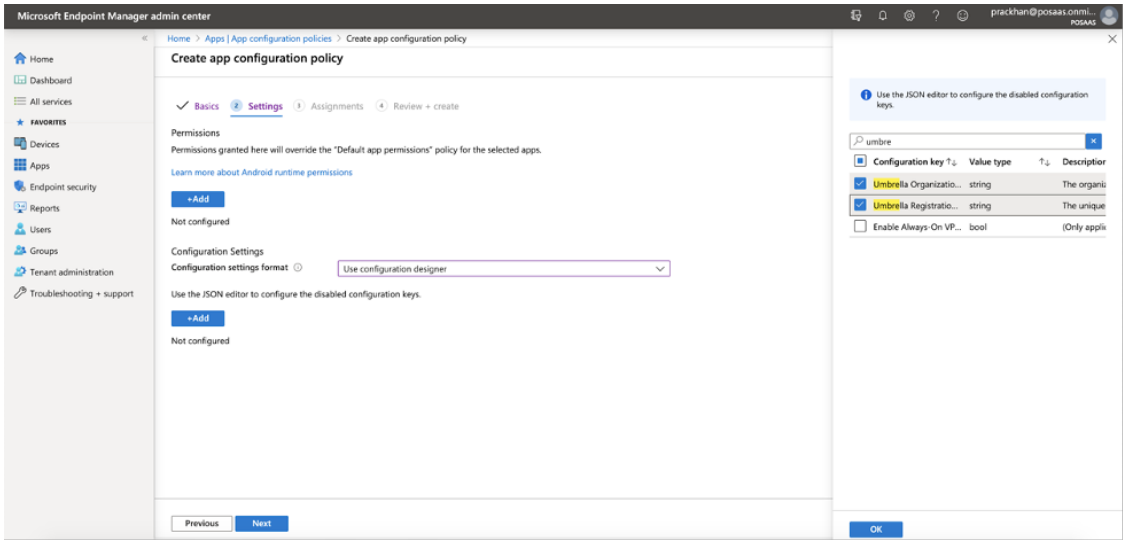
1. In your InTune dashboard, navigate to **Apps** > **Configuration Policy**.
2. Create a new policy, including name and description. Select the "Managed Device" enrollment type and set the platform to “Android”.

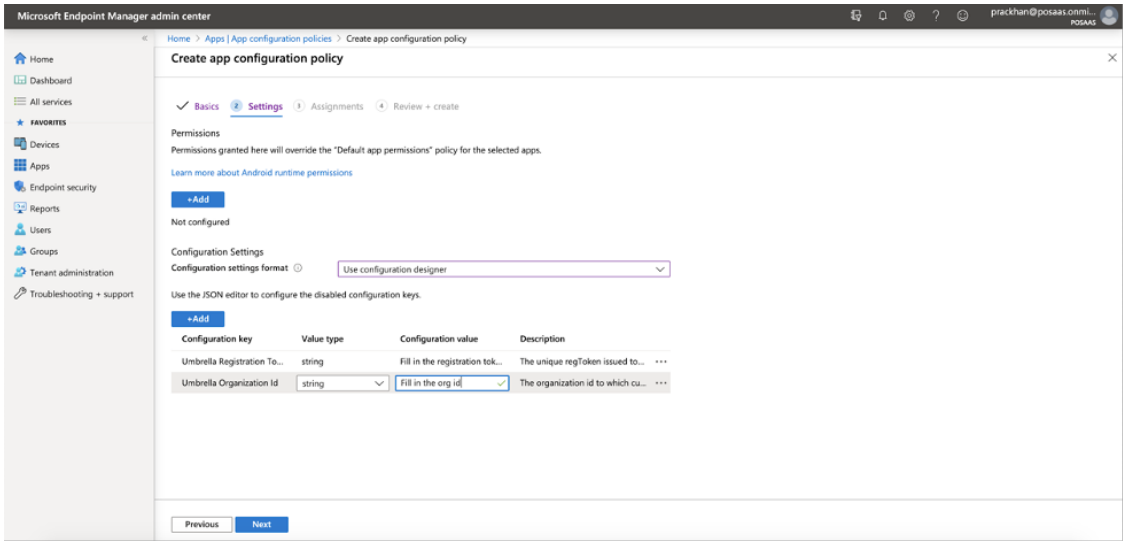


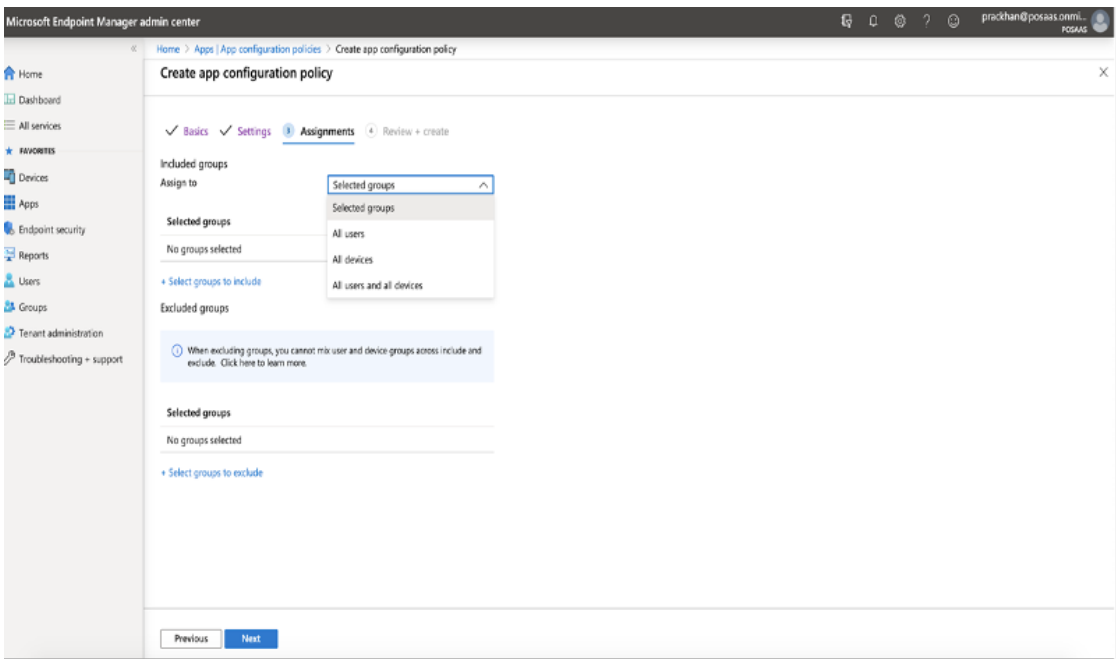
3. Click **Associated App**, search for **Cisco Secure Client - AnyConnect**, and then click **OK**.
4. Click **Configuration Settings**, select **Use Configuration Designer** and then click **Add**.



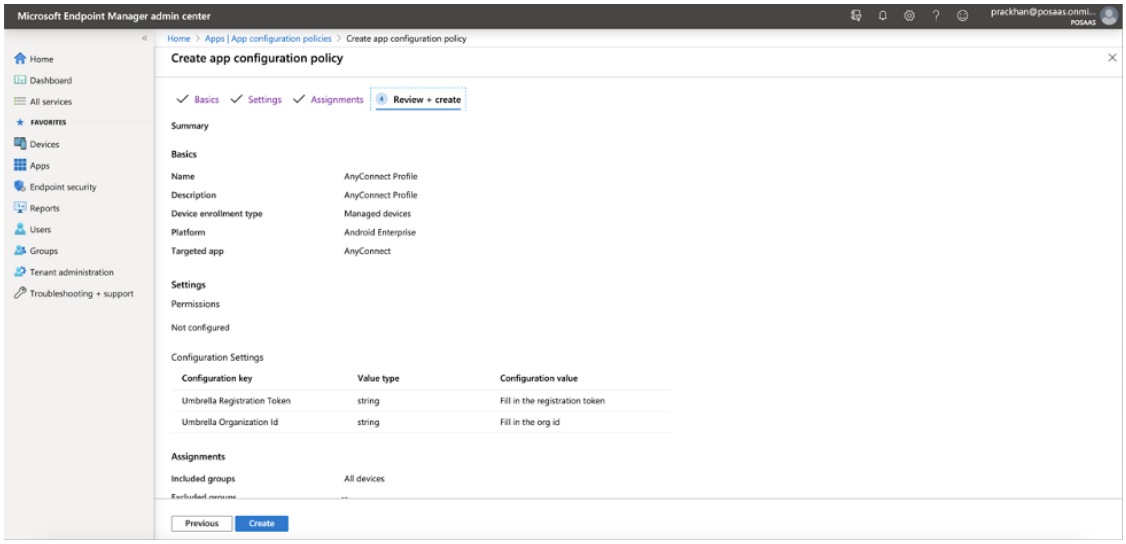
5. Search for Secure Access and add the values for **Umbrella Organization ID** and **Umbrella Registration Token** from the file you downloaded in the section Android Configuration Download.
6. Click **Add**.



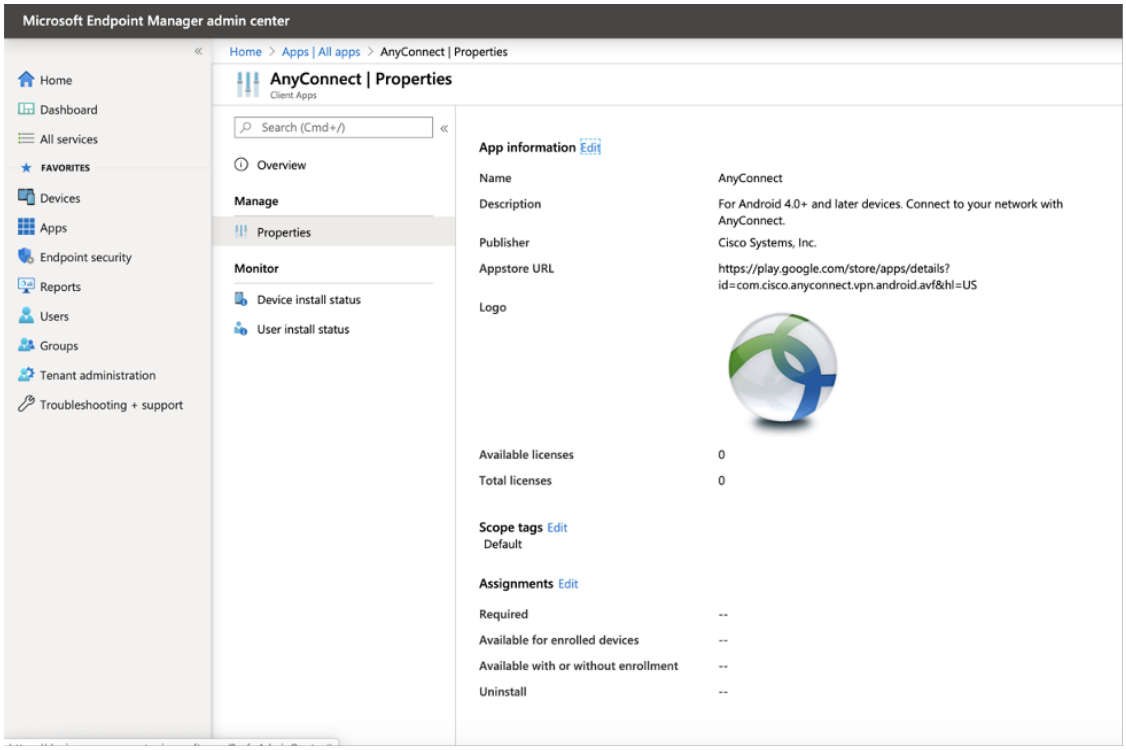




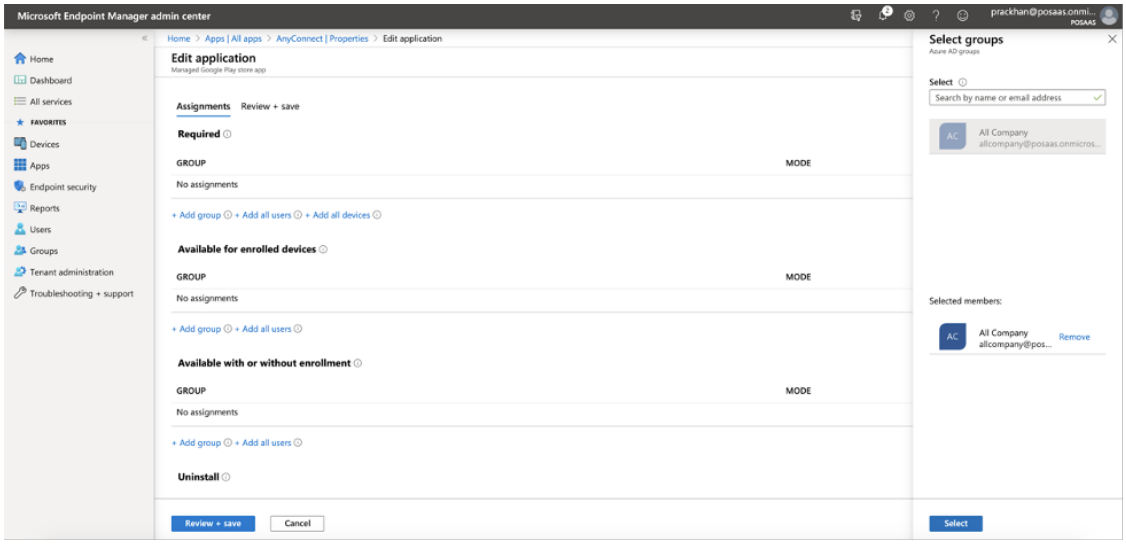
7. Click the newly created policy and assign it to the group to which you need to push the configuration.



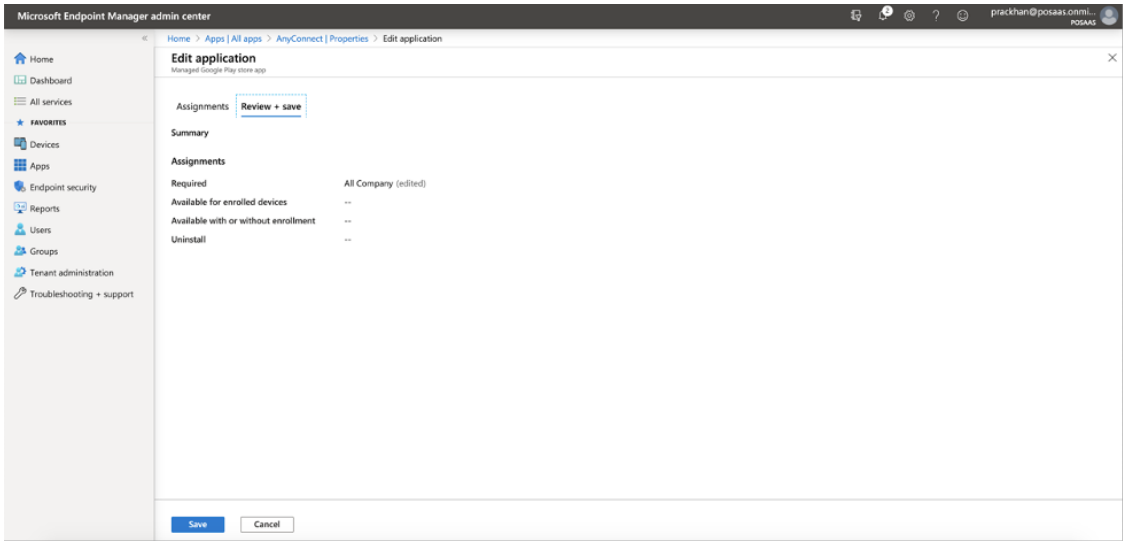
8. Navigate to **All Apps**, select **Cisco Secure Client – AnyConnect**, and then go to **Assignments**.



9. Click **Add Group**.
10. Set the **Assignment Type** to “Required”, select the groups to which the AnyConnect app is to be pushed and click **OK**.



11. To check the installation status for a user or device, navigate to **All Apps**, select **Cisco Secure Client - AnyConnect**, and then check **Device Install Status** and **User Install Status**.



Push User Identities

Describes Push User Identities in Cisco Secure Access. When user identities are pushed to Secure Access, you can identify and search users and devices.

When user identities are pushed to Secure Access, you can identify and search users and devices. For more information, see Manage Identities.

Push the Cisco Root Certificate

Describes Push the Cisco Root Certificate in Cisco Secure Access. For information, see Push the Cisco Root Certificate to Devices.

For information, see Push the Cisco Root Certificate to Devices.

Samsung Knox MDM

Describes Samsung Knox MDM in Cisco Secure Access and explains Register with the Enterprise Mobile Manager (EMM). It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

By downloading an XML file from Secure Access and then uploading it to your Knox system, Knox is able to push configuration information to both the Cisco Security Connector (CSC) and Secure Access so that your Android device is registered with Secure Access. The result is that your Android device is protected by Secure Access.

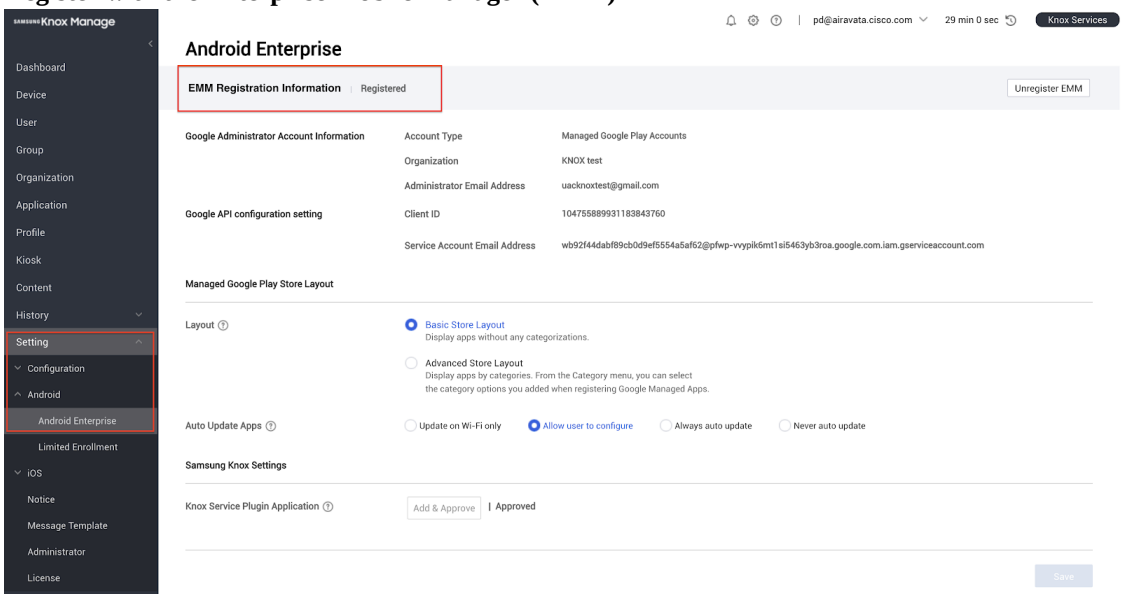
For information about configuring Knox, see Knox's documentation.

Note

Samsung Knox Details

For more information about using the Cisco Secure Access module with the Samsung Knox Mobile Device Manager, see Knox documentation, which is available online at the Samsung Knox support website.

Register with the Enterprise Mobile Manager (EMM)

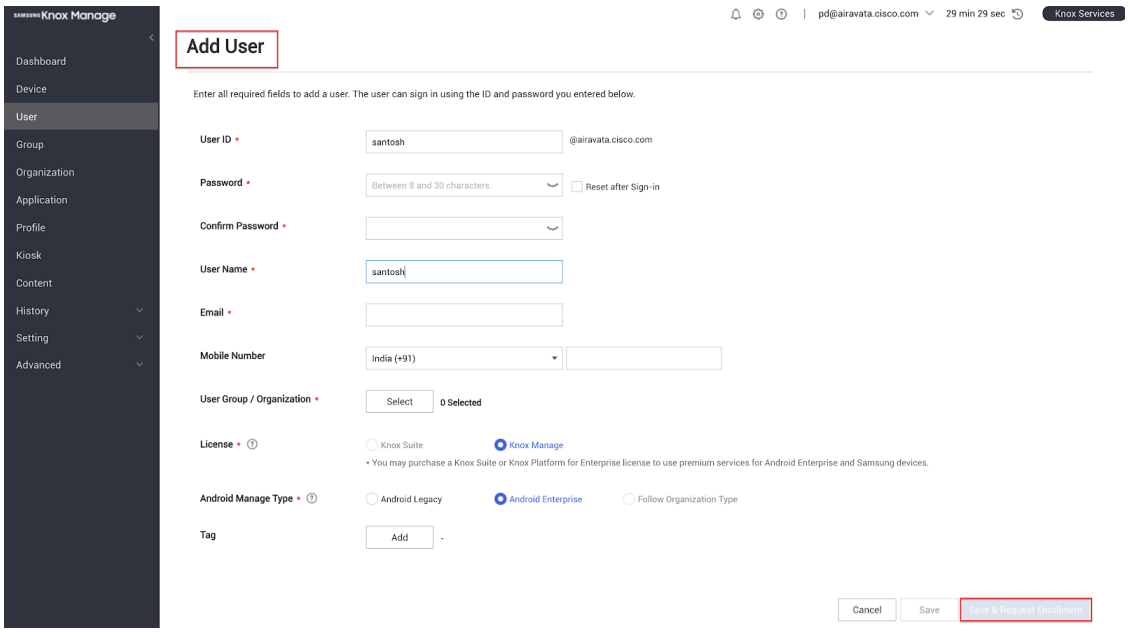


Enroll Android Devices

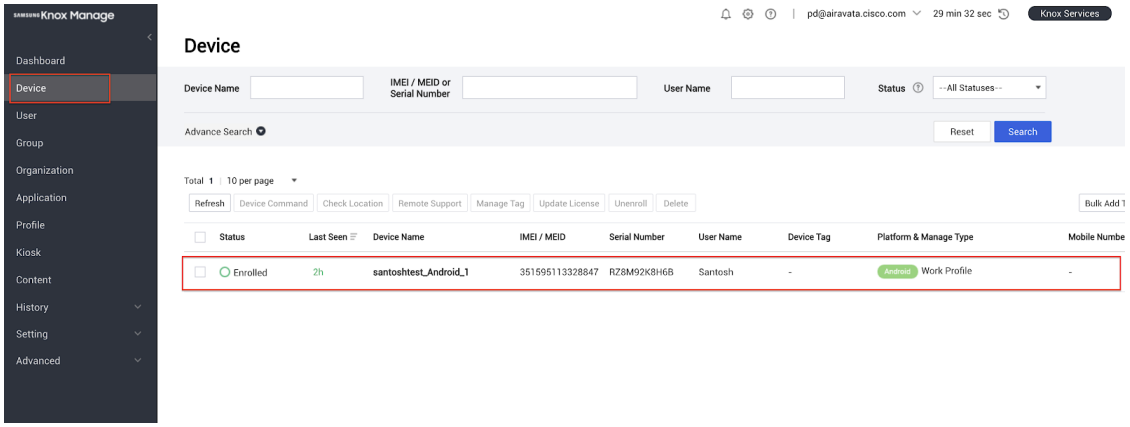
Provides instructions for completing the Enroll Android Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. In the Knox dashboard, navigate to Users.
2. Add necessary informatil,on and click **Save and Request Enrollment**.



3. Install Samsung Knox Manage from the Google Playstore and enroll the device if it is not already enrolled.
4. When the device is enrolled, follow the prompts to create the work profile mode.
5. Verify that the device appears in the Knox Manage Device list.

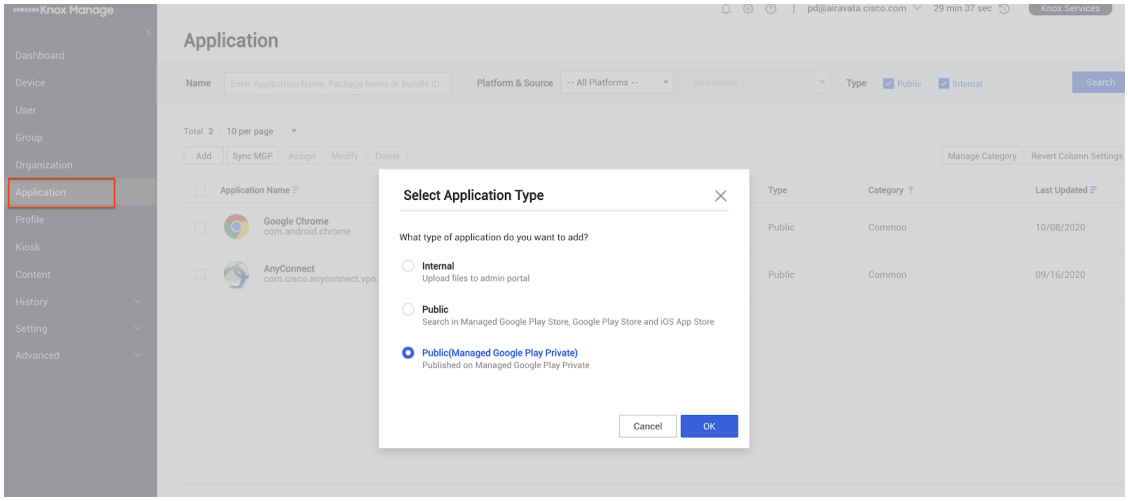


Push the App

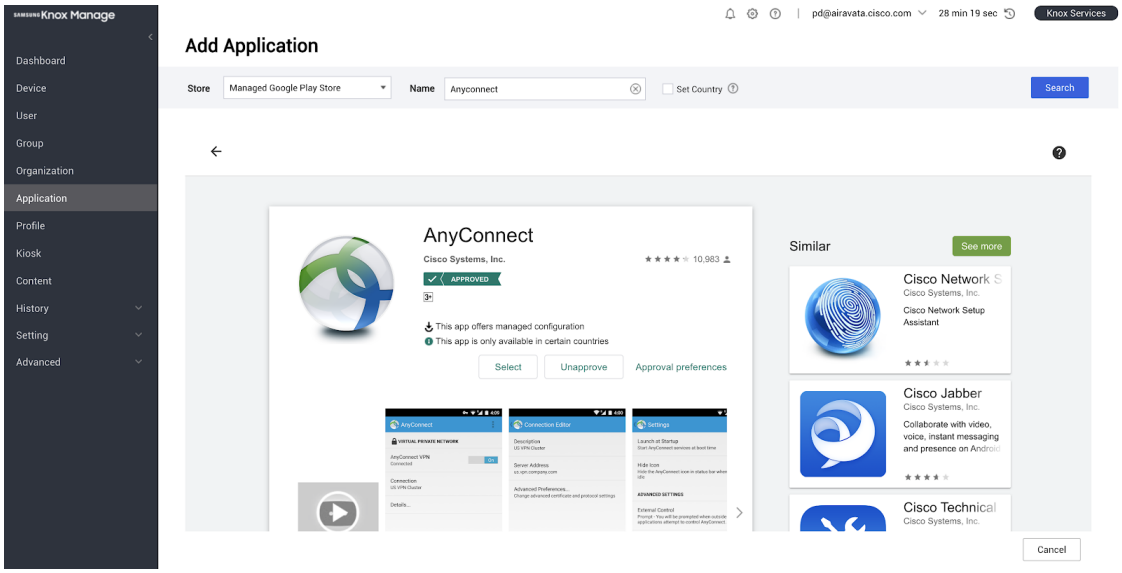
Provides instructions for completing the Push the App workflow in Cisco Secure Access. In the Knox dashboard, navigate to Application Add Select Application Type .

Procedure

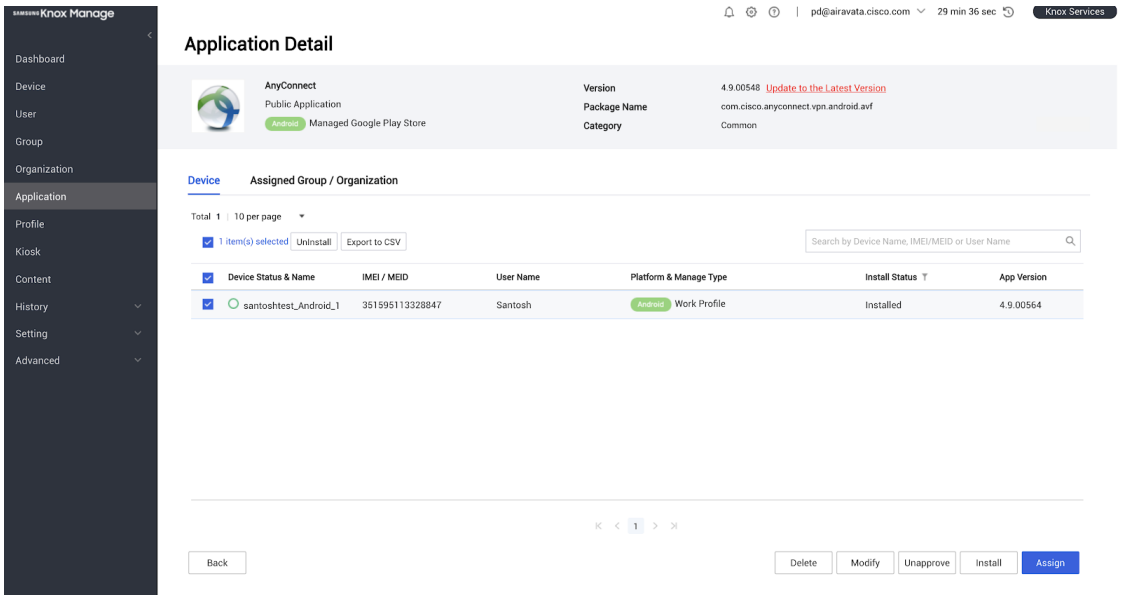
1. In the Knox dashboard, navigate to **Application** > **Add** > **Select Application Type**.



2. Select **Public**, search for **Cisco Secure Client - AnyConnect** in the Playstore and approve it.



3. Click **Assign**. This assigns the application to the device.

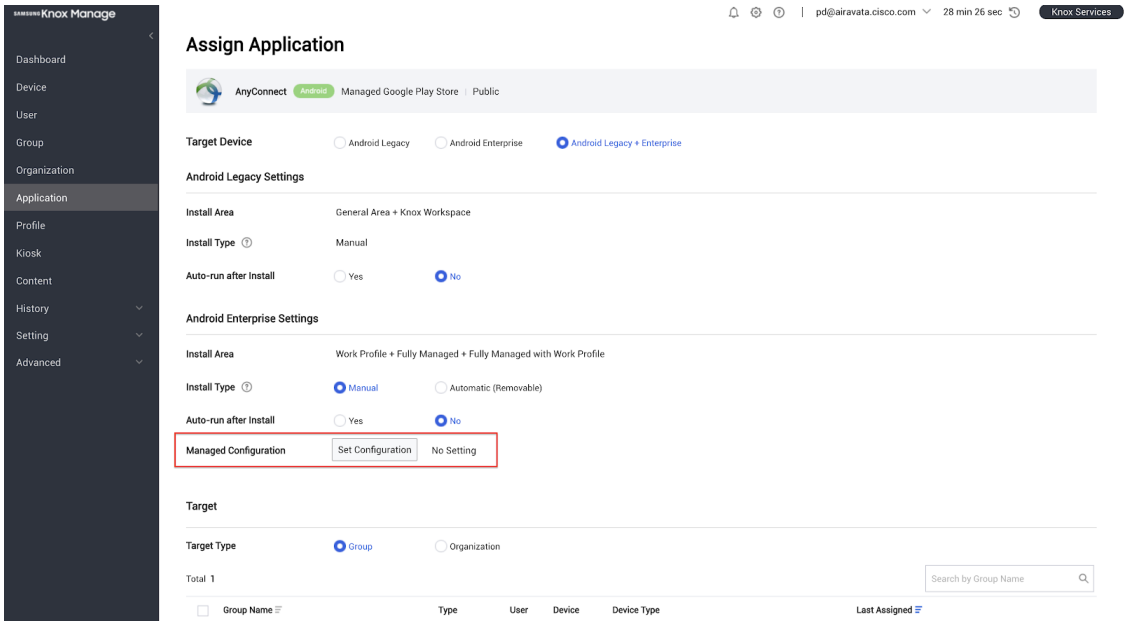


Set Managed Configuration

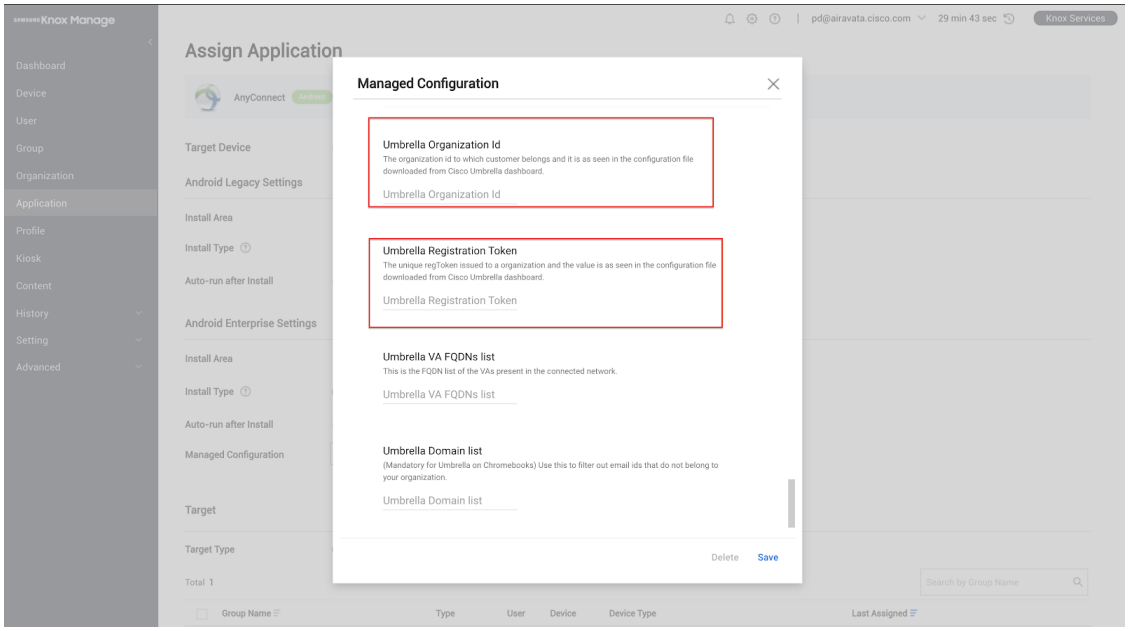
Provides instructions for completing the Set Managed Configuration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

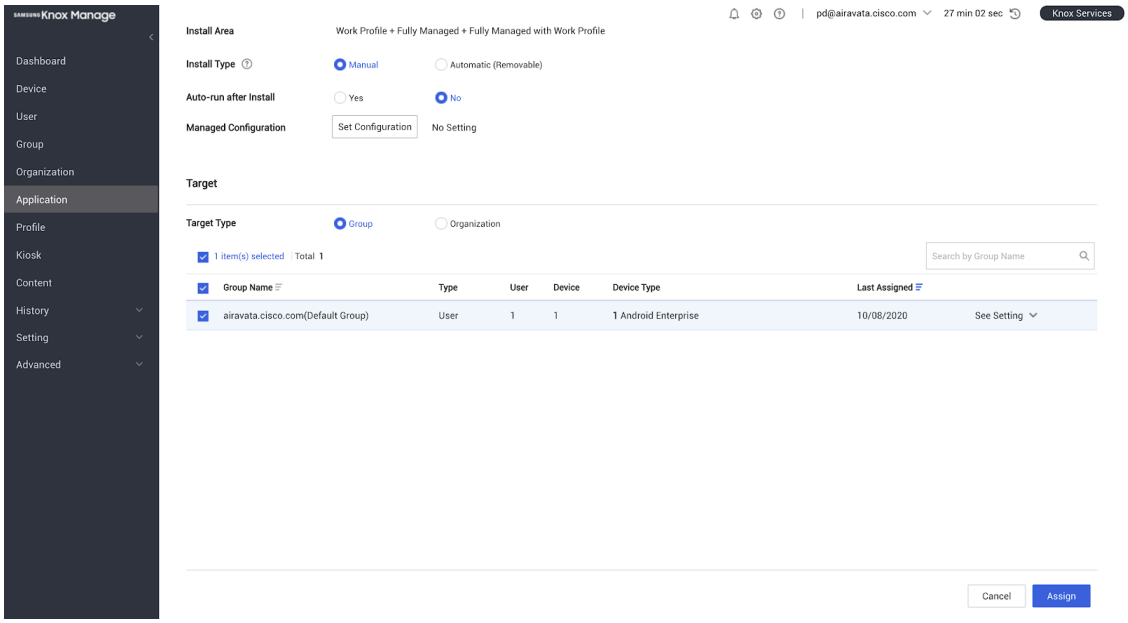
1. Set **Managed Configuration**.



2. Add the Secure Access organization and registration token.



3. Select the target group or organization and click **Assign**.

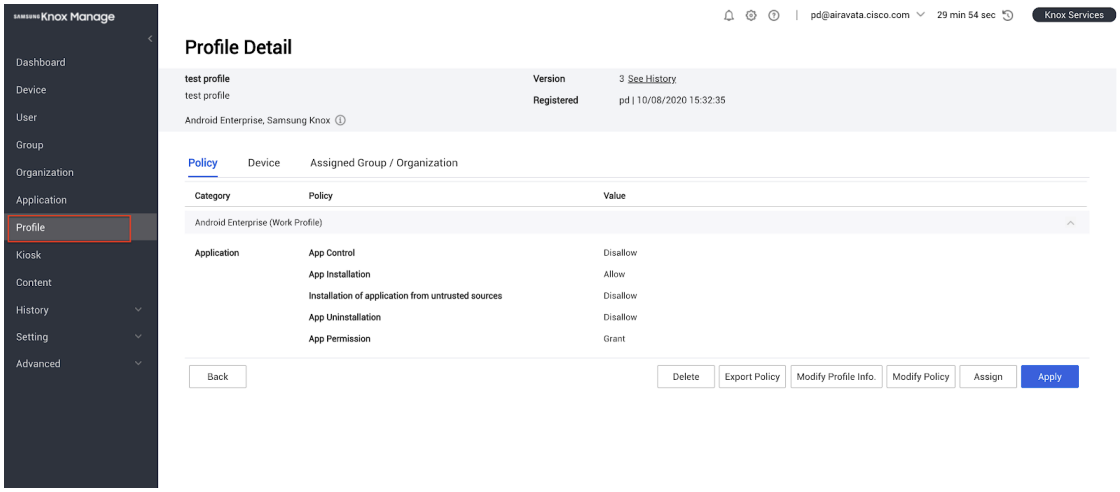


Create Profile in Knox Manage

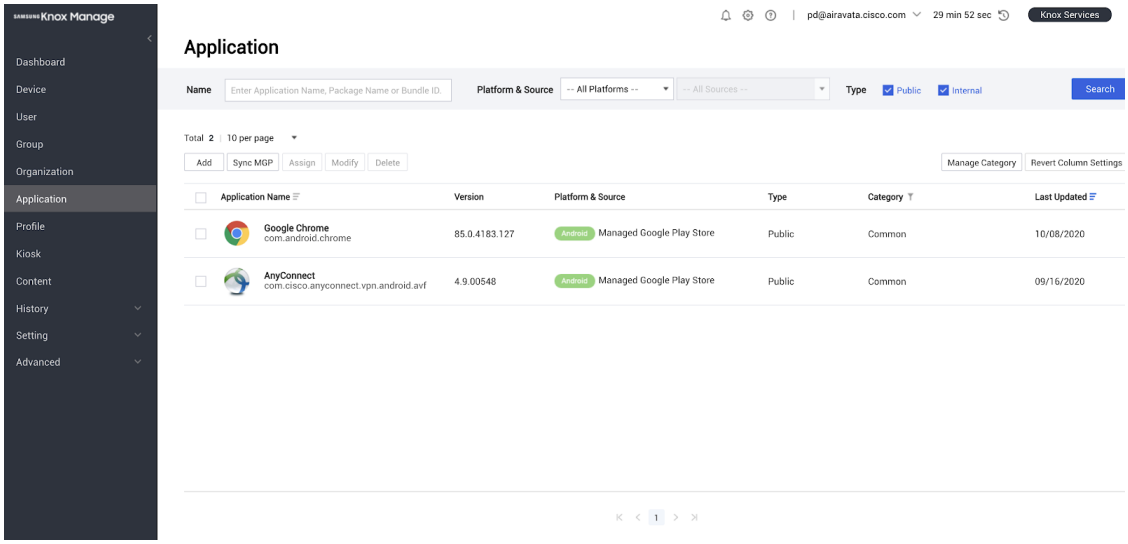
Provides instructions for completing the Create Profile in Knox Manage workflow in Cisco Secure Access. Navigate to Profile and apply application control settings.

Procedure

1. Navigate to **Profile** and apply application control settings.



2. Verify that the applications pushed to the device appear.



Push User Identities

Describes Push User Identities in Cisco Secure Access. When user identities are pushed to Secure Access, you can identify and search users and devices.

When user identities are pushed to Secure Access, you can identify and search users and devices. For more information, see Manage Identities.

Push the Cisco Root Certificate

Describes Push the Cisco Root Certificate in Cisco Secure Access. For information, see Push the Cisco Root Certificate to Devices.

For information, see Push the Cisco Root Certificate to Devices.

Push the Cisco Root Certificate to Devices

Describes Push the Cisco Root Certificate to Devices in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To support the display of block pages for HTTPS sites, HTTPS decryption if the Intelligent Proxy is used, and Trusted Network Detection if a VA is present you must push the Secure Access certificate to each of your managed devices.

Procedure

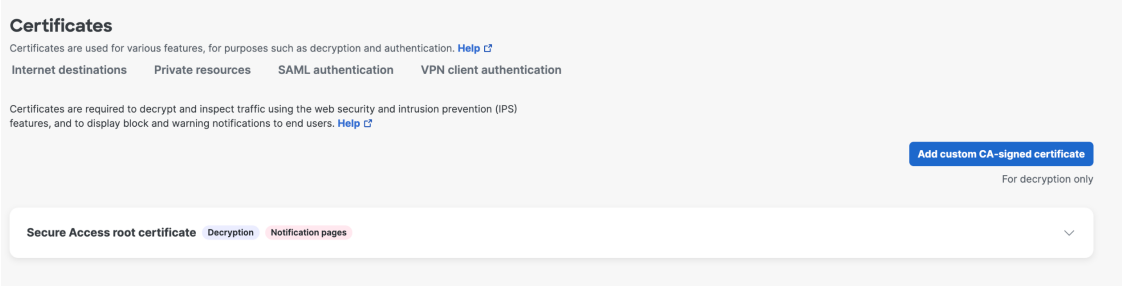
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full admin access to the Secure Access dashboard. See Manage Accounts.

Procedure

1. Navigate to **Secure** > **Settings** > **Certificate**.



2. Expand **Secure Access root certificate** and download the Cisco Secure Access root certificate.

   For more information about installing the root certificate, see Install the Cisco Secure Access Root Certificate.



3. Push the root certificate to all your devices from the MDM admin panel so that block pages can be displayed.

   This allows block pages for HTTPS sites to appear correctly, enables HTTPS decryption if the Intelligent Proxy is used, and enables Trusted Network Detection if a VA is present.

What to do next

Note

If there is an Secure Access VA in your network and you want to use Trusted Network Detection, configure the VA as detailed in Umbrella Virtual Appliance: Receiving user-IP mappings over a secure channel.

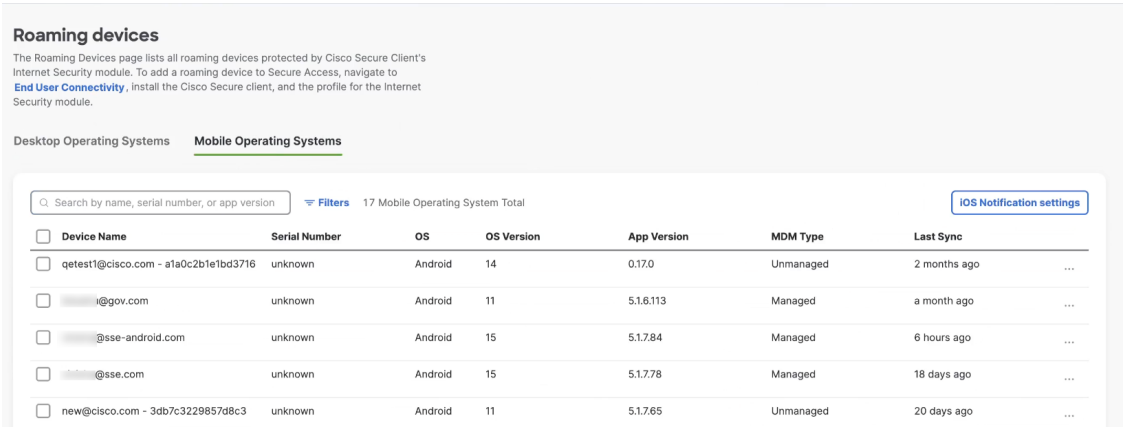
Manage Identities

Describes Manage Identities in Cisco Secure Access. To enable identity and be searchable in Secure Access, configure your Mobile Device Manager to share identity information.

To enable identity and be searchable in Secure Access, configure your Mobile Device Manager to share identity information. Identity can be any of the following based on what you choose to share with Secure Access:

- User email address
- Username
- Device serial number
- Any other unique device identifier

After you push the identities to Secure Access, they are listed in the Secure Access dashboard.

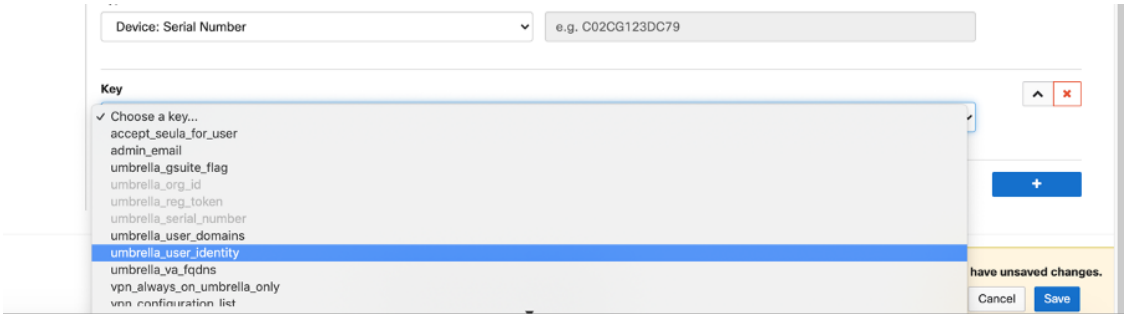


You can select user devices or use the user ID to search for them. To enable User Identities for Android clients, follow these steps.

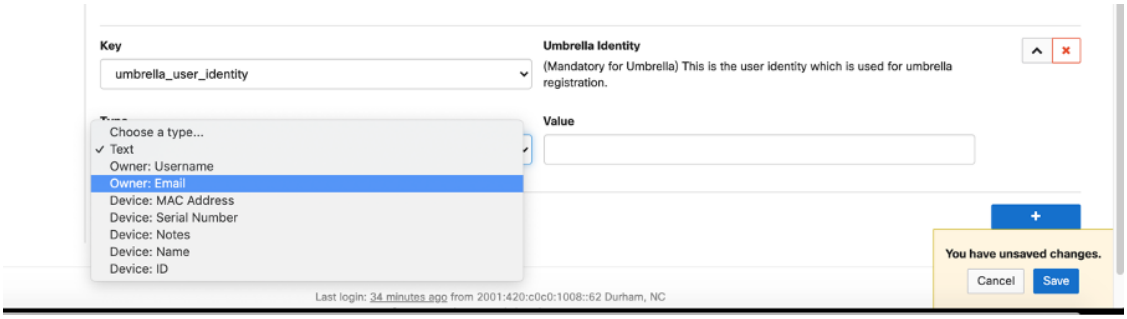
Cisco Meraki Systems Manager

Describes Cisco Meraki Systems Manager in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

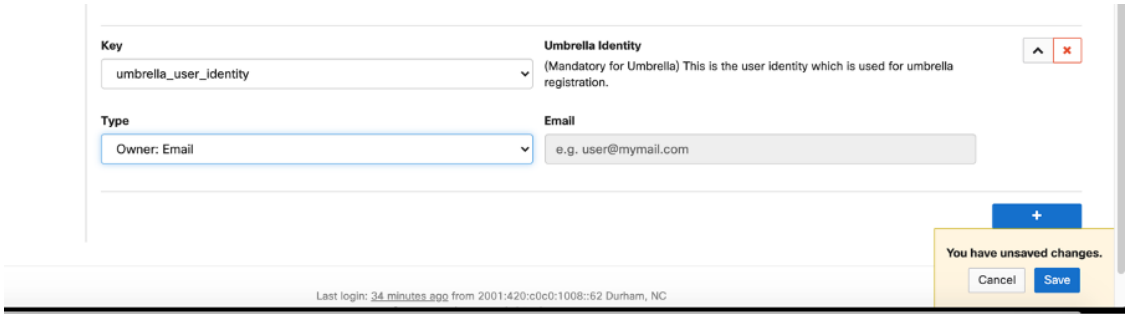
The key for User Identity in Meraki is umbrella_user_identity.



By default, the **Type** is a text field. Instead of choosing text, you can opt for the variables provided by Meraki SM. For setting up a user identity value, choose a type.



If a user identity is selected, the field looks as shown below:

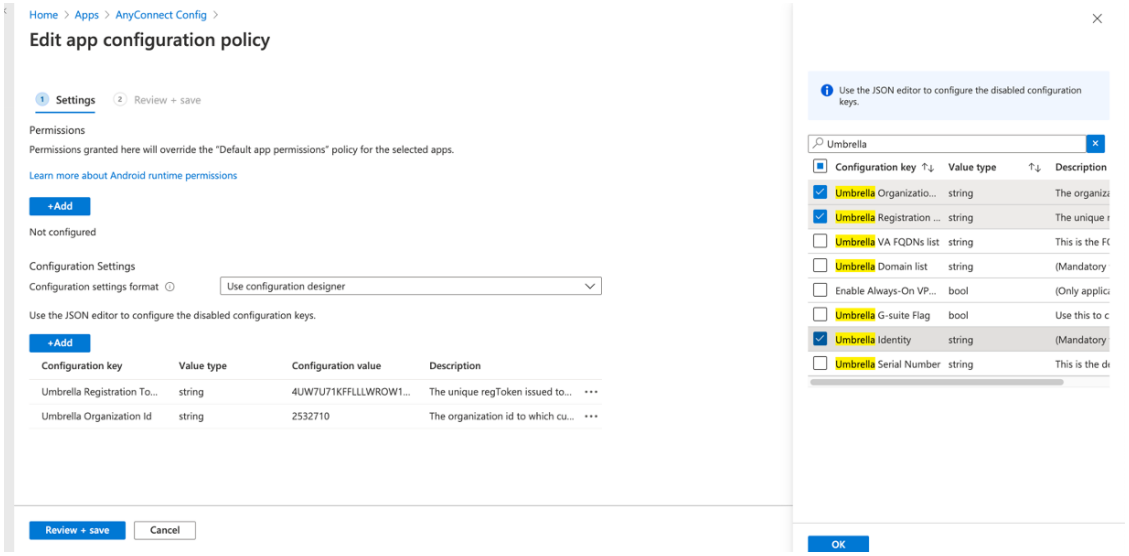


Once the configuration is pushed to the device, Meraki SM replaces the variable with the corresponding value.

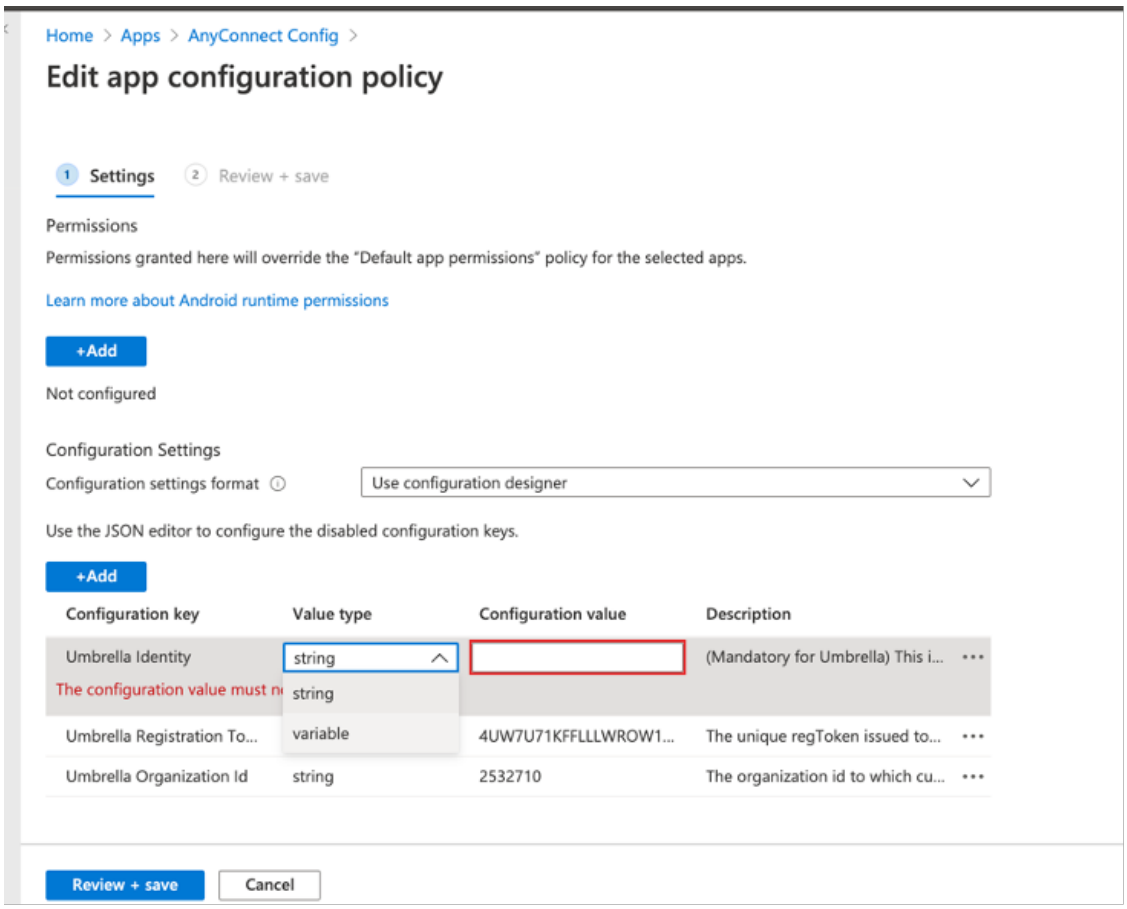
Microsoft Intune

Describes Microsoft Intune in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

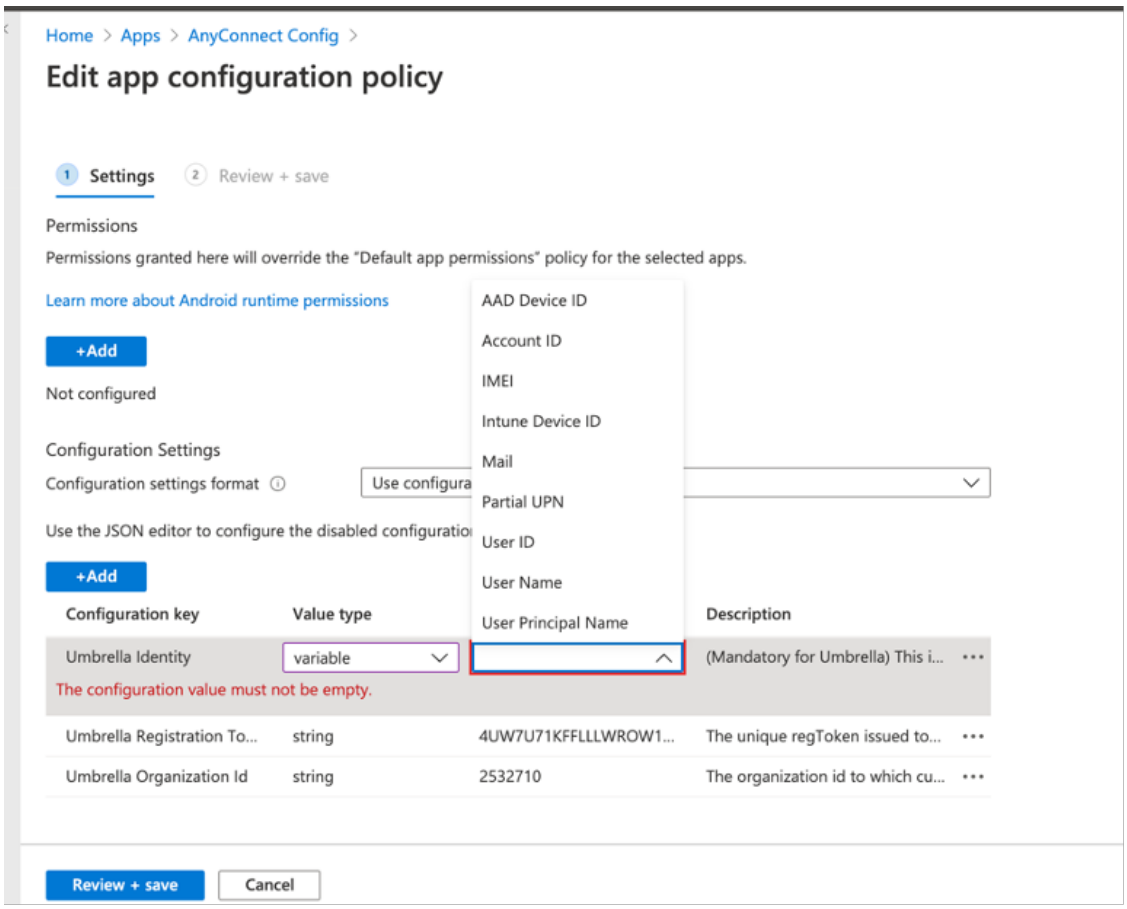
You can choose the key for user identity.



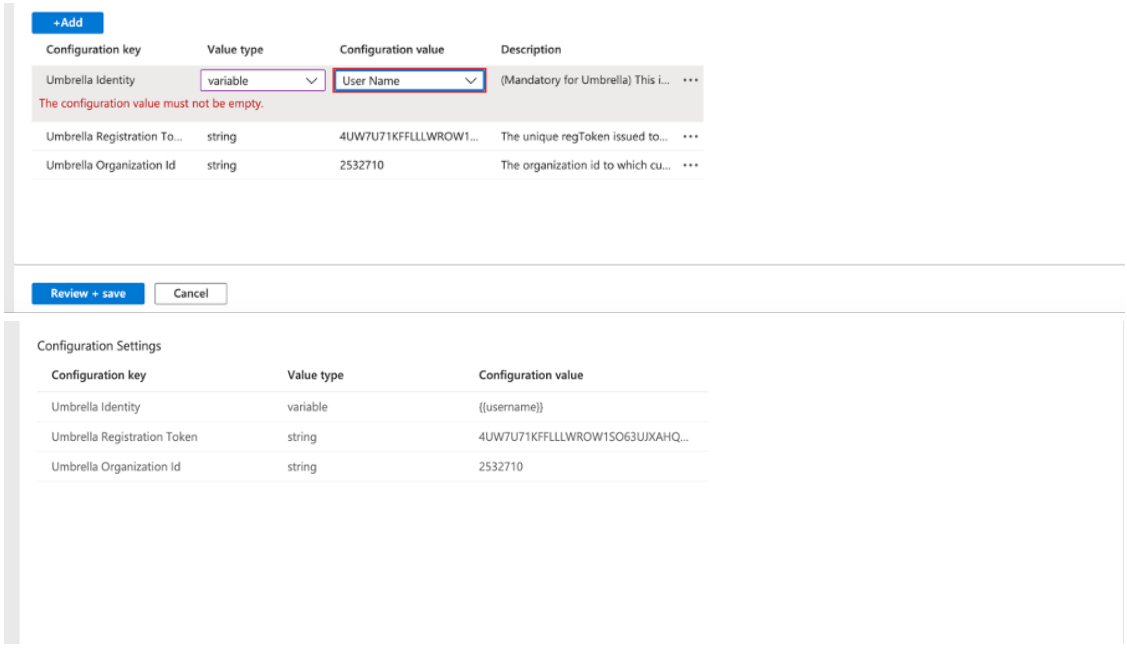
The **Value** type can either be a string or a variable.



Choose the value type as a variable so that configuration values can be selected from the options provided.



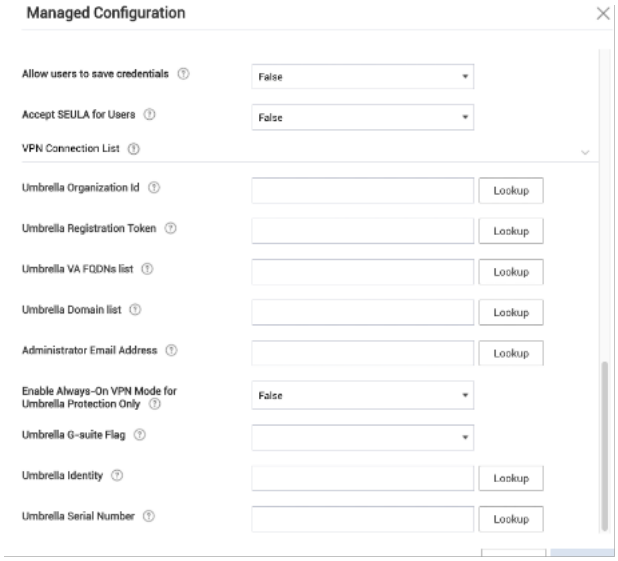
Choose any of the options from the list. Once the configuration is pushed to the device, MS Intune replaces the variable with the corresponding value.



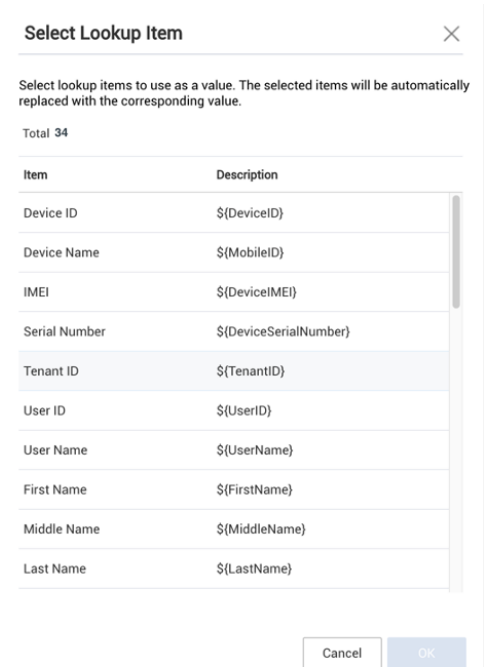
Samsung Knox

Describes Samsung Knox in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The key for user identity in Knox MDM is 'Umbrella Identity'.



Click **LookUp** for the **Select Lookup Item** and choose the appropriate variable for the identity.



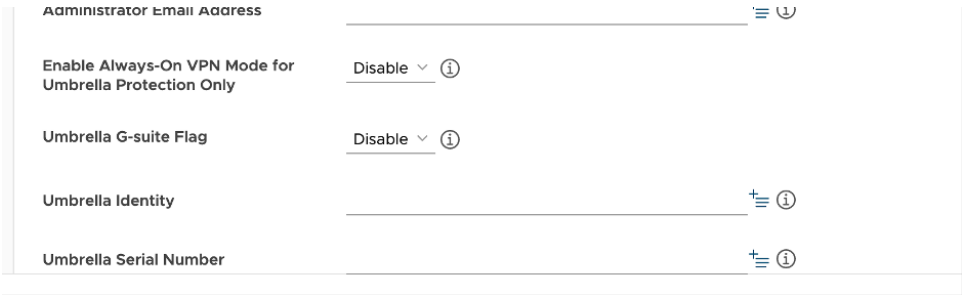
After you select the appropriate variable for the identity, the page appears.



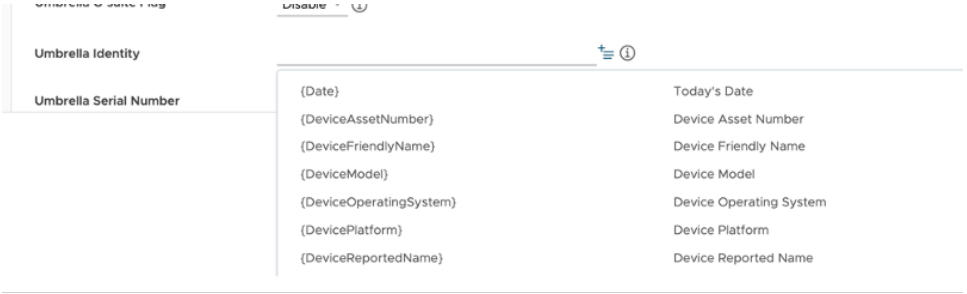
VMWare WorkspaceOne

Describes VMWare WorkspaceOne in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The key for user identity in VMWare WorkspaceOne is **Umbrella Identity**.



The **Value** can either be typed into the text box or you can be chosen from the **Select Lookup Item** tab. Click **LookUp** for the **Select Lookup Item**, and then choose the appropriate variable for the identity.



After you select the appropriate variable for the identity, the below screen appears.

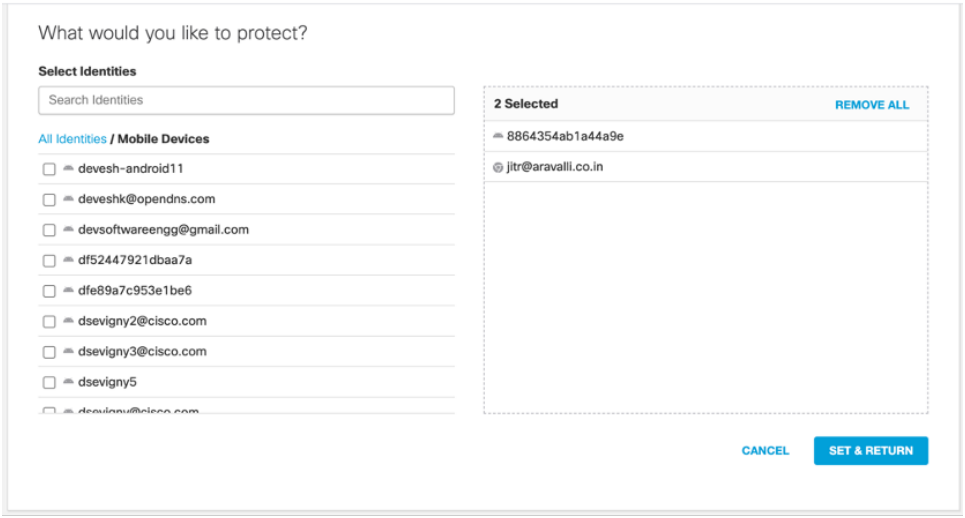


Access User Identities on the Secure Access Dashboard

Describes Access User Identities on the Secure Access Dashboard. After the user identity is shared with the Secure Access dashboard, you can select these identities in the policy configuration flow.

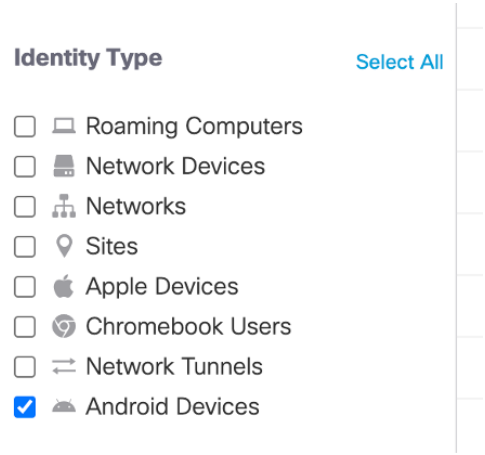
Configure Policy Based on User Identity

After the user identity is shared with the Secure Access dashboard, you can select these identities in the policy configuration flow. On the identity page, you can choose either a single identity or all the mobile devices.

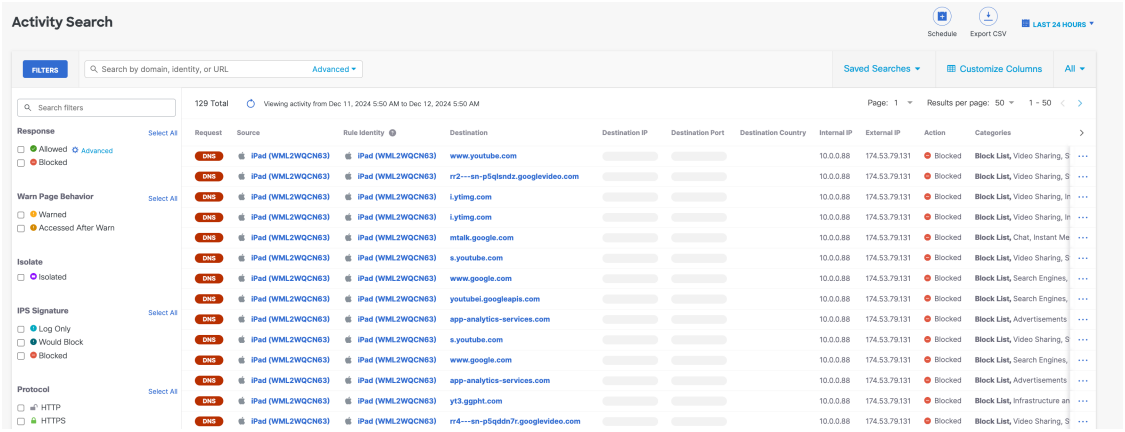


Monitor User Activity

As users start using the mobile device, you can monitor user activity through the Activity Search report. You can filter logs for the Android devices by selecting **Android Devices**.



You can see the user activity for the Allowed and Blocked.



Export Device Data to CSV

Describes Export Device Data to CSV in Cisco Secure Access. The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria.

The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria. Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

The exported CSV file contains the following information for each device:

- originId
- label
- serialNumber
- appliedBundle
- dnsProtectionStatus
- swgProtectionStatus
- lastDnsProtectionStatus
- lastSync
- version
- osVersion
- osVersionName
- type

Here the **dnsProtectionStatus** field displays the DNS protection status of respective devices. For information about the various DNS protection statuses, refer to the View DNS Protection Status topic.

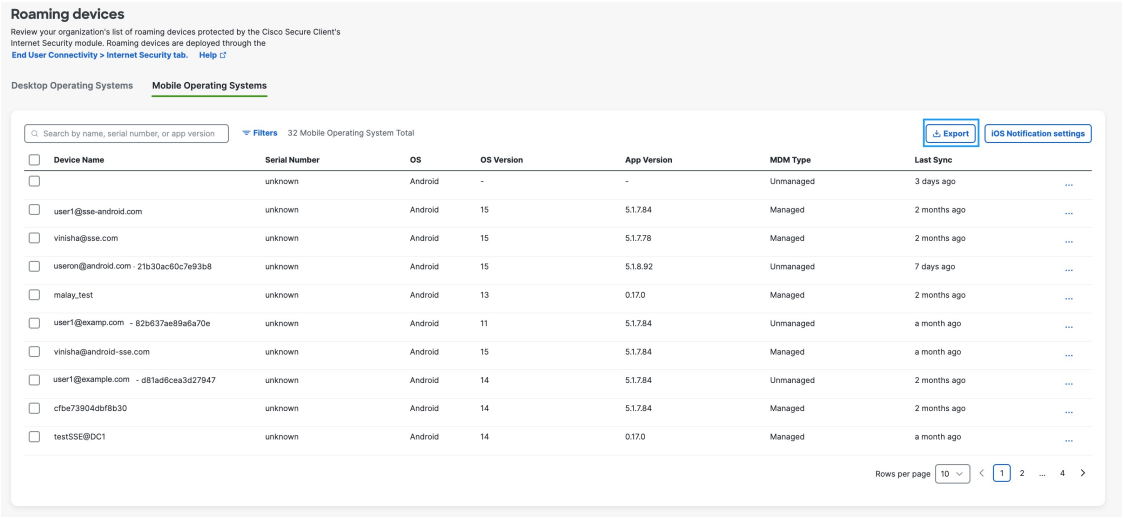
For information about the various SWG protection statuses, refer to the View SWG Protection Status topic.

Procedure

Provides instructions for exporting device data to a CSV It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Sources and destinations** > **Roaming Devices**.
2. For roaming devices running mobile operating systems, click **Mobile Operating Systems** or click **Desktop Operating Systems** for roaming devices running desktop operating systems.



3. Choose one of the following export options as per your requirement:
   - Export All Devices
     - Click **Export** at the top of the table to export all devices.
   - Export Selected Devices
     - Check the required number of devices and click **Export Selected** to export a specific number of devices.
   - Export Devices Based on Search Criteria
     - Search by name, serial number, or app version in the search bar. To further refine your search, click **Filter** and specify a search criteria to filter the devices accordingly.
     - Click **Export** to export all the devices meeting the search criteria. Check the required number of devices, and click **Export Selected** to export a specific number of devices that meet the search criteria.

What to do next

Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

DNS Protection Status in Exported Reports

Describes DNS Protection Status in Exported Reports in Cisco Secure Access. The dnsProtectionStatus column in Resources Roaming Devices exports uses these values.

The **dnsProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No DNS protection status is set or reported.	Not applicable
Open	The device is unprotected because Secure Access DNS resolvers are unreachable.	Unprotected (FailOpen)
Transparent	DNS protection is active and reporting, but DNS queries are not encrypted.	Protected

Status	Description	Related client state
Encrypted	DNS protection is active and DNS queries are encrypted.	Encrypted
VA	DNS protection is provided through a Virtual Appliance.	BehindVA
Network	DNS protection is provided at the network level.	BehindNetwork
Disabled	DNS protection is disabled by configuration or policy.	Disabled
Uninstalled	The Cisco Secure Client Secure Access module is uninstalled.	Not applicable
TrustedCustomerNetwork	DNS protection is disabled on a customer-defined trusted network.	Trusted customer network
CiscoTrustedNetwork	DNS protection is disabled on a Cisco trusted network.	Cisco trusted network
DisabledDueToACVpnFullTunnel	DNS protection is disabled while a full-tunnel VPN connection is active.	DisabledDueToACVpn
Off	The device has not synchronized within the timeout period. Its last status is stale.	Not applicable

Note

`Off` is not applied when the raw status is `Uninstalled` or `-`.

To know more about the DNS protection status of the Cisco Secure Client, see View DNS Protection Status

SWG Protection Status in Exported Reports

Describes SWG Protection Status in Exported Reports in Cisco Secure Access. The swgProtectionStatus column in Resources Roaming Devices exports uses these values.

The **swgProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No SWG protection status is set or reported.	Not applicable
Protected	SWG protection is active.	Protected
Unprotected	SWG protection is inactive.	Unprotected
Disabled	SWG protection is disabled by configuration or policy.	Disabled
DisabledDueToVPN	SWG protection is disabled while a VPN full-tunnel connection is active.	Disabled (VPN connection)

Status	Description	Related client state
DisabledDueToTrustedNetwork	SWG protection is disabled while the device is on a trusted network.	Disabled (trusted network)
ConfigError	SWG protection cannot be applied because of a configuration error.	Configuration Error
CloudServiceUnavailable	The SWG cloud service is unreachable from the device.	Cloud Service Unavailable
Offline	The device has not synchronized within the timeout period. Its last SWG status is stale.	Not applicable

To know more about the SWG protection status of the Cisco Secure Client, see View SWG Protection Status

Troubleshooting

Describes Troubleshooting in Cisco Secure Access. Check the scenarios below if you have difficulty validating the Secure Access module for Cisco Secure Client for Android OS after first installing it.

Check the scenarios below if you have difficulty validating the Secure Access module for Cisco Secure Client for Android OS after first installing it.

Known Issues

Describes Known Issues in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

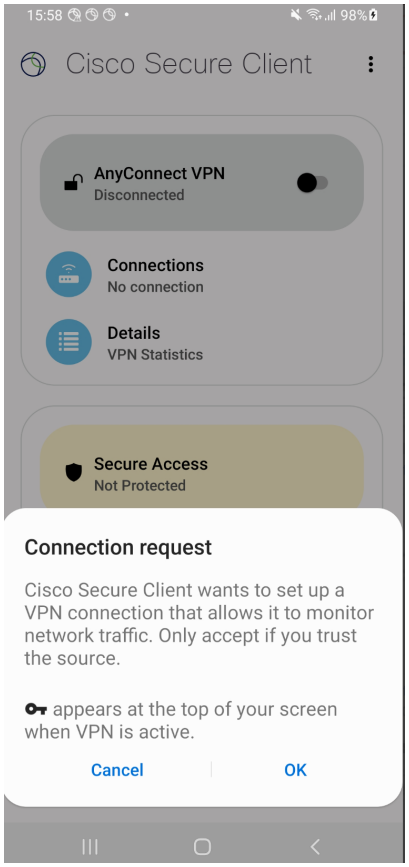
- App download fails in Google Play Store after enabling Cisco Secure client. This is a known limitation from Google on Android OS versions below v10. To avoid this, you must download Apps before enabling the Secure Access App. Google has fixed this behavior in their Android OS 10. Check the issue tracker.
- In Android 10 and later, Google restricts reading serial numbers from the device. As a result, the *Serial number* field in the Secure Access dashboard displays “unknown” for Android 10 and later devices.
- Avoid using the *Wifi Assistant*; it may conflict with Cisco Secure Client - AnyConnect and DNS interception.
- Private DNS must be turned off for DNS interception to function properly.
- Click for information about Unusual DNS queries showing in reports.
- Huawei phones, when running in Work Profile mode, do not automatically start Cisco Secure Client - AnyConnect, even when the app was previously open. This does not apply to Huawei phones in Fully Managed mode.

First Launch of App

Describes First Launch of App in Cisco Secure Access. On the first launch, there should be a request for Cisco Secure Client VPN session as shown below.

On the first launch, there should be a request for Cisco Secure Client VPN session as shown below. You must accept the connection request by clicking “OK” for the Secure Access protection to start.

> **Note**
>
> **Mandatory Security Step**: This cannot be bypassed; the behavior is built into Android OS for security reasons.

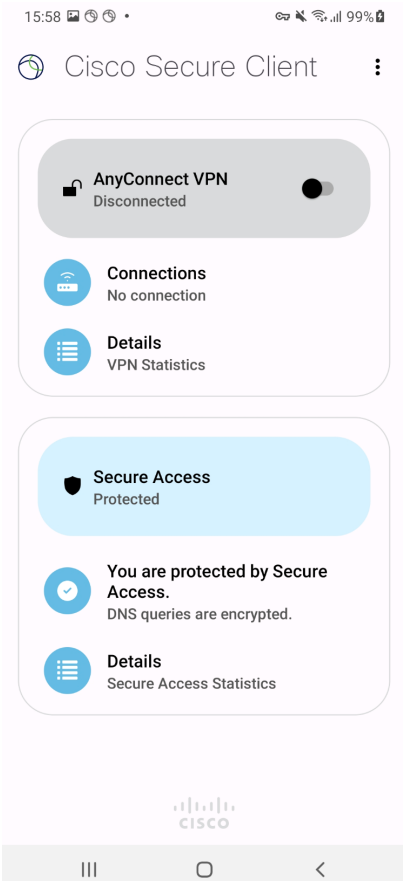


Is this a VPN to Secure Access?

Describes Is this a VPN to Secure Access. The Secure Access Module for Cisco Secure Client uses a VPN-like mechanism, but it is not in a traditional VPN.

The Secure Access Module for Cisco Secure Client uses a VPN-like mechanism, but it is not in a traditional VPN. This VPN-like mechanism is used to intercept DNS queries so that the module can process them (add metadata, encrypt and forward to Secure Access). The Android operating system's user interface does not show this distinction, so it appears as if a VPN were running.

When Secure Access protection starts, a green checkmark appears under the Secure Access UI subheading with the text “You are protected by Secure Access.”



Note

Virtual Appliance in the Network

If an Secure Access Virtual Appliance (VA) supporting HTTPS is configured in the network, the Secure Access module detects this and backs off. If a VA is not present, or is present but does not support HTTPS, then the Secure Access module remains active.

An Internal Site Isn't Loading

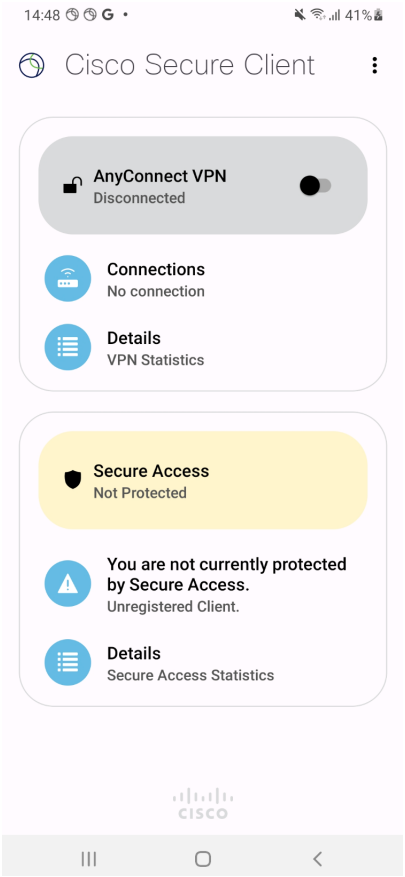
Describes An Internal Site Isn't Loading in Cisco Secure Access. The Secure Access module makes a best effort to automatically detect internal (intranet) sites and route DNS appropriately to the local DNS server.

The Secure Access module makes a best effort to automatically detect internal (intranet) sites and route DNS appropriately to the local DNS server. However, these mechanisms may not work in all scenarios. Therefore it's important to enter your internal / intranet domains in the Domain Management tools in the Secure Access dashboard. For more details, refer to Manage Domains.

Configuration Issues

Describes Configuration Issues in Cisco Secure Access. If the Secure Access Section in the Cisco Secure Client - AnyConnect app does not display a green checkmark, check the configuration details pushed from the MDM.

If the Secure Access Section in the Cisco Secure Client - AnyConnect app does not display a green checkmark, check the configuration details pushed from the MDM. If you don't have access, contact your administrator.



You can check if the configuration is available by clicking on the menu button at the top right in **Cisco Secure Client - AnyConnect** > **Diagnostics** > **Logging** and **System Information** > **System** > **Managed Configuration**.

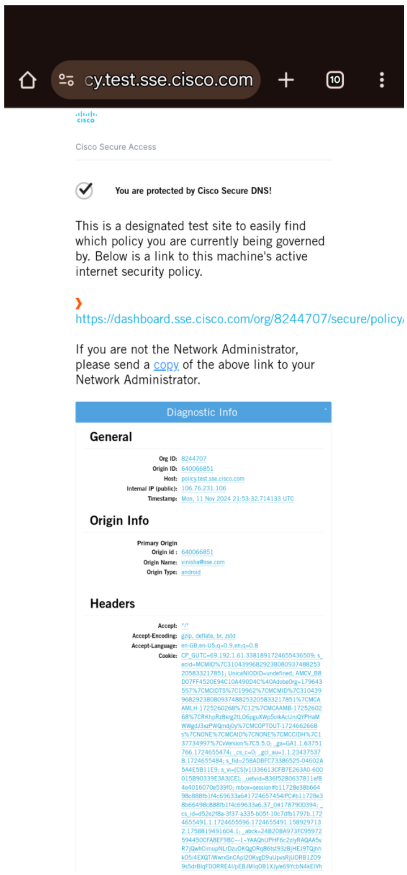
Verify that the managed configuration pushed by the administrator is available.

Check for VPN Connection and Policy

Provides instructions for completing the Check for VPN Connection and Policy workflow in Cisco Secure Access. Verify that the "key" icon (or something similar) is displayed in the notification panel for the VPN session created by Cisco Secure Client - AnyConnect.

Procedure

1. Verify that the "key" icon (or something similar) is displayed in the notification panel for the VPN session created by Cisco Secure Client - AnyConnect.
2. Open a browser.
3. Clear the cache.
4. Load `https://policy.test.sse.cisco.com/`. The page should load and display a URL to the active policy in the Secure Access dashboard. The format of the URL should be: `https://login.sse.cisco.com/o/<orgid>/#/configuration/policy/<policyid>`.
5. Verify that the organization ID displayed in the URL is the same as your Secure Access organization ID.



Check Block Page

Provides instructions for completing the Check Block Page workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Open `http://www.internetbadguys.com/`. You should see an Secure Access block page displaying the domain that was blocked along with the IP address of your device and the reasons for blocking. If you do not see the Secure Access block page, follow these steps:

Procedure

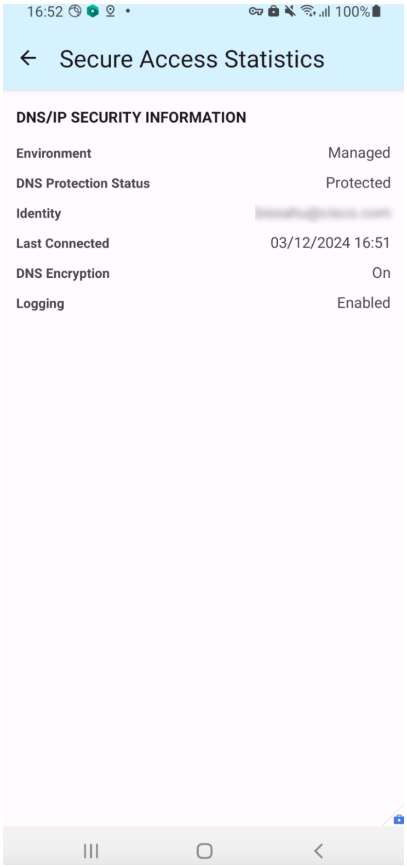
1. Select **Settings** > **Apps** > **Cisco Secure Client - AnyConnect** > **Force Close**.
2. Restart Cisco Secure Client - AnyConnect.
3. Reopen `http://www.internetbadguys.com/` and check for the Secure Access block page.

Get the Android ID

Provides instructions for completing the Get the Android ID workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

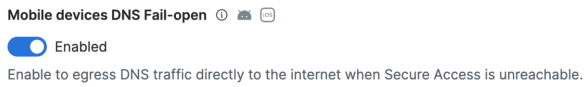
1. Launch Cisco Secure Client.
2. Open **Secure Access Security**.
3. Click **Options**, then open **Secure Access Statistics**. The Android ID is listed in that window.



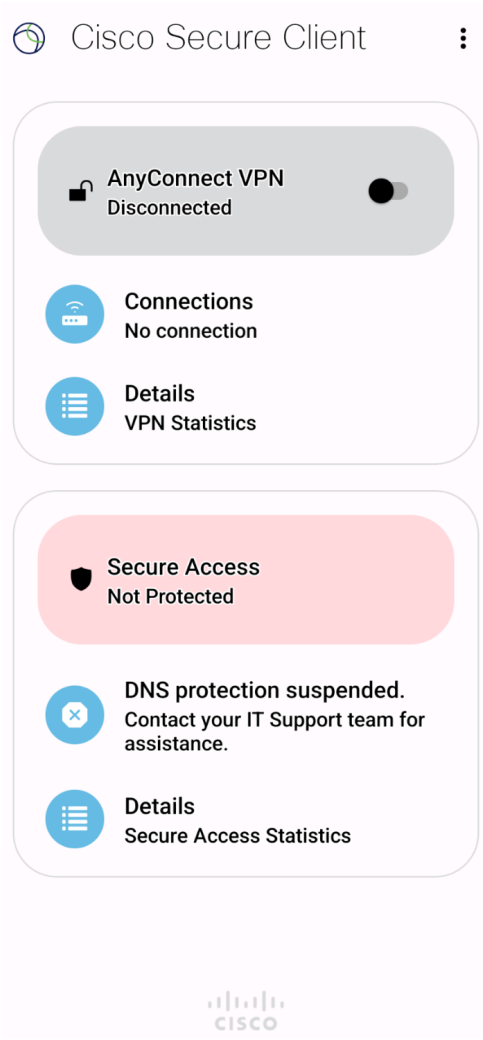
Fail Close/Open Scenario

Describes Fail Close/Open Scenario in Cisco Secure Access. Navigate to Cisco Secure Client settings Advanced , and enable the Mobile devices DNS Fail-open field to egress DNS traffic directly to the internet when Secure Access is unreachable.

Navigate to **Cisco Secure Client settings** > **Advanced**, and enable the **Mobile devices DNS Fail-open** field to egress DNS traffic directly to the internet when Secure Access is unreachable.



In case of internal errors, such as the Secure Access Resolver is not reachable or the DNSCrypt Certificate is not available, the Secure Access UI displays an error.



Check Device Registration

Provides instructions for completing the Check Device Registration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Find the `android_id` for your Android device.
2. Login to `https://login.sse.cisco.com/`,
3. Choose the `org id` associated with the device.
4. Navigate to **Resources** > **Roaming Devices** > **Mobile Operating Systems**.
5. Verify that the `android_id` is listed.

Missing CA Certificate

Provides instructions for completing the Missing CA Certificate workflow in Cisco Secure Access. If the Secure Access block page is not displayed but you see, instead, a warning about an insecure page, then there might be an error due to a missing Secure Access root certificate.

If the Secure Access block page is not displayed but you see, instead, a warning about an insecure page, then there might be an error due to a missing Secure Access root certificate.

Procedure

1. Download the Cisco Secure Access root certificate. **For more information about downloading the root certificate, Install the Cisco Secure Access Root Certificate**.
2. Secure the device with your PIN, password or pattern lock.
3. Install the certificate you downloaded.
4. Select the certificate file.
5. Reload the block page in your browser.

Org ID on Policy Page is 0

Describes Org ID on Policy Page is 0 in Cisco Secure Access. If the https://policy.test.sse.cisco.com/ URL shows 0 for the org id and bundle (policy) id, then refresh the page.

If the `https://policy.test.sse.cisco.com/` URL shows 0 for the org id and bundle (policy) id, then refresh the page. Alternatively, clear the browser cache, try an incognito window, or try a different browser.

App Installation is Blocked

Describes App Installation is Blocked in Cisco Secure Access. In order to download apps from the Google Play Store, a Gmail ID should be configured in the MDM.

In order to download apps from the Google Play Store, a Gmail ID should be configured in the MDM. If the ID is configured and the app still cannot be downloaded, the MDM admin may have chosen to disallow installation of apps from the Play Store.

Offboarding Users

Describes Offboarding Users in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

In order to fully remove an end user there are two steps:

- Delete the user from the Mobile Devices page in the Secure Access Dashboard.
- Delete the Cisco Secure Access Module for Android OS from the user's device. This can be done by the MDM. The MDM app itself need not be removed from the user's device.

Frequently Asked Questions about Managed Android

Describes Frequently Asked Questions about Managed Android in Cisco Secure Access. Does the Umbrella Android client (UAC) require an Cisco Secure Client - AnyConnect license?

Does the Umbrella Android client (UAC) require an Cisco Secure Client - AnyConnect license?

No. Only an active Secure Access subscription is required to use the Secure Access module on Cisco Secure Client - AnyConnect. No additional licenses are required.

Which MDMs are supported?

The client is MDM-agnostic and any MDM should be able to deploy it. However, we have validated the following MDMs in our lab: Cisco Meraki, MobileIron, VMware Workspace One and Microsoft Intune.

Which versions of Android OS are supported by the UAC?

UAC supports Android OS versions 6.0.1 and above.

Does the UAC client work on unmanaged Android devices?

No. The current Umbrella Android Client (UAC) works on managed (fully managed and work profile) Android devices only. However, support for unmanaged devices is planned for inclusion in future releases.

Does this client protect my entire Android mobile device?

For full details on device protection, refer to the Secure Access Android mobile security documentation.

Does this client support the Umbrella Secure Internet Gateway (SIG)?

No. The client supports DNS-layer security only.

Are there any differences between the UAC and the Endpoint Roaming Client (ERC)?

The feature differences between UAC and ERC are detailed below:

Feature	ERC	UAC
Supported Platforms	Windows, MacOS	Android
DNS-layer security blocks phishing and malicious domains	Yes	Yes
DNS logs augmented with endpoint IP information	Yes	Yes
EDNS message encryption between client and resolver	Yes	Yes
Customizable block page	Yes	Yes
User-based policies	Yes	Yes
Organization-wide policies	Yes	Yes
Safe Search	Yes	Yes
IP Blocking	Yes	No

Why does app download stop working as soon as the Secure Access protection is active?

A VPN connection is used to provide Secure Access protection on Android devices. After connecting to a VPN session one cannot download anything from the Google Play store. This is a known limitation in Android OS v9 and lower. To avoid this, download the apps *before* enabling VPN (i.e. Secure Access protection). This situation was corrected as of Android OS v10. Very few Android device manufacturers have included the update in their releases for Android versions older than v10. Refer to the Google issue tracker for more details.

Can I use a private DNS along with Secure Access protection?

No. Any private DNS must be turned off for DNS interception to work.

Can I use another VPN client along with the Cisco Secure Client - AnyConnect?

No. Due to Android OS limitations, two VPN sessions cannot run simultaneously. Cisco Secure Client - Anyconnect supports remote access VPN connections along with Secure Access DNS protection. As a best practice, Cisco recommends using Cisco Secure Client - AnyConnect for both Remote Access VPN and Secure Access protection needs.

Does UAC support IPv6?

Not in the current release. This feature planned for inclusion in future releases.

Does UAC support TCP DNS requests?

No. The current release supports only DNS on UDP.

How do I get the Android ID?

To obtain your Android ID, either:

- Launch the Cisco Secure Client - AnyConnect app, **or**
- In Secure Access Security, click Options. Then navigate to Secure Access Statistics to find the Android ID.

Why do I see multiple entries on the Secure Access dashboard for the same serial number?

Multiple entries for the same device appear in these circumstances:

- The user creates and deletes work profiles several times.
- The device is used by more than one user, each with their own login.
- The user tries to factory reset the device multiple times.

As an admin, how can I know whether users are using the app and the device is protected?

In the Secure Access dashboard, navigate to **Deployments > Core Identities > Mobile Devices**. Once there:

- Verify that the Android ID of the device is registered with Secure Access.
- Verify that the Android ID of the device is syncing regularly by checking for the last sync details.

Why am I able to browse blocked websites when the device says I am protected?

When the UAC is installed *within the work profile*, only the browser installed within the work profile is blocked from browsing blocked websites. When the UAC is installed in a *fully managed device*, and Secure Access protection is on, all the browsers on the device are blocked from such sites.

Can I use Secure Access Protection with the AnyConnect VPN?

Yes, Secure Access protection can be used when the remote VPN is on (that is, when the Cisco Secure Client - AnyConnect VPN is active).

How can I verify that Trusted Network Detection is working (Secure Access protection deactivates when a VA is detected in the network)?

Secure Access protection is deactivated when the UAC detects a VA in the network, unless the prerequisites are not met. For example:

- The VA and Android device belong to different Secure Access organizations.
- The VA is not configured to HTTPS event mode.
- The VA domain is not signed with a public certificate or the self-signed certificate has not been installed on the Android device.

For more information, see Android module prerequisites.

Does Secure Access RBI support mobile devices such as iOS and Android?

Remote Browser Isolation (RBI), which protects users by redirecting browsing to a cloud-based host, is not supported on mobile devices running iOS or Android.

66 Unmanaged Mobile Devices

Topics:

- Unmanaged Mobile Device Protection

Provides an overview of Unmanaged Mobile Devices in Cisco Secure Access, including Unmanaged Mobile Device Protection. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Unmanaged Mobile Device Protection

Describes Unmanaged Mobile Device Protection in Cisco Secure Access. Secure Access for unmanaged mobile devices is a solution targeted at devices that are not managed by a Mobile Device Manager (MDM).

Secure Access for unmanaged mobile devices is a solution targeted at devices that are not managed by a Mobile Device Manager (MDM). The solution can be deployed to any iOS or Android device that meets the minimum requirements.

As with any unmanaged solution, deployment of security coverage requires user action.

Administrator Actions

Describes Administrator Actions in Cisco Secure Access. An admin can deploy a mobile device that is not managed by a Mobile Device Management (MDM) system.

An admin can deploy a mobile device that is not managed by a Mobile Device Management (MDM) system. As a full administrator, you must provision authorized users by uploading the list of users from a comma-separated values (CSV) file or syncing the users from Active Directory (AD) using the AD Connector. Then, after you register a user in Secure Access, share the enrollment information with the user.

Enrolling Unmanaged Mobile Devices

Provides instructions for completing the Enrolling Unmanaged Mobile Devices workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Note

Be aware that:

- Only users in the authorized list are permitted to enroll.
- The enrollment is time-limited and the enrollment link expires at the date indicated.
- Once expired, a new enrollment data set must be supplied to continue enrollment.

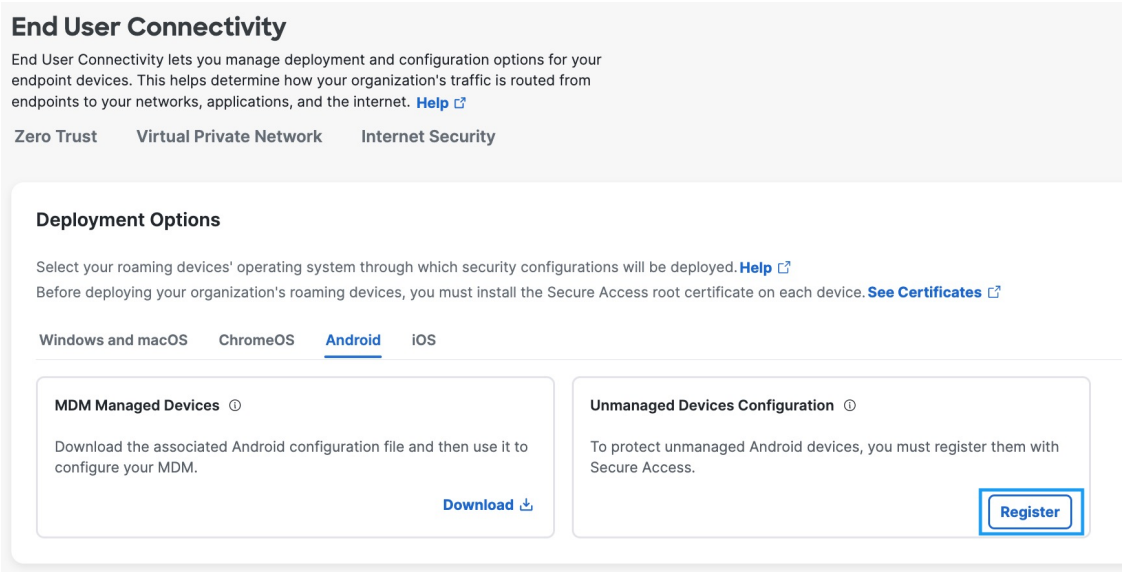
Before you begin

Ensure that you:

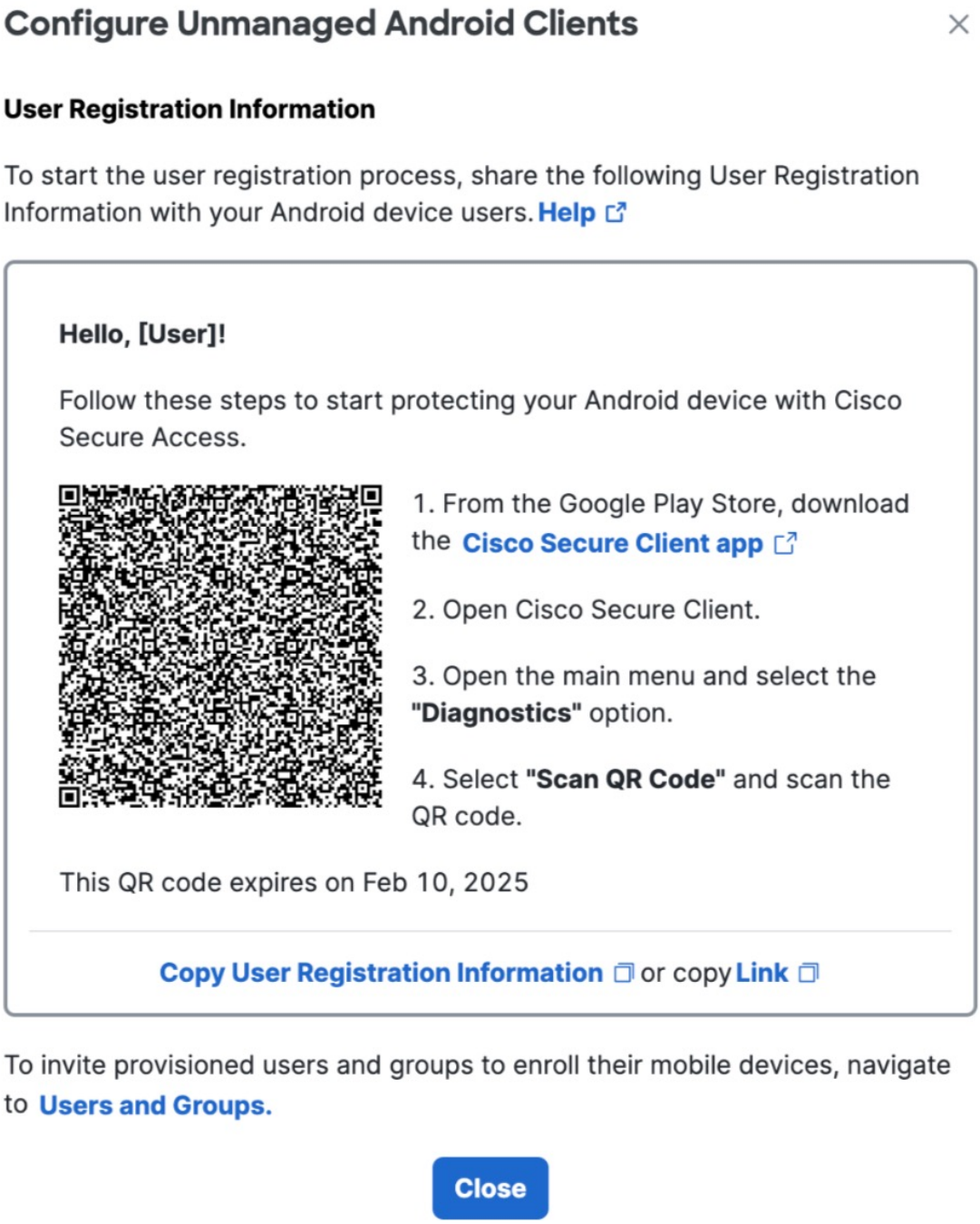
- Have full admin access to Secure Access. For more information, see Manage Accounts.
- Upload or sync authorized users to Secure Access:
  - Upload the list of users from a CSV file.
  - Integrate Active Directory (AD) users using the AD Connector.
- Have a Secure Access subscription that supports the deployment of mobile devices.

Procedure

1. Navigate to **Connect** > **End User Connectivity** and click **Internet Security**. Click the **Android** or **iOS** tab.



2. Under the **Unmanaged Devices Configuration** section, click **Register**.



3. In the **Configure Unmanaged Android Clients** window, click **Copy User Registration Information** to download the enrollment information.
4. Click **Link** to copy the enrollment link that will be used to enroll the Cisco Secure Client app on your mobile device.
5. Share the enrollment Information with the provisioned users.After at least one user is deployed, you can view any provisioned users in Secure Access. To enroll, an admin must share enrollment data with users directly.

End-user Actions

Describes End-user Actions in Cisco Secure Access. This topic walks you through how to register and enable Secure Access security on your mobile device when invited by a Secure Access administrator.

This topic walks you through how to register and enable Secure Access security on your mobile device when invited by a Secure Access administrator. Administrator enrollment is required to begin activation. Users that are not authorized to deploy Secure Access mobile are not permitted to configure the application.

Secure Access for unmanaged mobile devices can be deployed to any Android or iOS device that meets the minimum requirements.

Android

Describes Android in Cisco Secure Access and explains Prerequisites, Deployment, and Enrollment. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- Android 8.0 or higher version
- Valid invite to an authorized user from a Secure Access administrator
- Device with a camera or Firefox Browser installed
- Cisco Secure Client application installed

Deployment

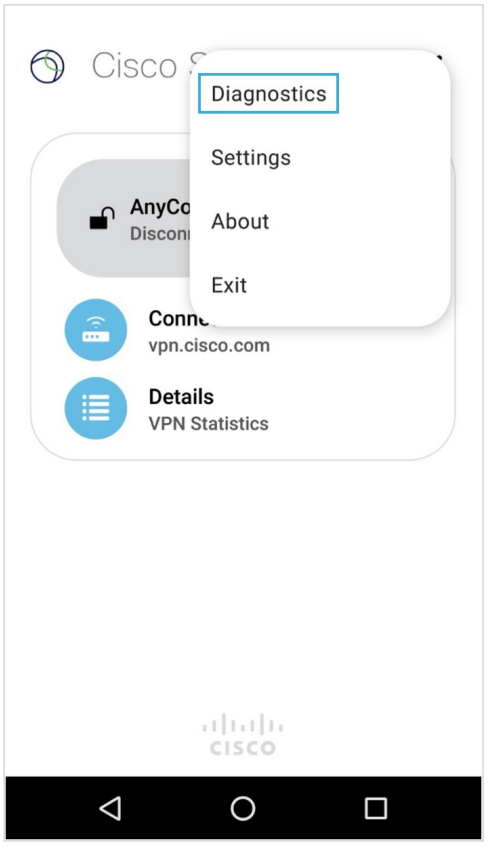
Download the Cisco Secure Client application from the Google Play Store.

Enrollment

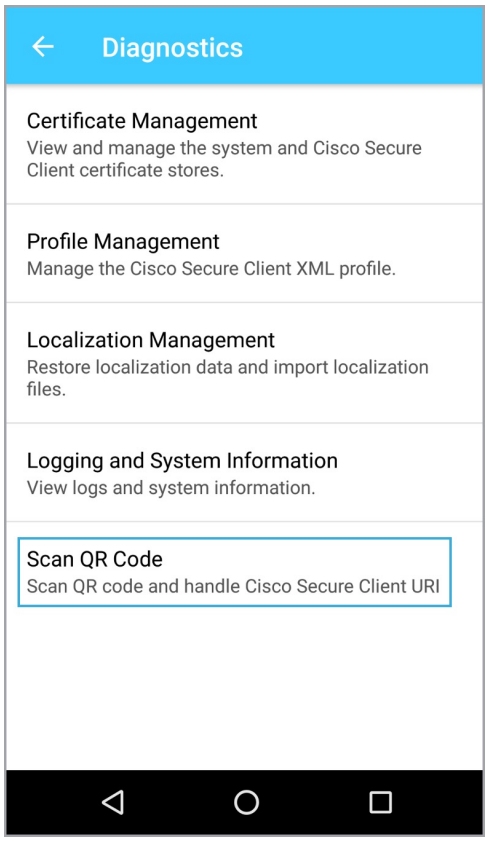
Enrollment is available in two ways: **QR code** (camera required) or manual enrollment **link**. Follow the steps of your desired enrollment method:

Enrollment by QR code

1. Open the Cisco Secure Client app and open the main menu.
2. Select **Diagnostics**.



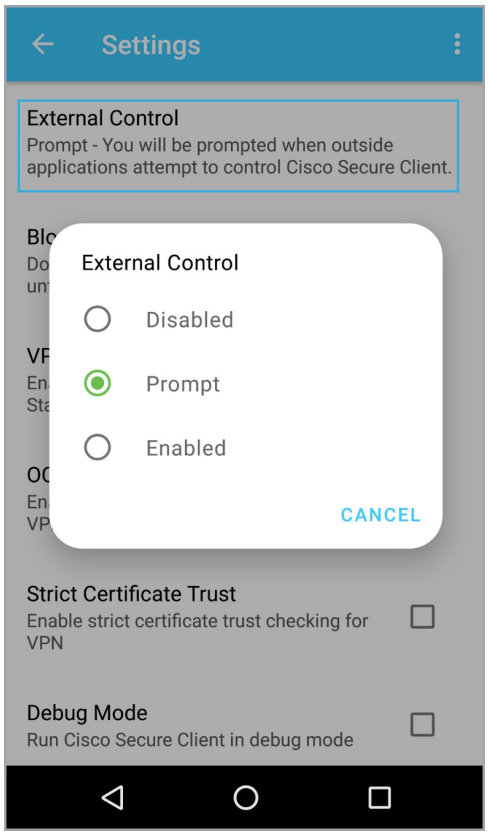
3. Select **Scan QR Code** and scan the QR code provided.



Continue to activation steps.

Enrollment without Camera Access

1. Open the Cisco Secure Client app and open the main menu.
2. Select **Settings**.
3. Select **External Control** and change the setting to **Prompt**.



4. Open the browser on your phone and paste the enrollment link into the address bar. You can obtain the enrollment link from the enrollment information shared by the Administrator.
5. Open the main menu and select the option for **Open in App**.

   Continue to activation steps.

Registration and Activation

Provides instructions for completing the Registration and Activation workflow in Cisco Secure Access. Enter your authorized email address to complete enrollment.

Procedure

1. Enter your authorized email address to complete enrollment.

   Note

   If the email provided is not authorized, the registration fails, and protection will not be prompted to activate. Please try again or contact your administrator.

2. Activate the prompted VPN connection to initialize DNS coverage.

A VPN connection is used locally to apply protection to your DNS queries. Allow the VPN Connection when prompted to complete activation of protection.

3. Visit welcome.umbrella.com to verify that your protection is active.

---

iOS

Describes iOS in Cisco Secure Access and explains Prerequisites, Deployment, and Enrollment via Link. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Prerequisites

- iOS 14 or higher version
- Valid invite to an authorized user from a Secure Access administrator
- Cisco Security Connector application installed

Deployment

Download the Cisco Security Connector application from the AppStore. Once installed, we recommend enrolling with the enrollment link. If a link is not provided, enrollment is also possible by scanning the QR code.

Enrollment via Link

1. Open the browser on your phone and paste the enrollment link shared by the Administrator.
2. When prompted, tap to open it with the Cisco Security Connector app. If you are not prompted and the link opens directly in Safari, please ensure the Cisco Security Connector app is installed.

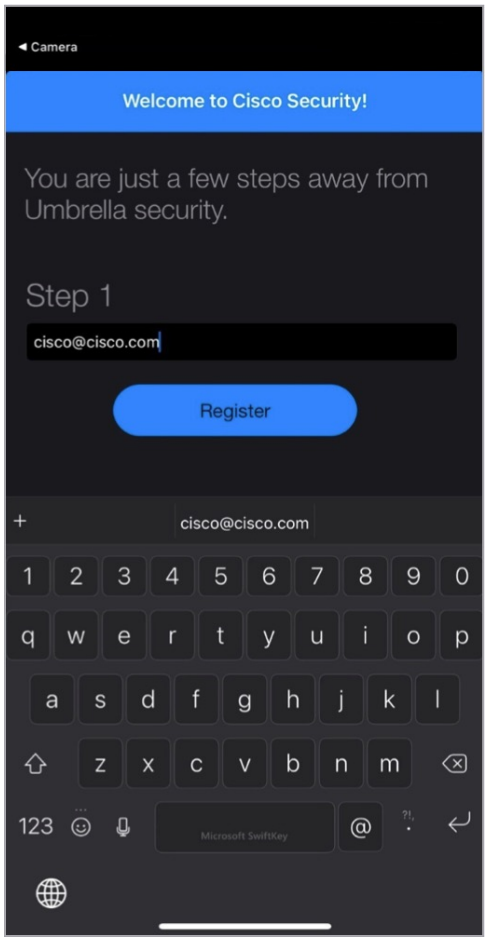
Enrollment by QR code

1. Scan the QR code provided.
2. Allow the link to be opened via the Cisco Security Connector.

Registration and Activation

Provides instructions for completing the Registration and Activation workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

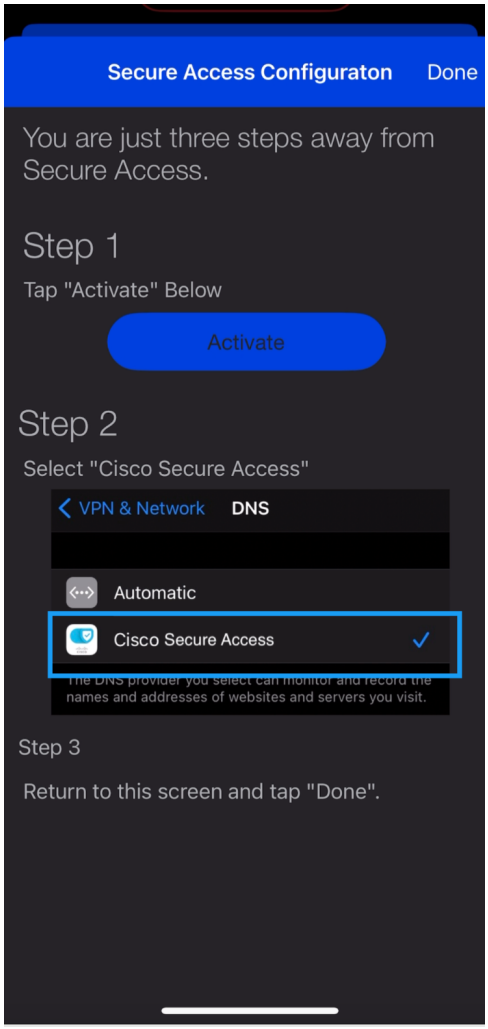
After tapping enrollment, a popup appears. In this text field, enter your email address. This must be the email address configured by your administrator.



Follow the on-screen instructions to enable DNS Security.

Procedure

1. Tap **Enable**.
2. Under the DNS option list, select **Cisco Secure Access**.



What to do next

If the direct settings link does not appear, the setting may also be reached manually with the steps below:

1. Navigate to **Settings**.
2. Tap **General**.
3. Tap **VPN and Device Management**. Once enabled, this will read **VPN, DNS, and Device Management**.
4. Under the DNS option, select **Umbrella**.

Return to the Cisco Security Connector app and visit welcome.umbrella.com to verify that your protection is active.

Part VI

Monitor and Report

Topics:

- Experience Insights
- Logging
- Monitor with Alert Rules
- Monitor with Reports
- Activity Reports
- Admin Audit Log Report
- AI Related Reports
- App Related Reports
- Cloud Malware Report
- Data Loss Prevention Report
- Data Security Posture Management Report
- Events Report
- Network Connectivity Monitoring
- Network Tunnel Group Usage Report
- Remote Access Log Report
- Top Categories Report
- Top Destinations Report
- Total Requests Report

Monitoring system health, user experience, and events, and creating reports.

67 Experience Insights

Topics:

- About Experience Insights
- Onboard Experience Insights
- Cisco AI Assistant for Experience Insights
- ThousandEyes Account Management in Experience Insights
- Experience Insights Overview
- Endpoints
- Wi-Fi Descriptions
- Experience Score
- View SaaS Application Performance
- View User Dashboard
- Configure Identity Providers for Experience Insights
- About Endpoint Agent Tests

Provides an overview of Experience Insights in Cisco Secure Access, including About Experience Insights, Onboard Experience Insights, and Cisco AI Assistant for Experience Insights. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

About Experience Insights

Describes About Experience Insights in Cisco Secure Access. Experience Insights enables you to monitor your end users' digital experiences when they access public, private, and collaboration applications.

Experience Insights enables you to monitor your end users' digital experiences when they access public, private, and collaboration applications. Examples include monitoring the memory usage and local network performance of endpoints and the network performance of your corporate resources. Having visibility into issues that can impact the employee experience is important as hybrid workforces move on and off the network and more apps and services exist in the cloud.

Experience Insights leverages digital experience monitoring (DEM) technology, which measures the real-time performance and availability of applications and services that IT operations teams can use to resolve issues quickly and improve employee productivity. The module is integrated with Cisco ThousandEyes, a SaaS product that measures network performance and delivers automated insights for digital experiences across the network.

Key insights and capabilities include:

- Real-time health, availability, and performance of endpoints.
- Hop-by-hop path of performance and service dependencies from the endpoint to Secure Access. The final hop to the application is viewable for organizations with a ThousandEyes Essentials or Advantage license.
- Endpoint topology map.
- User-specific client-based Zero Trust Access security events.
- Health of collaboration applications with digital-experience scores.
- End-to-end user identity mapping that correlates device-level performance data with OS-authenticated user identities, including first name, last name, and user group, to enable intuitive, user-centric troubleshooting.
- Historical data for identifying behavioral patterns to improve the end-user experience.
- Remote troubleshooting for end-user IT issues.
- Recommendations to help administrators remediate end user issues.

Key Terms

Term	Definition
Digital experience monitoring (DEM)	A technology that monitors the availability, performance and quality of an end user or digital agent experiences when using a device or application.
Secure Access	A Cisco software product that enhances troubleshooting capabilities and proactively monitors users' connectivity experience to their applications.
Experience Insights	Cisco's offering for Digital Experience Monitoring in Secure Access.
ThousandEyes	Cisco's network intelligence SaaS platform that provides you with real-time visibility into Internet-enabled applications and networks. To learn more, see ThousandEyes Documentation.

Onboard Experience Insights

Provides instructions for completing the Onboard Experience Insights workflow in Cisco Secure Access. An active Cisco ThousandEyes account with the Organization Admin role.

Use the Experience Insights onboarding wizard to connect Secure Access to your Cisco ThousandEyes account for end user experience monitoring of endpoint, application, and network performance.

Before you begin

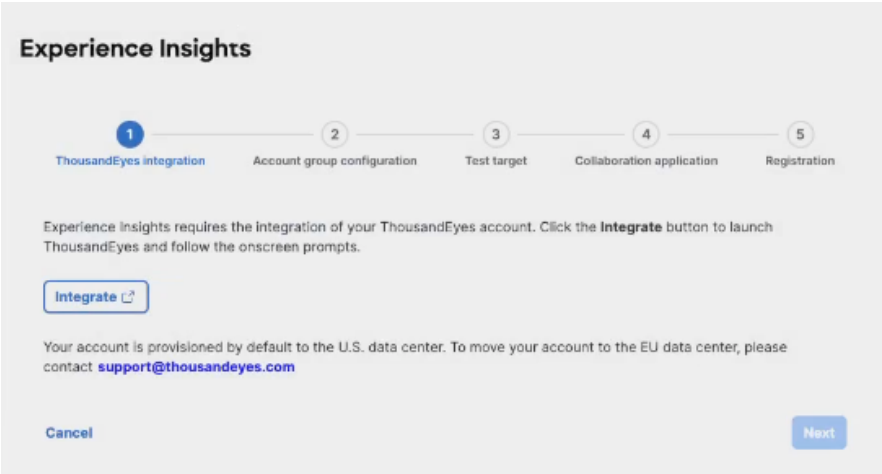
- An active Cisco ThousandEyes account with the Organization Admin role. For more information, see Role-Based Access Control and Built-in Roles and Permissions in ThousandEyes documentation.
  - The administrator who received email notification of Secure Access activation will also receive email notification of ThousandEyes activation. Follow ThousandEyes provisioning instructions within 72 hours of receiving the activation email. If the activation email is expired, visit the ThousandEyes login page and click **Forgot password?**
- The ThousandEyes login account group is correct for integration with Experience Insights.
  - The Login Account Group determines ThousandEyes test and agent visibility to Secure Access Experience Insights. For more information, see What is an Account Group? in ThousandEyes documentation.
  - The ThousandEyes User Profile for the integration account must have a Login Account Group intended for integration with Secure Access. For more information, see Role-Based Access Control: Login Account Group and Role-Based Access Control: Account Groups Screen in ThousandEyes documentation.
- Cisco Secure Client must be installed on your endpoints. The ThousandEyes endpoint agent is included in the installation.
  - For information about installation, see Download Cisco Secure Client.
  - For information about installing Secure Client on multiple endpoints, see Mass Deployment Overview.
- If you intend to use RAVPN as the target for the synthetic network default test, it must be configured.
  - For instructions, see Manage Virtual Private Networks.

Procedure

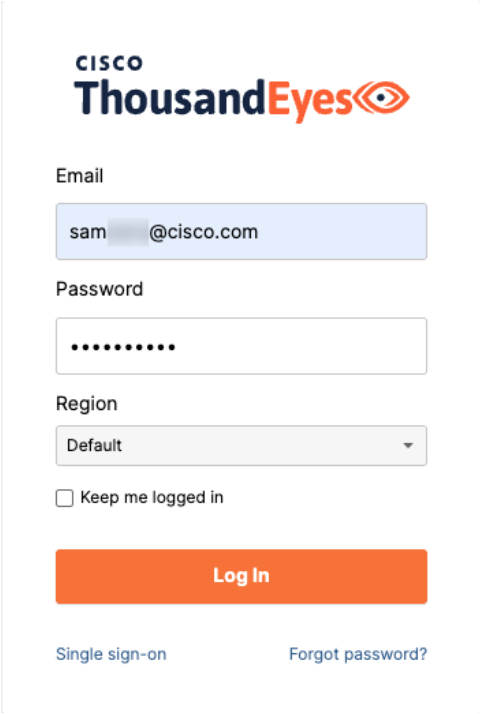
Step 1: ThousandEyes integration

Experience Insights requires the integration of your ThousandEyes account.

1. Navigate to **Experience Insights** > **Insights Management** > **Management**, then click **Begin onboarding**.
2. Click the **Integrate** button to launch ThousandEyes.



3. Log into ThousandEyes using an account with the Organization Admin role.



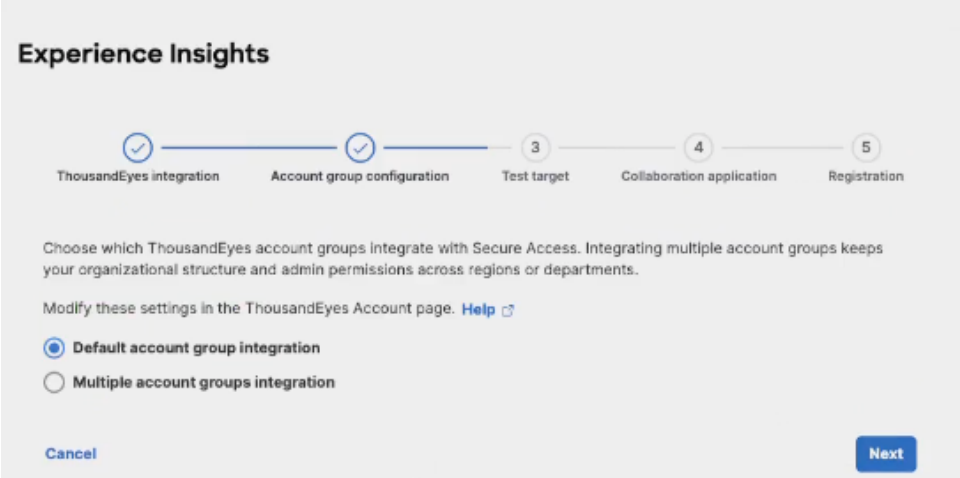
4. Confirm that you authorize the following Secure Access permissions in ThousandEyes:
   a) **Read organization** - Allows the reading of the organization credentials, account groups, users, user events, roles, permissions, usage and quotas.
   b) **Manage endpoint agents** - Allows the end user to manage their endpoint agents.
   c) **Manage endpoint tests** - Allows the end user to manage their endpoint tests.
   d) **Manage tags** - Allows the end user to manage their tags and labels.
   e) **Read tests** - Allows the end user to read their tests and the respective results.

> **Note**
>
> **OAuth 2.0 with ThousandEyes**
>
> ThousandEyes uses the OAuth 2.0 protocol to grant Secure Access limited access to your ThousandEyes data. For more information, see OAuth 2.0 with ThousandEyes.

5. After confirming, wait for the Experience Insights onboarding wizard to reload and display the `Integration successful` message, then click **Next**.

Step 2: Account group configuration

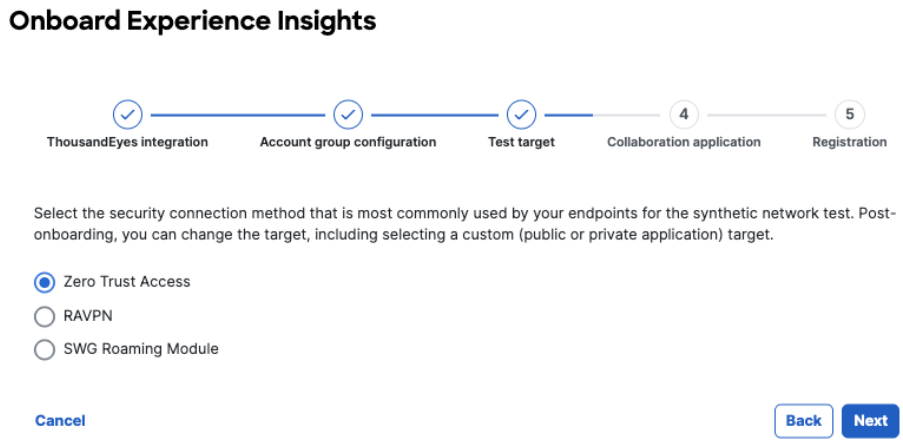
6. Choose your ThousandEyes account groups integration: Default account group integration or Multiple account groups integration. After the integration you can change the integration method by navigating in Secure Access to **Account Management > Account group integration**.
   a) **Default account group integration**: By selecting this integration, two default tests are only created in the default account group. If you need to edit these tests after the completion of onboarding, navigate to Account Management. For more information, see Edit Default Test Target.
   b) **Multiple account groups integration**: By selecting Multiple account groups, you will see all the ThousandEyes account groups and tests associated with the ThousandEyes user who did the initial integration with Secure Access



Step 3: Default test target

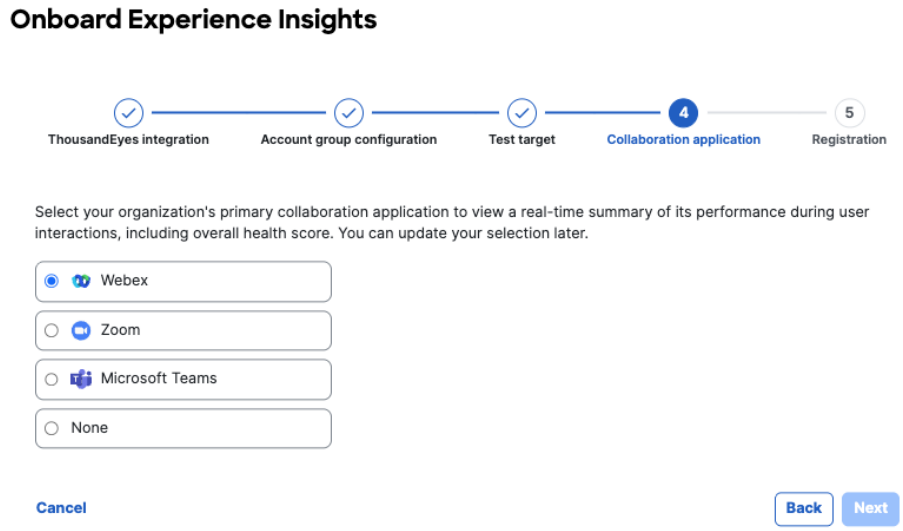
7. For the synthetic network test, select the security connection method most commonly used by your endpoints. Test target options include Zero Trust Access, RAVPN, and SWG Roaming Module.

   Synthetic tests identify performance issues in user journeys to their destinations. After onboarding, you can modify the test target to include custom public or private applications.



Step 4: Unified collaboration application

8. Select your organization's primary collaboration application (Webex, Zoom, Microsoft Teams, or None) to view a real-time summary of its performance during user interactions, including overall health score. You can update your selection later.



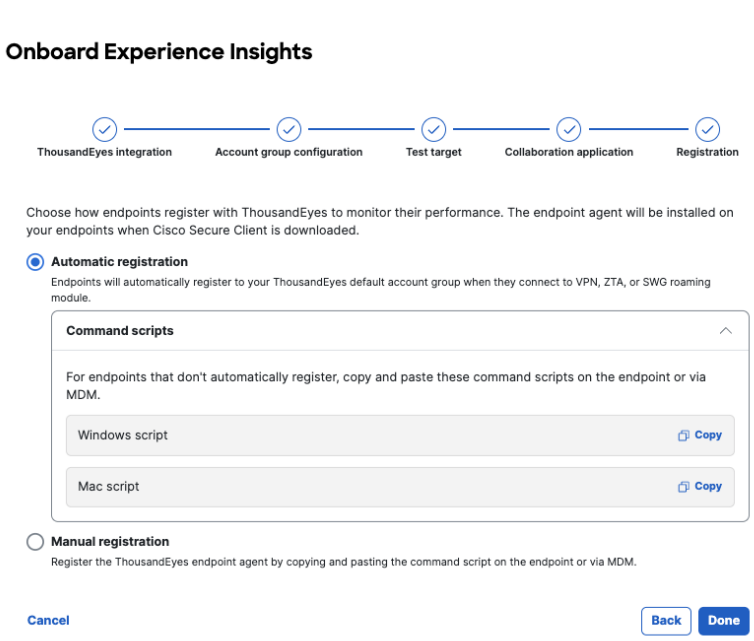
Step 5: ThousandEyes agent

Endpoints must be registered to your Secure Access organization to be monitored for performance.

When you deployed Cisco Secure Client to your endpoints, the ThousandEyes Endpoint Agent was installed.

The ThousandEyes Endpoint Agent will register to your Secure Access organization automatically once your endpoints have connected to VPN, ZTA, or Roaming Module.

9. Manually register the ThousandEyes Endpoint Agent for endpoints that are not using VPN, ZTA, or the Roaming Module for their security connection.



This process involves copying and pasting a command script onto the specific endpoints. The registration script includes a ThousandEyes connection string that is unique to your organization. Your organization's connection string is the parameter following the `--register` argument.

```
"C:\Program Files (x86)\Cisco\Cisco Secure Client\ThousandEyes Endpoint
Agent\csc_te_agent" --register <connection string>
```

```
sudo /Applications/Cisco/Cisco\ Secure \Client\ -\ ThousandEyes\ Endpoint\
Agent.app/Contents/MacOS/csc_te_agent --register <connection string>
```

a) Navigate to **Experience Insights** > **Configure Account** to find your organization's registration scripts. You can access these scripts at any time after onboarding is completed.
b) Copy the appropriate command script for your endpoint's operating system.
c) On the target endpoints, paste and execute the copied script.

What to do next

Once you complete the Experience Insights onboarding wizard and the registration of one or more endpoints, data reported by the ThousandEyes endpoint agent will appear in your Experience Insights dashboard.

Navigate to **Experience Insights** > **Endpoints** to confirm that your endpoint is reporting data.

For more information, see the following resources:

- Cisco Secure Client ThousandEyes Endpoint Agent Module
- Get Started with Cisco Secure Client on Windows and macOS Devices
- Download Cisco Secure Client
- Deploy Cisco ThousandEyes Module via Microsoft Intune (for an MDM example)

Cisco AI Assistant for Experience Insights

Describes Cisco AI Assistant for Experience Insights in Cisco Secure Access. Use the Cisco AI Assistant to investigate device performance issues reported by the ThousandEyes endpoint agent.

Use the Cisco AI Assistant to investigate device performance issues reported by the ThousandEyes endpoint agent. Ask natural language questions of the assistant about network traffic, device availability, and SaaS application performance.

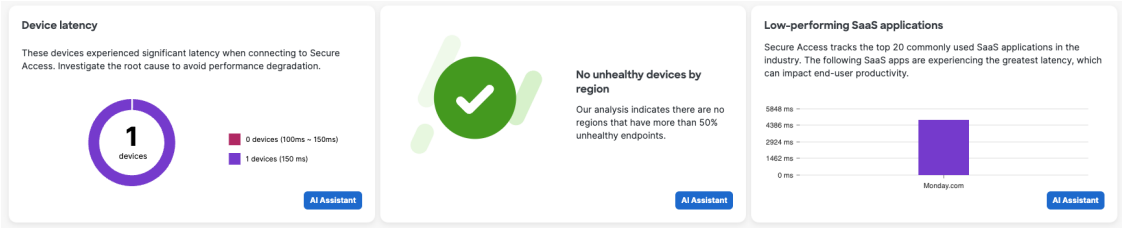
> **Note**
>
> For more information on using Cisco AI Assistant in Secure Access, including best ways to prompt the assistant, see Get Started with the Cisco Assistant.

How to Use the Cisco AI Assistant in Experience Insights

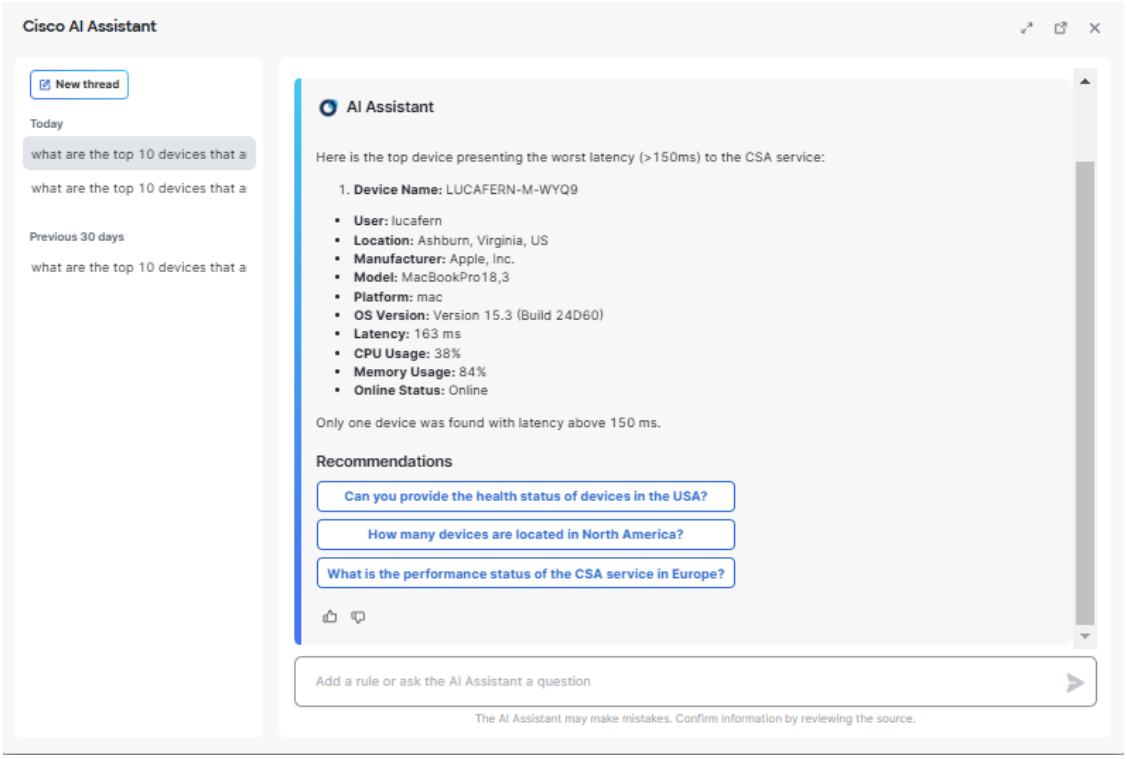
Provides instructions for completing the How to Use the Cisco AI Assistant in Experience Insights workflow in Cisco Secure Access. On the Experience Insights Home page, click AI Insights.

Procedure

1. On the Experience Insights Home page, click **AI Insights**.
2. Select one of the three cards to launch the AI Assistant. Each card–Device Latency, Unhealthy Regions, and Low-performing SaaS Applications–highlights potential performance issues in your environment, as identified by ThousandEyes endpoint agents.



Based on your selected card, the Cisco Assistant displays an answer to the most common pre-populated question and suggests additional prompts for further exploration.



Limitations

- Cisco Assistant cannot identify devices by username. Use the device name or the OS username of the signed-in user.
- Cisco Assistant does not have access to historical data; responses reflect the latest information only.

Prompt examples

Describes Prompt examples in Cisco Secure Access. The Cisco Assistant will interpret questions about ThousandEyes endpoint licenses, DEM endpoint licenses, and Experience Insights endpoint licenses as synonymous.

> **Note**
>
> The Cisco Assistant will interpret questions about ThousandEyes endpoint licenses, DEM endpoint licenses, and Experience Insights endpoint licenses as synonymous. For more information about ThousandEyes licensing, see ThousandEyes Endpoint Agent Licensing.

Contextual Conversations

Describes Contextual Conversations in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Cisco Assistant for Secure Access has context awareness within each thread. Once you begin a thread with a prompt, you can continue the conversation with follow-up prompts that the Assistant can interpret by referring to earlier prompts.

Examples of Contextual Conversations for Experience Insights Prompts
Beginning prompt: What is the response time of Monday.com? Follow-up prompt: Is it reachable?
Beginning prompt: How many Experience Insights Advantage licenses do we have? Follow-up prompt: How many of those licenses are in use?

Note

The Assistant's context window for Experience Insights prompts is limited to the thread's five most recent prompts and does not include details from the Assistant's responses.

ThousandEyes Account Management in Experience Insights

Provides reference information about ThousandEyes Account Management in Experience Insights in Cisco Secure Access, including ThousandEyes Organization and Default Account Group, Unified Collaboration Application, and Default Test Target. It summarizes the values, options, and related details presented in the topic.

Account Management in Experience Insights is a centralized interface to manage your ThousandEyes organization and account group, configure collaboration applications, update default test targets, view tenant and data storage details, and register ThousandEyes agents on endpoint devices.

Navigate to **Experience Insights** > **Overview** > **Account Management**.

ThousandEyes Organization and Default Account Group

The top of the ThousandEyes Account page displays your ThousandEyes organization and default account group. To delete the integration between Secure Access and ThousandEyes, click **Remove Integration**. Removing the integration means that endpoints registered to the account group will no longer be monitored within Experience Insights. Your endpoints will continue to be monitored directly in ThousandEyes.

Unified Collaboration Application

View your organization's current collaboration application. You chose the application during onboarding. To change it, click the **pencil icon** and select the most commonly used application within your organization from the options: Webex, Zoom, Microsoft Teams, or None.

Default Test Target

Synthetic tests allow you to identify performance issues with user journeys to destinations. You chose the default target during onboarding. To change the default test target that will apply to all endpoints, click the **pencil icon** and select from the options: Zero Trust Access, RAVPN, SWG Roaming Module, and Custom Target. For more information, see Edit Default Test Target.

Tenant and Data Storage Location

The section displays the location of your ThousandEyes tenant and data storage. To update data storage location, contact Thousand Eyes support via support@thousandeyes.com

ThousandEyes Agent Registration Scripts

When you deployed Cisco Secure client to your endpoints, the ThousandEyes Endpoint Agent was installed. The ThousandEyes Endpoint Agent will register to your Secure Access org automatically once your endpoints have connected to VPN, ZTA, or Roaming module so that you can monitor their performance.

For endpoints that are not using one of those security connection methods, you must register the ThousandEyes Endpoint Agent manually by copying and pasting the command script on the endpoints. For more information, see Register ThousandEyes Agents on page 2251

Account Group Integration

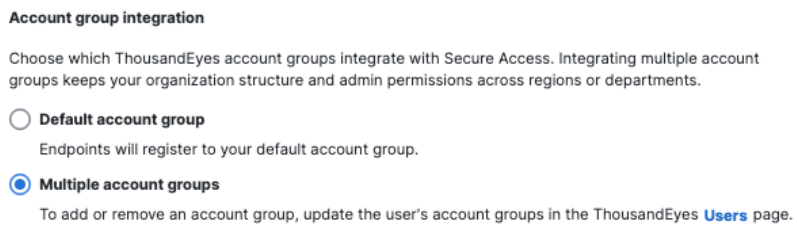
This is where you select multiple ThousandEyes account groups to integrate with Secure Access. You can select Default account group or Multiple account groups.

Default Account Group:

If you choose the Default Account Group during onboarding: Data is pulled only from the default group. No default tests are created in other account groups.

If you switch to the Default Account Group after onboarding: If you are switching from Multiple account groups to Default account group, then only tests for the default account group are enabled and tests for the multiple account groups are disabled. You can still edit the tests in ThousandEyes.

Multiple account groups: By selecting Multiple account groups, you will see all the ThousandEyes account groups and tests associated with the ThousandEyes user who did the initial integration with Secure Access. Additionally, you can see the unique registration scripts for each connected account group.



Changing user roles or account group settings may take up to 5-10 minutes to reflect the new changes.

Endpoint Registration

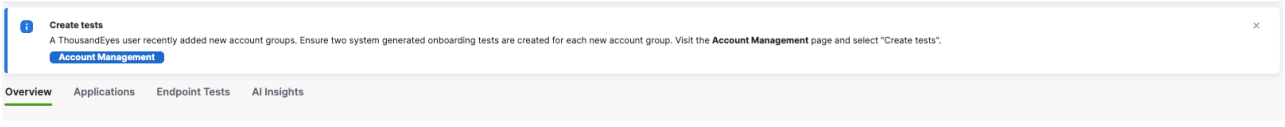
Automatic Registration: Enabling automatic registration will register all agents with the Default account group. If you change your mind, you can manually transfer the agents to other account groups in the ThousandEyes agent settings.

Manual Registration: You can create distinct deployment packages, each with a unique registration script for a specific account group.

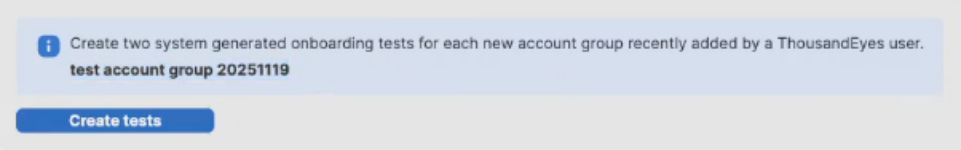
To learn more about Automatic and Manual registration, see Step 5: ThousandEyes agent in Onboard Experience Insights.

Create Tests for New Account Groups

If the ThousandEyes admin who completed the Secure Access integration was added to a new account group in ThousandEyes and the two default tests were not generated- then a **Create tests** banner will appear on the Experience Insights Overview page.



Click Account Management > Create tests. The two default tests from the Default account group are copied to the new account group. This ensures that all your account groups have consistent monitoring and performance baselines from the start.



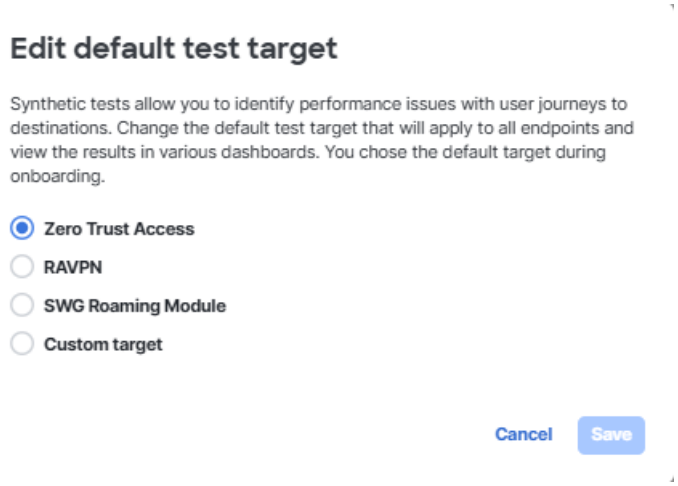
Edit Default Test Target

Provides instructions for completing the Edit Default Test Target workflow in Cisco Secure Access. When you onboarded Experience Insights, you chose a security method as a target for the default test based on what is used by most of your endpoints.

When you onboarded Experience Insights, you chose a security method as a target for the default test based on what is used by most of your endpoints. If needed, you can change the target, including choosing a custom private or public application as the target.

Procedure

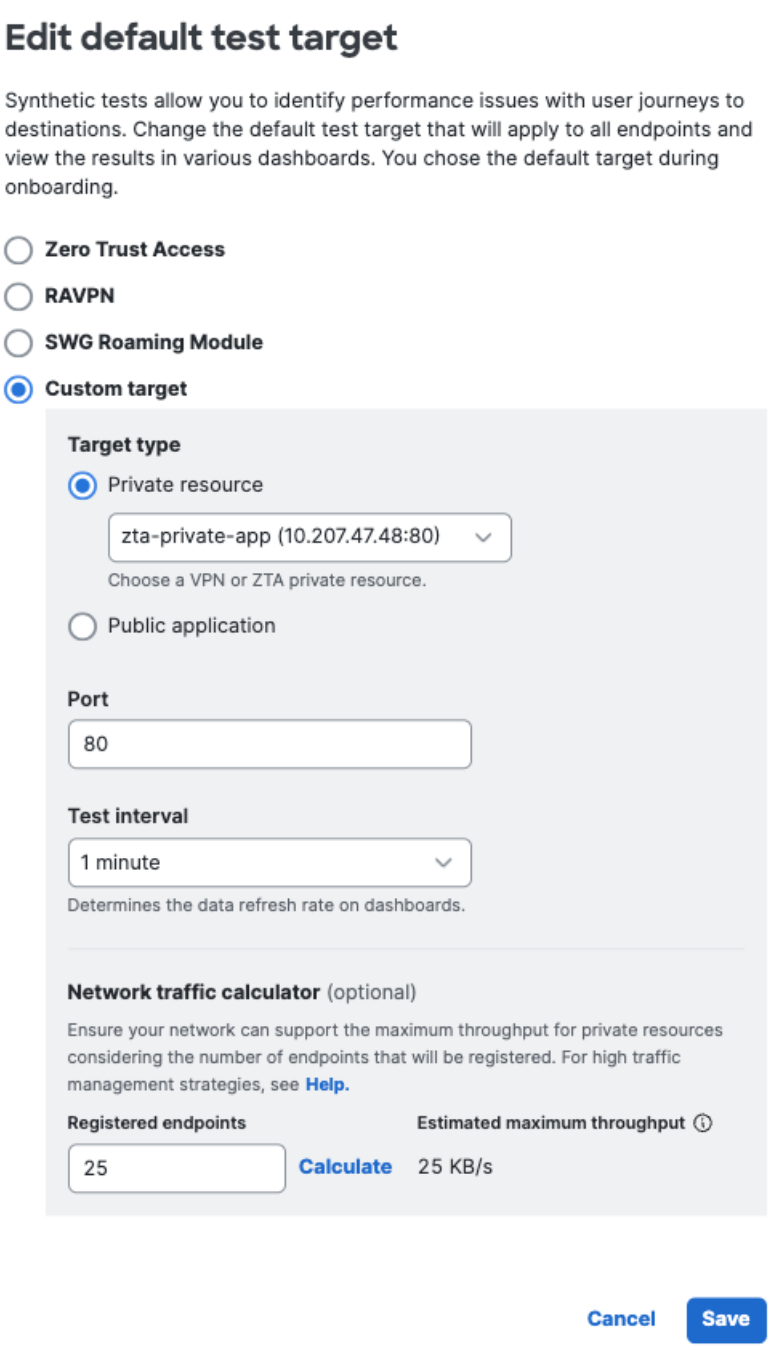
1. Choose a target for the default test.



2. If you choose Custom target, complete the onscreen fields.

Note

Heavy traffic may be sent to custom applications (per the onscreen note). For information on managing the traffic, see Estimate Peak Traffic to Custom Targets for Default Endpoint Tests.



Register ThousandEyes Agents

Provides instructions for completing the Register ThousandEyes Agents workflow in Cisco Secure Access. When you set up Secure Access, you registered the ThousandEyes endpoint agent on all endpoints.

When you set up Secure Access, you registered the ThousandEyes endpoint agent on all endpoints. Each time you add a new endpoint device in your organization, you must register the agent on the new device.

This process explains how to register ThousandEyes endpoint agents and begin reporting endpoint telemetry. You can enroll agents in different ways:

Procedure

1. **Automatic registration (recommended)** – happens automatically when users connect using Cisco Secure Client.
2. **Manual registration** – you enroll by running the registration script on the endpoint's command line manually or via MDM.

What to do next

Result: The endpoint is now available in Experience Insights and will begin reporting data. To see the endpoint in the endpoint list, navigate to: **Experience Insights** > **Endpoint list**.

> **Note**
>
> The process for managing your ThousandEyes account is different than the process for managing your Secure Access account. In Secure Access, you choose whether to save logs for events and traffic for your account to the data center in the U.S. or Europe.

Automatic Registration of ThousandEyes Endpoint Agents

Provides instructions for completing the Automatic Registration of ThousandEyes Endpoint Agents workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

When Cisco Secure Client is installed and users start an active session with ZTA, URC, or VPN, the ThousandEyes endpoint agent automatically registers to the connected default ThousandEyes account group.

We recommend that you validate the workflow with a small test group before deploying the configuration more broadly.

Before you begin

To use automatic registration, ensure that the following requirements are met:

- ThousandEyes endpoint agent is installed.
- Integration completed between your Cisco Secure Access and your ThousandEyes account.
- Cisco Secure Client is installed on the endpoint and is connected using at least one of the following features: Zero Trust Access (ZTA), Umbrella Roaming Client (URC), or VPN.
- An active user session on the endpoint with at least one of the following features enabled: Zero Trust Access (ZTA), Umbrella Roaming Client (URC), and VPN.

Procedure

1. Follow these steps to Download and Install Cisco Secure Client on the endpoint.
2. The end user establishes a valid session using ZTA, URC, or VPN.

   The following happens automatically once the user establishes a valid session: The agent automatically requests the default ThousandEyes Account Group to confirm the Secure Access integration. Next, the system automatically verifies that the device is a legitimate asset belonging to the organization.

What to do next

Once the session is active, the ThousandEyes Endpoint Agent automatically validates local data collected from the device. The agent gathers device and organization identifiers from the active module.

Depending on the active connection type, the agent uses the following data sources:

- VPN: The ThousandEyes endpoint agent uses the vpncli tool to identify the active VPN connection and extract the FQDN from the VPN profile folder. The agent uses this FQDN to resolve the Secure Access OrgID. VPN cluster FQDN identifiers can be 4 or 6 characters.
- ZTA: The ThousandEyes endpoint agent reads cached configuration data from Windows or macOS and uses it to retrieve the ztna_device_id, user_id, and org_id.
  - Windows:

    ```
    C:\\ProgramData\\Cisco\\Cisco Secure Client\\ZTA\\enrollments\
    ```

  - macOS:

    ```
    /opt/cisco/secureclient/zta/enrollments
    ```

- URC: The ThousandEyes endpoint agent reads cached configuration data from the local OrgInfo.json file on Windows or macOS and uses it to retrieve the organizationId and userId.
  - Windows:

    ```
    C:\\ProgramData\\Cisco\\Cisco Secure Client\\Umbrella\\OrgInfo.json
    ```

  - Mac:

    ```
    /opt/cisco/secureclient/umbrella/OrgInfo.json
    ```

What happens if automatic registration fails?

If automatic registration does not succeed on the first attempt, the agent retries every 10 minutes. The agent attempts registration in the following order: ZTA, Umbrella Roaming Client (URC), and VPN. The agent continues retrying until it validates a supported session and completes registration.

Manual Registration of ThousandEyes Endpoint Agents

Provides instructions for completing the Manual Registration of ThousandEyes Endpoint Agents workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

If an endpoint will **not** connect via Zero Trust Access (ZTA), the Umbrella Roaming Client (URC), or a VPN, you can manually register the endpoint with Secure Access by running the registration script on the endpoint command line.

Procedure

1. Navigate to **Experience Insights > Account Management> Endpoint registration> Manual registration** to copy your organization's registration scripts with your unique connection string.
   a) For **Windows**: you can manually register the agent using your connection string and execute the subsequent register command:
   ```
   "C:Program Files (x86)CiscoCisco Secure ClientThousandEyes Endpoint Agentcsc_te_agent" --register <connection string>
   ```
   b) For **macOS**: you can manually register the agent using your connection string and execute the subsequent register command:
   ```
   sudo /Applications/Cisco/Cisco Secure Client - ThousandEyes Endpoint Agent.app
   ```
2. **MDM Registration to use ThousandEyes Endpoint** (Intune, Jamf, and other MDM Tools)
   a) Navigate to Deploy Cisco ThousandEyes Module via Microsoft Intune for steps to install Secure Client and register the ThousandEyes endpoint agent.

Experience Insights Overview

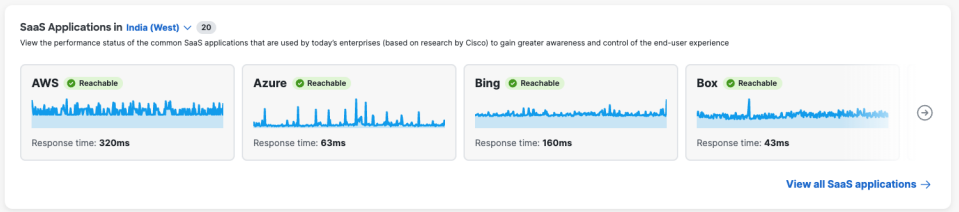
Provides reference information about Experience Insights Overview in Cisco Secure Access. The Overview page provides a centralized view of your network's health and performance, featuring insights into both common SaaS applications and the status of your registered endpoints.

The **Overview** page provides a centralized view of your network's health and performance, featuring insights into both common SaaS applications and the status of your registered endpoints.

Navigate to **Experience Insights** > **Overview**.

SaaS Applications

View the availability and performance of SaaS applications as traffic flows from the Secure Access cloud. These are common SaaS applications used by today's enterprises, based on research by Cisco.



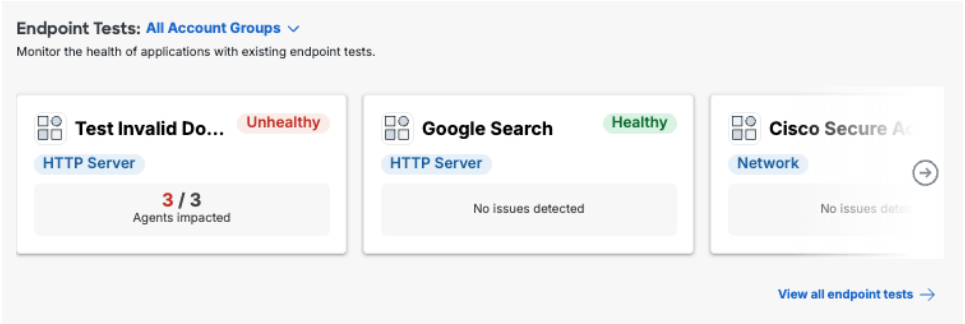
Interact with the SaaS Applications Carousel

- In the **SaaS applications drop-down menu**, select a region. For more information, see Secure Access Regions on page 113.
- Click the arrow to scroll to the right.
- Click **View all SaaS applications** to navigate to the **Applications** page. For more information, see View SaaS Application Performance on page 2262.

Endpoint Tests

View the health of your synthetic endpoints tests that monitor the connectivity from endpoints to various destinations. These tests help assess network performance and identify issues affecting user experience.

- **Tests Sources**: Both Secure Access created tests and ThousandEyes created tests appear together in this carousel, providing a unified view of endpoint test health.
- **Display Order**: Displays up to five applications at a time. Tests are shown in order from the worst performing (unhealthy) to healthy, allowing you to quickly focus on the worst-performing tests.
- An endpoint is considered healthy or unhealthy based on the application score for a specific test. For more information, see Experience score.



Interact with the Endpoint Tests Carousel

Navigation: Clicking on a specific test widget in the carousel takes you directly to that endpoint test's results page to see the metrics and diagnostics for that test.

- In the **Endpoint Tests** drop-down menu, select an **Account Group**. This filter is only present if you have multiple account group enabled for your account. For more information, see ThousandEyes Account Management in Experience Insights.
- Click **View all endpoint tests** to navigate to the **Endpoint tests** page. For more information, see About Endpoint Agent Tests.

Experience Score Map

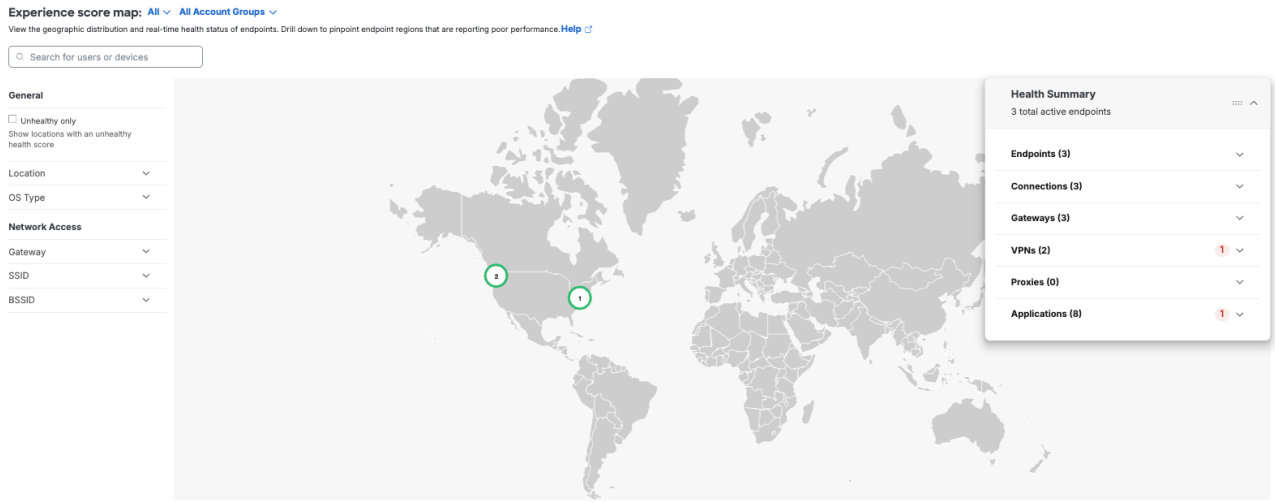
The Experience score map visually represents all endpoints installed and registered to your integrated ThousandEyes account groups. For instructions on how to install and register your endpoints, see ThousandEyes Account Management in Experience Insights.

This map offers real-time insights into the geographic distribution and health status of your endpoints. An endpoint's status is determined by experience score that is calculated by **Segment Thresholds: Agent, Connection, Gateway, Proxy, VPN, and Application**.

Continuously monitoring endpoint health can serve as a starting point for investigating issues.

For example:

- If a specific endpoint is consistently unhealthy, examine its hardware and network connection for issues.
- If all endpoints in a region are unhealthy, a service outage might be the cause.



Interact with the Endpoints Map

- **View Location Details**: Hover over a location marker to view the number of healthy, at-risk, and unhealthy endpoints for that location.

> **Note**
>
> Endpoint locations are not the same as the location of your VPN or ZTA connection, but the geolocation of the endpoint itself. If an endpoint cannot be collected, ThousandEyes detects the public IP of the endpoint which may be based on VPN or ZTA or URC and selects the closest Secure Access region you are connected to.

- **Explore Endpoint Concentration**: Click a number on the map to see the concentration of endpoints for an area. Continue zooming in on the map until you reach the exact endpoint location.

Enabling location services for the ThousandEyes endpoint agent on each endpoint ensures accurate identification and display of the endpoint, along with correct BSSID and SSID information, enabling filters and true location visualization critical for resolving end-user network issues.

For more information on how to enable location services for ThousandEyes Endpoint Agent, see Enabling Location Services for Endpoint Agent Wi-Fi Reporting for MacOS and Endpoint Agent Wi-Fi Reporting on Windows 11 (24H2) and Later for Windows.

Filters

- **All**: View all running endpoint tests or select a specific test to view performance issues. The experience score is calculated based on the selected test filter. When All is selected, it reflects all tests currently running on the endpoints. When a specific test is selected, it reflects only the endpoints running that test and their connectivity to that destination.
- **All Account Groups**: View all account groups or select a specific group to view the health status of the endpoints. (This option only appears when you have multiple ThousandEyes account groups selected in Account Management.)
- **Search by users or devices**: Enter a first name and last name, ThousandEyes username, or device name into the search bar and press **Enter** to find matches. If there's an exact match, the endpoint table will update to show only that single endpoint. If your entry is not an exact match, the search will fail, and no endpoints will display in the table.

General

- **Unhealthy only**: Select to view the locations where endpoints have an unhealthy experience score.

- **Location**: View endpoints by country or drill down to specific cities.
- **OS type**: View operating system by type and version.

Network Access

- **Gateway**: View the local network gateway or the router that provides connectivity for the endpoint.
- **SSID** (Service Set Identifier): View the Wi-Fi network name end users see.
- **BSSID** (Basic Service Set Identifier): View the unique identifier for a specific wireless access point broadcasting for the Wi-Fi network.

Health Summary

Health Summary provides a high-level overview to see what is healthy or unhealthy in a selected location. The section shows the top five unhealthy locations for each segment. Health Summary includes the following components:

- **Endpoints**: Shows the health of an endpoint based on the agent score-which is based on CPU and memory. This helps identify device specific issues.
- **Connections**: Displays the health status of network connections, including wired, wireless, and cellular links. Connection health is based on metrics such as link speed and signal quality, helping identify issues with the endpoint's network connectivity.
- **Gateways**: Shows the health of gateways (local routers or network gateways) that endpoints connect through. Gateway health is assessed using metrics like packet loss, latency, and jitter measured from devices connected to the gateway, indicating the quality of the local network segment.
- **VPNs**: Reflects the health of VPN connections used by endpoints. VPN health scores are derived from metrics such as VPN ping loss, latency, jitter, and error flags, aggregated across devices connected to the VPN, providing insight into VPN performance and reliability.
- **Proxies**: This indicates the health of proxy servers used by endpoints. Proxy health is measured primarily using **HTTP connect times** and **proxy-specific error codes** obtained from end-to-end HTTP measurements. Additionally, **latency, jitter, and loss metrics** are derived from both local network (ping) and end-to-end network measurements. These combined metrics help detect proxy-related issues by reflecting the responsiveness and reliability of the proxy servers.
- **Applications**: Displays the health status of monitored applications based on scheduled tests and performance metrics, allowing identification of application-level degradations affecting user experience.

Using the Experience Score Map Filters for Endpoints List

1. **Select Filters on the Experience Score Map**: On the left-hand side of the Experience Score Map, choose various filters to narrow down the data based on your criteria.
2. **Choose a Component in the Health Summary Section**: After setting your filters, move to the Health Summary section. Select a specific component that you want to investigate further.
3. **Click View**: to see the endpoints impacted in a specific city or View All to see all cities in the selected location with the impacted endpoints for that segment. This action takes you directly to the Endpoints List page.
4. **View the Filtered Endpoints List**: The Endpoints List page displays the specific endpoints affected and retains all the filters you initially selected in the Experience Score Map. You see a focused list of endpoints that match your selected criteria and component.
5. **Click on a User name**: For further investigation, see historical data in the performance section of the user details page and identify which hop the user is having issues with. The selected test from the Endpoint List carries over to the Endpoint test results on the user details page.

> **Note**
>
> These filters are based on real-time data, and these filters cannot be saved for future use.

Endpoints

Provides reference information about Endpoints in Cisco Secure Access. View a real-time summary of the health of your endpoints for faster troubleshooting and to take action to deliver a better, more secure experience for your end users.

View a real-time summary of the health of your endpoints for faster troubleshooting and to take action to deliver a better, more secure experience for your end users.

Navigate to **Experience Insights** > **Endpoints**.

By default, the Endpoints List is sorted by Experience score in the order of unhealthy, healthy, and then undetermined. For more information, see Experience score.

In the Endpoint list, click on the ellipsis to edit, disable, enable, and delete endpoints. Deleting an endpoint permanently removes it from both Secure Access and ThousandEyes.

In ThousandEyes, you can configure the Agent Status Settings to auto-disable, auto-delete, or auto-enable endpoint agents. These options allow you to configure the number of days after which the agents can be **disabled** or **deleted**. You can also configure the number of days an active but disabled agent can be **re-enabled**. For more information, see Auto - manage the status for Endpoint Agents in our ThousandEyes documentation.

Changes may take a couple minutes to reflect on the dashboard. Disabling or deleting an endpoint frees up a license that can be reassigned to another endpoint, such as a new device, or one with a lower-tier license. Upgrading an endpoint to a higher-tier license allows you to retain data for a longer period and run more tests.

Use the search and filter options to review endpoint table results by user name, device name, account group, impacted segment, experience score, or location. There are additional filters that can be selected: Gateway, VPN Target, BSSID, and SSID.

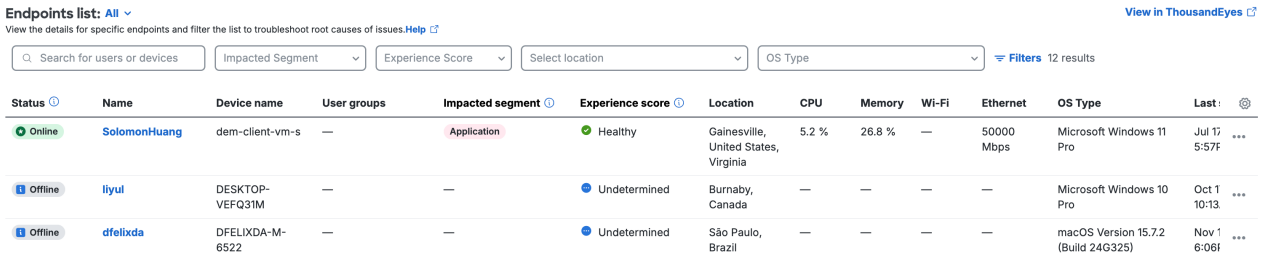
View Endpoint List

- **All** : Use this filter to view endpoint connectivity across all currently running endpoint tests for each endpoint or select a specific running test. The experience score changes depending on the selected running test. The list shows only running endpoint tests and only endpoints that are included in those tests.
  - HTTP test: selecting this test displays additional columns for response time and response code.
  - Network test: selecting this test displays additional columns for latency, jitter, and loss.
- **Name**: Displays the OS-authenticated user first and last name. If identity resolution criteria are not met, the table defaults to the ThousandEyes agent name.
- **Search by users or devices**: Enter a first name and last name, ThousandEyes username, or device name into the search bar and press **Enter** to find matches. If there's an exact match, the endpoint table will update to show only that single endpoint. If your entry is not an exact match, the search will fail, and no endpoints will display in the table.
- **User Group**: User group information is pulled directly from your customer active directory (AD) or identity provider (IDP) integration.
- **Account group** column only appears when you have multiple ThousandEyes account groups selected in Account Management. For more information, see ThousandEyes Account Management in Experience Insights. An endpoint can only be registered to a single account group.

- **Impacted Segment**: is a drop-down list to view specific impacted segments: Agent, Connection, Gateway, Proxy, VPN, or Application.
- **Experience Score**: shows the overall health of an endpoint, categorized as Healthy, Unhealthy, or Undetermined. The score is calculated as the average of several scores including agent, connection, gateway, VPN, proxy, and applications. An endpoint with a score below 50 is marked Unhealthy. If there is not enough data to calculate a score, the status appears as Undetermined. For more information, see Experience Score.
- **Select Location**: search by specific locations.
- **OS Type**: The operating system of the user device.

Click **Filters** to select additional search criteria to narrow your search results.

- **Gateway**: view the local network gateway or the router that provides connectivity for the endpoint.
- **SSID** (Service Set Identifier): View the Wi-Fi network name end users see.
- **BSSID** (Basic Service Set Identifier): View the unique identifier for a specific wireless access point broadcasting for the Wi-Fi network.
- **OS Version**: view the specific operating system's version.



Wi-Fi Descriptions

Describes Wi-Fi Descriptions in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Following are common Wi-Fi terms and descriptions. End users use this wireless network technology to connect securely to your network and to Secure Access when accessing your organization's private resources.

Wi-Fi term	Description
Signal quality	The overall strength of the wireless signal. Higher values represent better signal quality.
RSSI (received signal strength indicator)	The signal strength from the access point. A higher (less negative) RSSI indicates a stronger signal.
SSID (Service Set Identifier)	A unique identifier that is assigned to a wireless network. Allows devices on the network to identify and connect to the correct network.
BSSID (Basic Service Set Identifier)	The physical address of a wireless router or access point that's used to connect to Wi-Fi.
Channel	Communication frequency used by a wireless network. Optimal channels can reduce interference and improve performance.

Wi-Fi term	Description
SNR (signal-to-noise ratio)	Ratio of signal strength to background noise. High SNR indicates a clearer, more reliable wireless connection.
Transmit rate	Data transmission speed between the device and access point. Higher transmit rates generally indicate faster connections.
Noise	Interference level or background noise in a wireless environment. A lower (more negative) noise value indicates less interference and a cleaner communication environment.

Experience Score

Experience Score is a real-time measure of an endpoint's overall health and user experience.

Experience Score is a real-time measure of an endpoint's overall health and user experience. It is calculated by averaging multiple segment scores, each representing a different aspect of the endpoint's performance and connectivity. Based on the final score, the endpoint is shown as **Healthy**, **Unhealthy**, or **Undetermined**.

Based on the final averaged score, the endpoint's status is categorized as:

- **Healthy**: The endpoint is performing well across all segments.
- **Unhealthy**: One or more segments indicate poor performance or connectivity.
- **Undetermined**: Insufficient data or inconclusive results to determine health.

Each segment score is calculated independently, and the overall Experience Score is the average of all segment scores. The experience score aggregates the following segment scores:

- **Agent**: Reflects the device's CPU and memory usage.
- **Connections**: Displays the health status of network connections, including wired and wireless. Connection health is based on metrics such as link speed and signal quality, helping identify issues with the endpoint's network connectivity.
- **Gateways**: Shows the health of gateways (local routers or network gateways) that endpoints connect through. Gateway health is assessed using metrics like packet loss, latency, and jitter measured from devices connected to the gateway, indicating the quality of the local network segment.
- **VPNs**: Reflects the health of VPN connections used by endpoints. VPN health scores are derived from metrics such as VPN ping loss, latency, jitter, and error flags, aggregated across devices connected to the VPN, providing insight into VPN performance and reliability.
- **Proxies**: This indicates the health of proxy servers used by endpoints. Proxy health is measured primarily using **HTTP connect times** and **proxy-specific error codes** obtained from end-to-end HTTP measurements. Additionally, **latency**, **jitter**, and **loss metrics** are derived from both local network (ping) and end-to-end network measurements. These combined metrics help detect proxy-related issues by reflecting the responsiveness and reliability of the proxy servers.
- **Applications**: Displays the health status of monitored applications based on scheduled tests and performance metrics, allowing identification of application-level degradation affecting user experience.

Since the experience score is an average, it is possible for some segments to be impacted while the overall score remains **Healthy**. This means:

- Even if certain segments show issues, the overall experience score may still indicate a healthy status.

- This occurs because strong scores in other segments can offset unhealthy segments when averaged.

Experience Insights assigns a summary Experience Score to each endpoint in the table and on the endpoint performance map. Navigate to **Experience Insights** > **Overview** page to see the **Experience score map**.

Segment Thresholds: Agent, Connection, Gateway, Proxy, VPN, and Application

Table 27: Experience Score

Quality	Score Range
Unhealthy	0 to 50
Healthy	51 to 100

Table 28: Agent Score

	Healthy	Unhealthy
CPU usage	≤ 70%	>70%
Memory usage	≤ 90%	> 90%

Table 29: Application Score

	Healthy	Unhealthy
HTTP Test		
Experienced Time To First Byte (TTFB)	≤ 3000ms	> 3000ms
Network Test (PING)		
Latency (ms)	≤ 250ms	> 250ms
Jitter (ms)	≤ 75ms	> 75ms
Loss (%)	≤ 10%	> 10%
Dynamic Test (AST)		
Latency (ms)	≤ 300ms	> 300ms
Jitter (ms)	≤ 50ms	> 50ms
Loss (%)	≤ 10%	> 10%

Table 30: VPN Score

	Healthy	Unhealthy
VPN Loss	< 10%	> 10%
VPN Latency	≤100ms	>100ms
VPN Jitter	≤30ms	> 30ms

Table 31: Gateway Score

	Healthy	Unhealthy
Gateway Loss	<10%	>10%

	Healthy	Unhealthy
Gateway Latency	<30ms	>30ms
Gateway Jitter	<25ms	>25ms

Table 32: Proxy Score

	Healthy	Unhealthy
Proxy Latency	<150ms	>150ms
Proxy Jitter	<75ms	>75ms
Proxy Loss	<10%	>10%

Table 33: Connection Score

	Metric	Healthy	Unhealthy
Wired Connection	Link Speed	>10 Mbps (typical good speeds)	<10 Mbps
Wireless Connection	Signal Quality (RSSI)	> 50 (strong signal quality)	<50

An endpoint with a health status of **Undetermined** indicates one of the following scenarios in which Experience Insights has not received test data from the endpoint agent.

- The endpoint is offline.
- The endpoint agent is disabled.
- The endpoint agent is online, but the test was interrupted by an error reported in the **Error** column.
- Only for Windows: The endpoint has an Npcap error, shown next to the device name in the endpoint table.

ThousandEyes Agent Version

Use the endpoint table to monitor endpoints that have not updated to the latest **ThousandEyes agent version**. For more information about features and fixes delivered by each agent version, see the ThousandEyes Changelog for **Endpoint Agent Client** release notes.

- Endpoint health metrics reported by an out-of-date agent may not match metrics reported by up-to-date agents.
- The ThousandEyes endpoint agent checks for updates every four hours. If an update is available, it will download in the background and attempt installation later. Updates occur only if a new version is available, typically once a month, but can be more frequent if patches are needed. If an update fails, the **ThousandEyes agent version** field in the Experience Insights endpoint table shows a warning icon with a tooltip.
- There is no method for retrying a failed update. However, you can download and reinstall Cisco Secure Client with the ThousandEyes Endpoint Agent Module to trigger an update to the endpoint agent. For detailed instructions, see Download Cisco Secure Client. It is not necessary to uninstall Secure Client before running the Secure Client `Setup.exe` wizard. Reinstalling without uninstalling means that you do not need to run the registration script to associate the endpoint with your ThousandEyes account.
- For more information, see Endpoint Agent FAQ.

The ThousandEyes endpoint agent leverages the Npcap driver library to collect metrics on Windows devices. A warning icon in the endpoint table **Device name** field indicates a Windows device with an Npcap version that is unsupported by ThousandEyes. ThousandEyes will not collect metrics from Windows devices with unsupported versions.

To enable unsupported versions of Npcap, navigate to Advanced agent settings in ThousandEyes. For more information, see Npcap Driver Upgrade Management in ThousandEyes documentation.

ThousandEyes Metrics

Experience Insights defines metrics as follows. For more information, see ThousandEyes Metrics: What Do Your Results Mean?

- **Latency:** The average of the round-trip packet time. Round-trip packet time is the time from which a packet is sent by the agent to the time the agent receives a reply.
- **Jitter:** The mean deviation of latency. The mean deviation represents how far, on average, all measurements are from the mean of the data.
- **Loss:** End-to-end packet loss. The percentage of packets lost is calculated by subtracting the number of reply packets the agent receives from the target (responses) from the number of packets sent by the agent, then dividing by the number of packets sent, then multiplying by 100.
- **Response time:** The time elapsed from the beginning of the request (before the DNS request) until the client receives the first byte of the response from the server. Also known as time-to-first-byte.

View SaaS Application Performance

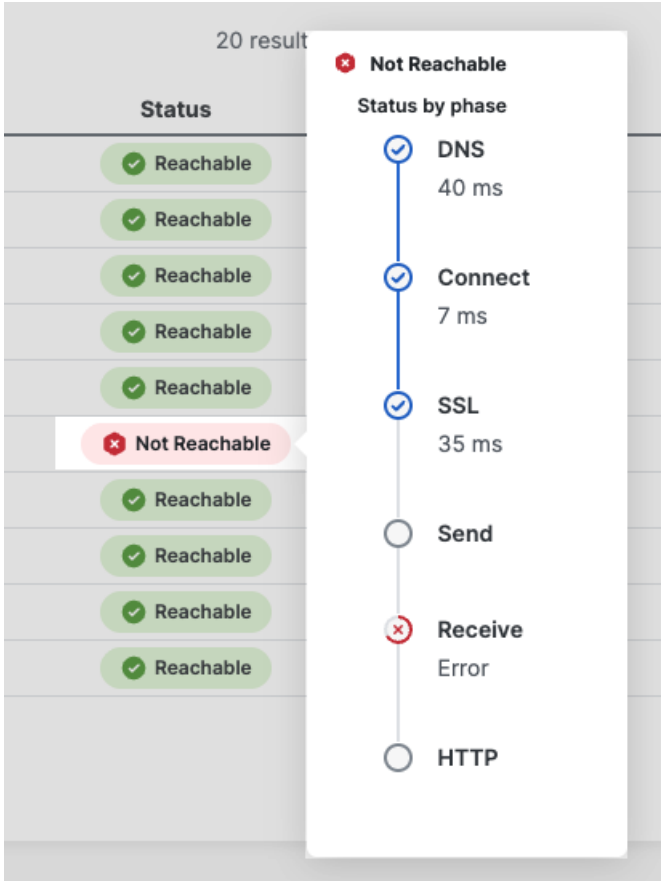
Provides reference information about View SaaS Application Performance in Cisco Secure Access. This section describes how to view the availability and performance of SaaS applications as traffic flows from the Secure Access cloud.

This section describes how to view the availability and performance of SaaS applications as traffic flows from the Secure Access cloud. These are common SaaS applications used by today's enterprises, based on research by Cisco.

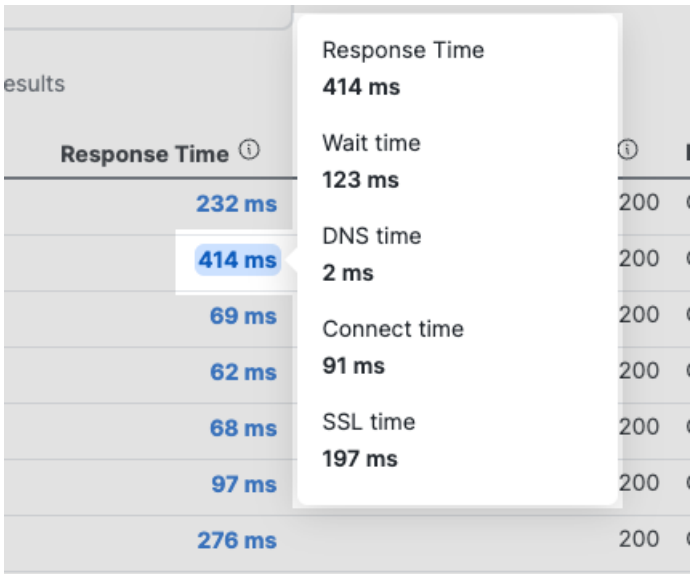
Navigate to: **Experience Insights** > **Insights Management** > **Management**. In the SaaS applications in drop-down menu, select a region. For more information, see Secure Access Regions on page 113.

The table displays the following information for the selected location:

- **Status**: Indicates whether the SaaS application is reachable. Click the **Status** value of a specific application to view a detailed breakdown of traffic flow by phase.



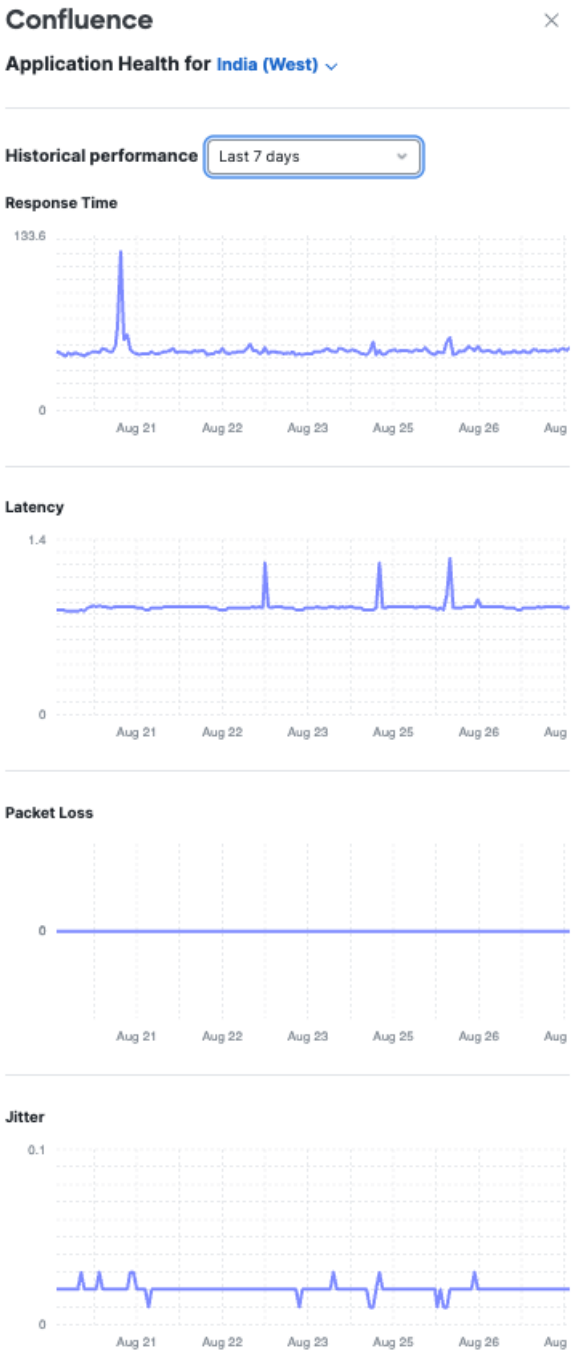
- **Response Time:** The time a SaaS application takes to respond to user requests. High response times can indicate network latency or application inefficiencies. Click the **Response Time** value for a specific application to view a detailed breakdown by Wait time, DNS time, Connect time, and SSL time.



- **Response Code**: Represents the interaction between the client and the server. A successful response code is in the 200-299 range.
- **Description**: Provides the reason for an issue if a SaaS application is not reachable.
- **Latency**: The time a data packet takes to travel from its source to its destination in a network.
- **Jitter**: The variation in delay between data packets transmitted over a network.

- **Loss**: Occurs when data packets transmitted across a network do not reach their destination (packet loss).

Click an **Application name** to open the **Application Health** detail pane. This pane displays the application's historical performance for Response Time, Latency, Packet Loss, and Jitter. You can filter this data by region and historical performance duration (24 hours, 7 days, or 30 days).



View User Dashboard

Provides reference information about View User Dashboard in Cisco Secure Access. The User dashboard displays endpoint activity for a single endpoint, offering end-to-end visibility for efficient troubleshooting and issue diagnosis.

The User dashboard displays endpoint activity for a single endpoint, offering end-to-end visibility for efficient troubleshooting and issue diagnosis.

User Summary

The User summary section includes the User Details, Device Details, Zero Trust Access, and VPN Access.

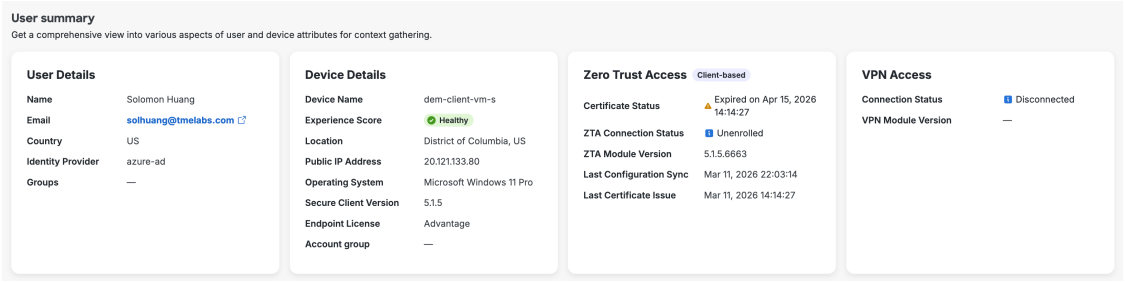
View high-level information about the user and their devices that have the ThousandEyes agent installed and registered with Secure Access.

User Details: Shows the identity information such as the full name, email, country, identity provider name, and associated user groups, if available. User group information is pulled directly from your customer active directory (AD) or identity provider (IDP) integration.

Device Details: shows the relevant information for the end user's device.

Zero Trust Access: shows the status, version, last sync, and certificate issued date.

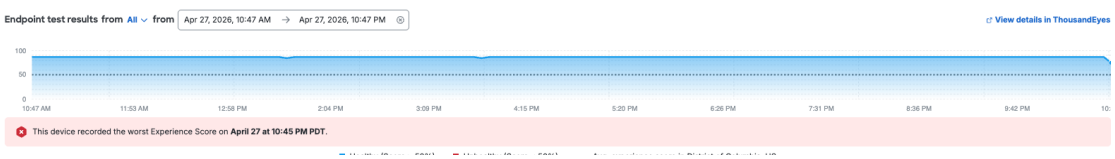
VPN Access: shows connection status and VPN module version.



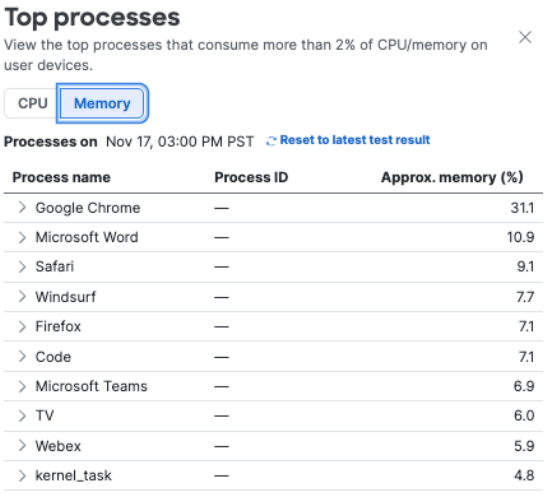
Performance

Performance section shows you in real time the endpoint test results for the endpoint user's data and the application's data. This allows you to form a baseline of what is normal by viewing trends over time and comparing real time performance to previous performance to see any hop-by-hop path anomalies.

- **Endpoint Test Results** drop-down list allows you to select different views for specific endpoint-related data. If you select All then the graph disappears and you only see the Segment visualization section. To see the endpoint and network thresholds see, Endpoint List.
- **Time Range Selector** allows you to set the date to view the data history based on the endpoint's license type. For more information on the test data retention, see Endpoint license usage. The time range selector updates the Endpoint test results graph and the Segment visualization card.
- **Experience score** graph is visible when you select **All** from the Endpoint test results drop-down list. Click on a point in time to see how the endpoint was performing. Time range selector displays up to four days of historical performance data.
- **Endpoint** graph shows the CPU and memory of the device.
- **Application** score on the graph shows the end-to-end metrics including latency, jitter, loss, and response time.
- **Worst Performance Event Timestamp** section is located below the graph. The timestamp shows the date and time when the device experienced its lowest performance. This timestamp is determined by your selected custom date range. If no custom date range is specific, it defaults to showing the worst performance event within the last 12 hours.

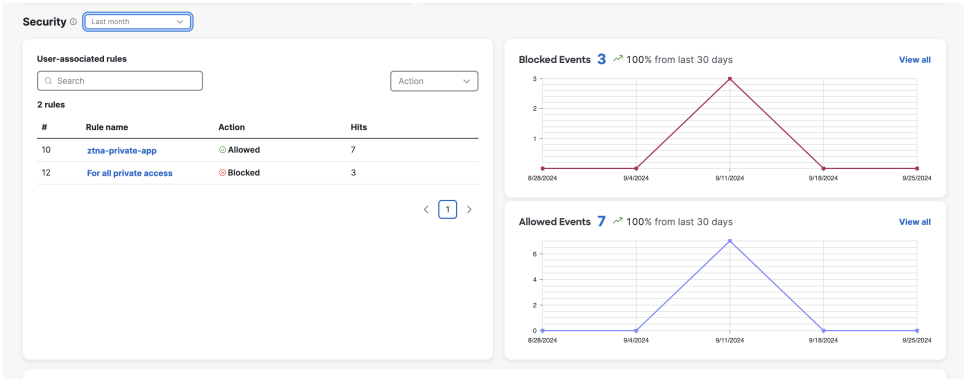


- **Top processes** drawer shows any process using more than 2% of CPU or memory on an endpoint. The displayed processes correspond to the same time frame as the current endpoint test results graph. Click **Top processes** to view more information about different running processes.



Security Events

The section displays the allowed and blocked events that occurred when a user's device attempted to access an organizational resource using Zero Trust Access.



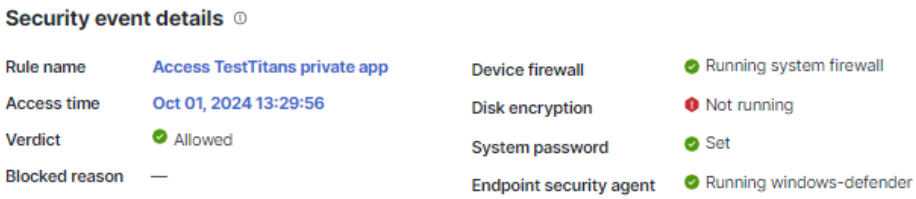
The **User-associated rules** section displays the Zero Trust Access security rules that were triggered by the user's device in a specified period, sorted by descending order of frequency.

- When an event is both allowed and blocked, its user-associated rule displays as two separate entries in the table.

The **Blocked and Allowed Events** graphs display the combined total of blocked and allowed Zero Trust Access events for the user's device within the specified time period.

- To see a comprehensive view of events that are associated with the user, click **View all**.

The **Security event details** section shows information for the security event that was triggered for the user's device most recent attempt to access an organizational resource using Zero Trust Access. For more information, see Add a Client-Based Zero Trust Access Posture Profile on page 1250.



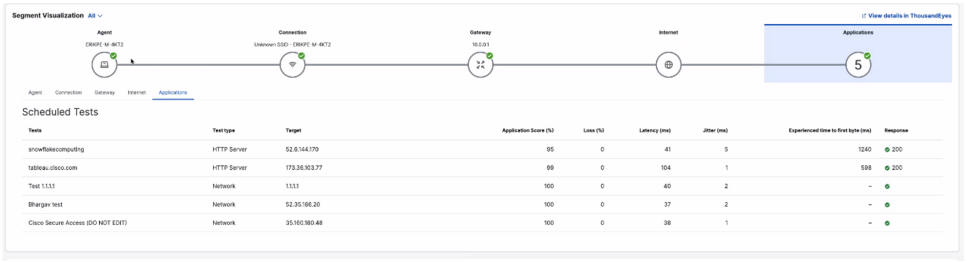
Segment Visualization

The view provides a look at the entire network journey, starting from the agent and ending at the destination, so that you can pinpoint the specific segment that is causing performance degradation. Each segment provides detailed information to troubleshoot underlying network issues.

- Your ThousandEyes license allows for one scheduled test and one dynamic test. Upgrading your license allows for additional tests. For more information about ThousandEyes licenses, see About Endpoint Agent Tests.

By default, the view covers all tests running on the agent. To filter results by test, use the drop-down menu in the top left corner.

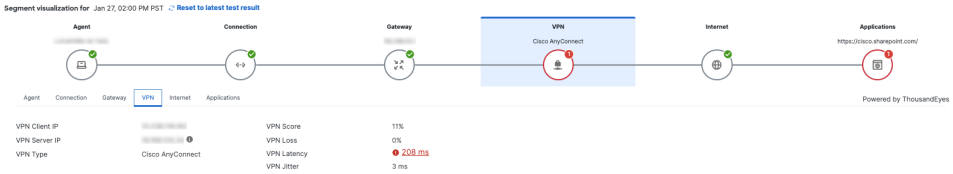
To display the view, click the **Applications** button.



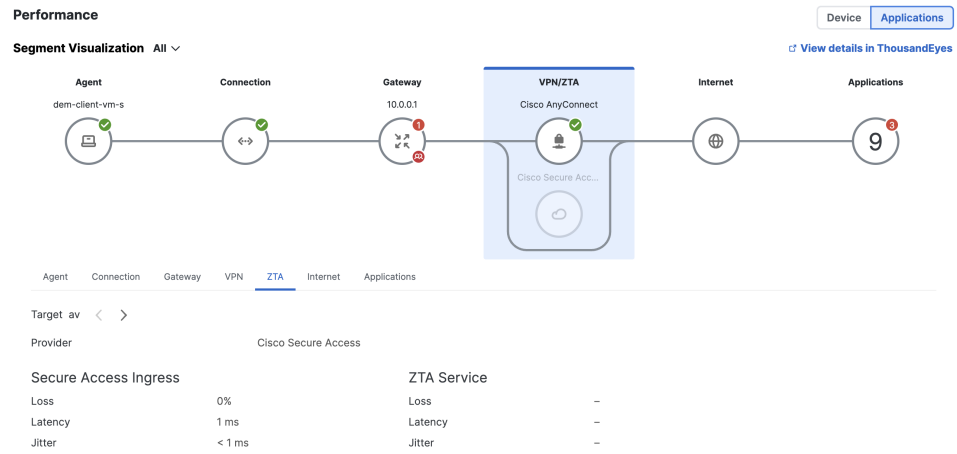
Segment details

- **Agent**–Score is calculated using CPU and memory.
- **Connection**–Score expressed as a percentage, indicates how well the wired or wireless connection is performing.
  - **Wired connection score**–A score of 100% means the link speed is excellent, such as 1 Gbps, reflecting a healthy and reliable connection.
  - **Wireless connection score**–is calculated using different metrics depending on the operating system, focusing on the quality of the wireless network connection. For more information, see Wi-Fi Descriptions.
    - **For Windows**:
      - **Transmit rate**: Data transmission speed between the device and access point. Higher transmit rates generally indicate faster connections.
      - **Frame Retry Rate (FRR)**: The ratio of frames retransmitted to total transmitted frames, indicating wireless transmission reliability.
    - **For MacOS**:
      - **Transmit rate**: Same as Windows.
      - **Signal-to-Noise Ratio (SNR)**: Calculated as RSSI (Received Signal Strength Indicator) minus Noise level, representing signal quality.
- **Gateway**–Score is derived from local network tests to the gateway based on loss, latency, and jitter values.

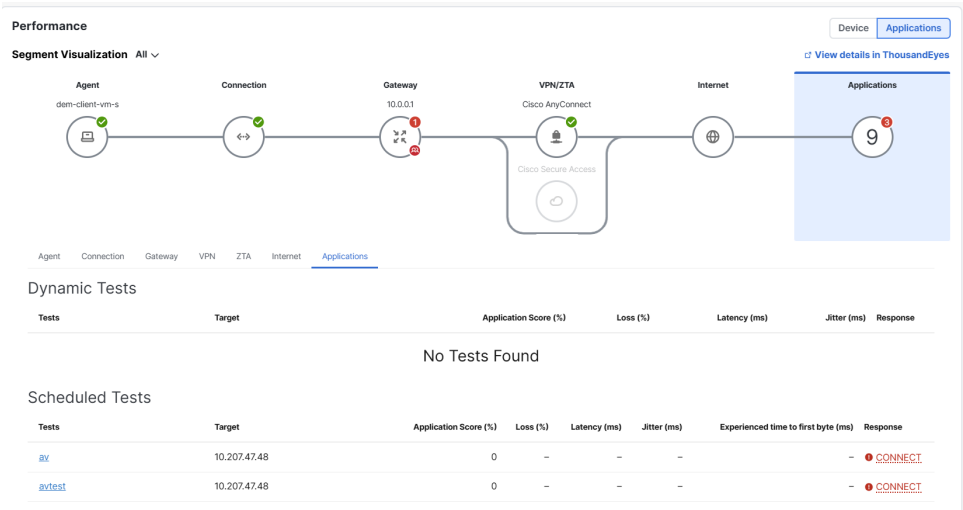
- **VPN**–Score is derived from the local network tests of the VPN that are computed using network metrics including loss, latency, and jitter.



- **ZTA**–Shows performance metrics (loss, latency and jitter) to the Secure Access ingress, which represents the unencrypted path over the internet from the client to the ZTA proxy load balancer. Also view performance metrics to the ZTA service, which represents the encrypted path towards the service.
  - Your ZTA version must be 5.17 or higher, as earlier versions lack the necessary telemetry support. Updating ensures full visibility into the secure access path for better monitoring and troubleshooting.



- **Internet**–Shows the IP addresses that the device data passes through and the delay (similar to how traceroute works).
- **Application**–Score reflects the overall performance of the scheduled or dynamic test that is running for an application. Calculated using loss, latency, jitter, and overall HTTP availability and response time.



View the User Dashboard

Provides instructions for completing the View the User Dashboard workflow in Cisco Secure Access. The ThousandEyes agent must be registered on the end user machine with the account group that is linked to your Experience Insights integration.

Before you begin

The ThousandEyes agent **must** be registered on the end user machine with the account group that is linked to your Experience Insights integration. Registration occurred during onboarding with Experience Insights.

- To register agents that were added after onboarding, see: Configure Experience Insights.

To see data in the Security Events section, the following must be installed on the end user's machine:

- Cisco Secure Client. For information, see Download Cisco Secure Client.
- ThousandEyes. For information, see Set Up Experience Insights.
- Zero Trust Access. For information, see Add a Client-Based Zero Trust Access Posture Profile on page 1250 for client-based ZTA serivces and Add a Browser-based Zero Trust Access Posture Profile on page 1253 for browser-based ZTA services.

Procedure

1. Navigate to: **Experience Insights** > **Endpoints**.
2. In the **Endpoint List** click a user name.

The User dashboard displays.

Configure Identity Providers for Experience Insights

Describes Configure Identity Providers for Experience Insights in Cisco Secure Access. Identity provider configuration integrates your organization's identity sources with Secure Access to enable user-centric monitoring in Experience Insights.

Identity provider configuration integrates your organization's identity sources with Secure Access to enable user-centric monitoring in Experience Insights. This configuration allows the system to map OS-authenticated user identities to ThousandEyes-managed endpoints, providing a comprehensive view of network performance by user rather than by device.

Prerequisites

- **Agent Version:** The ThousandEyes Endpoint Agent must be version 2.13.3 or later.
- **Identity Integration:** Your organization must have an Active Directory (AD) or Identity Provider (IdP) integration configured with Secure Access via SCIM or AD Connector.
- **Supported identity providers:**
  - **Windows:** Active Directory (AD) and Entra ID.
  - **Mac:** Mosyle, JAMF Connect, Enterprise Connect, Kerberos, and Managed Preference.
- **User Domain:** The user must be part of the customer organization domain.
- **Authentication:** The device running the ThousandEyes endpoint agent must have the user logged in and authenticated.

- **Single user sessions:** Devices with multiple users logged in and authenticated at the same time are not supported.

Benefits of Identity Mapping

When you configure your identity provider, Experience Insights uses a translation layer to associate ThousandEyes endpoint data with identity information. This mapping provides several benefits:

- **Correlation of issues by user group:** Isolate connectivity issues to a specific user group to streamline troubleshooting and ensure targeted remediation.
- **Intuitive Troubleshooting:** Search for endpoints using first and last names of a user to identify the correct device across your organization. This approach is more intuitive than using a device name and helps reduce the mean time to resolution for connectivity issues.

Identity Resolution Logic

The name and email displayed in the dashboard are not necessarily based on the currently logged-in user. Instead, the system uses an identifier associated with the device to look up the user in your identity directory.

If a device has more than one possible identifier, the system uses them in the following order:

1. **Zero Trust Access (ZTA) client identity:** Used first, if available.
2. **Cisco Secure Client (RAVPN) identity:** Used next.
3. **Other device records:** Includes records with an identity, such as URC or Umbrella.
4. **Logged-in username:** Used only as a final fallback.

Identity Mapping Considerations

Consider the following behaviors when reviewing identity information:

- **Offline device status:** If an endpoint meets all identity resolution criteria but is currently offline, Secure Access displays the last seen user identity associated with the device.
- **Synthetic test impact:** When a synthetic test is executed, the displayed user identity might update based on the configured test interval and the data collected during that specific test run.

Fallback Behavior

If a device does not meet the identity resolution criteria, Experience Insights defaults to displaying the ThousandEyes username instead of the user's full name.

About Endpoint Agent Tests

Describes About Endpoint Agent Tests in Cisco Secure Access. Secure Access endpoint tests powered by Cisco ThousandEyes simulate the user path to sites and applications using real traffic to gain insights into performance issues.

Secure Access endpoint tests powered by Cisco ThousandEyes simulate the user path to sites and applications using real traffic to gain insights into performance issues. When you onboard Experience Insights and install the ThousandEyes endpoint agent on end user devices, the agent goes where the user goes. This enables synthetic testing that closely matches end user experience.

Manage endpoint tests in Secure Access

Describes Manage endpoint tests in Secure Access. To manage and configure your endpoint licenses, synthetic endpoint tests, and default network and collaboration app tests, log into Secure Access and navigate to Experience Insights > Endpoint tests.

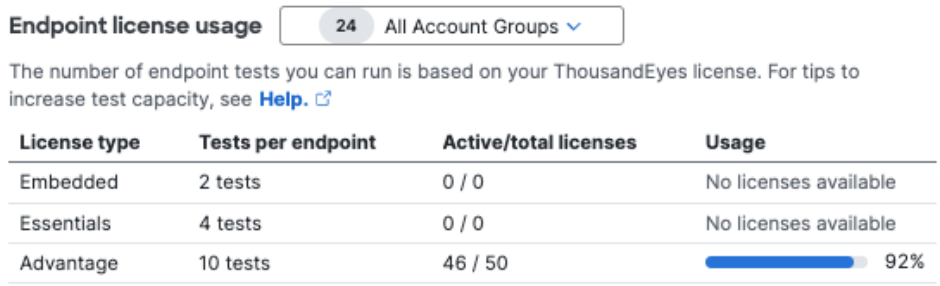
To manage and configure your endpoint licenses, synthetic endpoint tests, and default network and collaboration app tests, log into Secure Access and navigate to **Experience Insights > Endpoint tests**.

Endpoint license usage

Describes Endpoint license usage in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The first table displays your ThousandEyes license usage. You can click on the **All Account Groups** drop-down list to select specific account groups to view their license usage.

Changing the All Account Groups drop-down list does not update the Endpoint tests table.



The number of tests you can run is based on your organization's ThousandEyes license type. The embedded license is assigned by default when you onboard Experience Insights.

License type	Synthetic tests per endpoint	Test data retention
ThousandEyes Endpoint Embedded (default)	2	4 days
ThousandEyes Endpoint Essentials	4	14 days
ThousandEyes Endpoint Advantage	10	30 days

You can run a combination of multiple scheduled and dynamic tests at a time. If you exceed the number of allowed tests, ThousandEyes uses a mechanism to determine which tests should run on a given agent. For information, see Assigning tests to an Endpoint Agent.

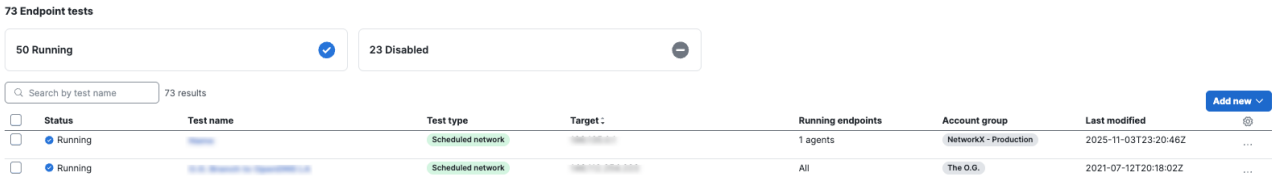
For more information about ThousandEyes licensing, see ThousandEyes Endpoint Agent Licensing.

Endpoint tests

Describes Endpoint tests in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The second table lists your running and disabled tests. In the table you can:

- Search by test name.
- Filter by test type: All test types, Network, or HTTP.
- View all ThousandEyes created tests and tests created in Experience Insights, or only view Experience Insights tests.

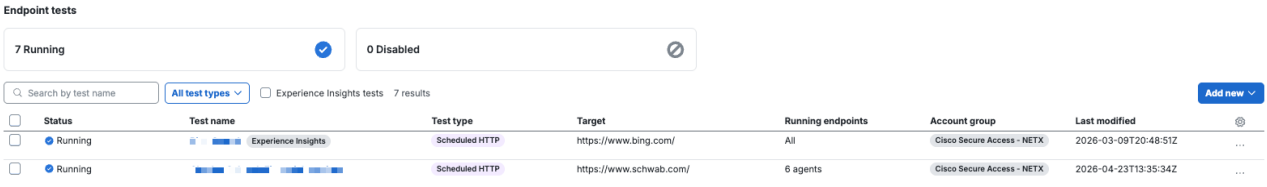


Click a test name to view **Endpoint test results**. For more information, see View HTTP Server Test Results and View Network Test Results.

Click **Add new** to configure a new synthetic test. For more information, see Create HTTP Server Tests and Create Network Tests.

Account Group: Shows all the account groups that the Endpoint tests are configured in. (This option appears only when you have multiple ThousandEyes account groups selected in Account Management.)

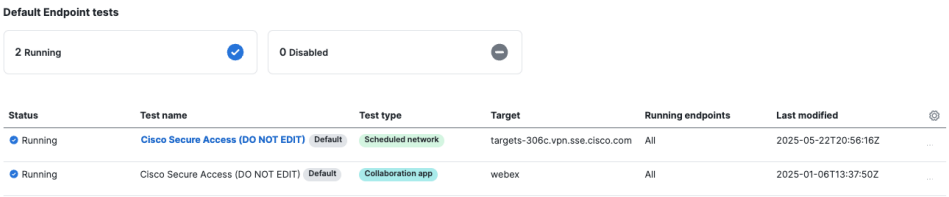
Select one or more table rows to delete, disable, or enable tests.



Default Endpoint tests

Describes Default Endpoint tests in Cisco Secure Access. The third table lists the default network and collaboration app tests that you configured during Experience Insights onboarding.

The third table lists the default network and collaboration app tests that you configured during Experience Insights onboarding. For more information, see Onboard Experience Insights and Configure Experience Insights.



Manage endpoint agents and tests in ThousandEyes

Describes Manage endpoint agents and tests in ThousandEyes in Cisco Secure Access. Additional options are available in the ThousandEyes dashboard.

Additional options are available in the ThousandEyes dashboard.

- You can configure alerts for specific tests. For more information, see Alerts.
- You can adjust test priority for each endpoint agent. For more information, see Test Priority.
- You can reallocate a license to another endpoint. For more information, see Assigning licenses to Agents.
- For more information about managing synthetic endpoint tests in ThousandEyes, see Managing Synthetic Tests.

Limitations

Describes limitations for synthetic endpoint tests in Cisco Secure Access. A single synthetic test is limited to a maximum of 150,000 endpoint agents.

A single synthetic test is limited to a maximum of 150,000 endpoint agents.

Estimate Peak Traffic to Custom Targets for Default Endpoint Tests

Describes Estimate Peak Traffic to Custom Targets for Default Endpoint Tests in Cisco Secure Access. Endpoint tests sent to custom targets (whether public or private) require bandwidth.

Endpoint tests sent to custom targets (whether public or private) require bandwidth. A high number of endpoint agents sending synthetic traffic to a custom target can generate network throughput high enough to negatively impact custom target performance.

Before selecting a custom target for a default endpoint test, we recommend using the traffic calculator to estimate peak throughput. Use that estimate to ensure your network and server have the capacity to handle peak throughput. You can also use mitigation strategies described below to attempt to reduce peak throughput.

Calculate Estimated Peak Throughput of Test Traffic

Describes Calculate Estimated Peak Throughput of Test Traffic in Cisco Secure Access. Estimated peak throughput of test traffic is an estimate of the upper limit of bandwidth required in the event that the default test runs for all endpoint agents at at the same time.

Estimated peak throughput of test traffic is an estimate of the upper limit of bandwidth required in the event that the default test runs for all endpoint agents at at the same time. At the default test interval of 1 minute, actual test throughput will be at or near estimated peak throughput. At higher test intervals, actual test throughput may not be as high as estimated peak throughput, but this is not guaranteed.

Estimated peak throughput = A x N

- A = Agent throughput for a single test (in KB/s). Peak throughput is 1 KB/s per endpoint agent.
- N = Number of endpoint agents, assuming one synthetic test per agent to the same custom target. By default, all endpoint agents are included in the default test.

Consult with internal teams (IT, network, or firewall administrators) to compare the results to your network and server capacity to ensure that your systems can withstand the load.

> **Note**
>
> **Estimated Peak Throughput Calculation Example**
>
> A = 1 KB/s
>
> N = 1000 agents
>
> Peak throughput: A x N = 1,000 KB/s (1 MB/s)

Mitigation Strategies

Describes Mitigation Strategies in Cisco Secure Access. Follow these strategies to mitigate default test throughput that exceeds your available bandwidth.

Follow these strategies to mitigate default test throughput that exceeds your available bandwidth.

- Change the default test target (RAVPN, Zero Trust Access, or SWG remote module) or custom target that is more capable of managing the load.
- Increasing the test interval may mitigate impact on your network. At the default test interval of 1 minute, actual throughput will be at or near estimated peak throughput. Increasing the interval will likely redistribute the tests over the longer interval.

> **Note**
>
> It is not possible to predict actual throughput at test intervals greater than 1 minute. In the worst case scenario, if all endpoint agent tests run at the same time (for example, at minute 30 of a 30-minute test interval), they would still generate actual throughput at or near estimated peak throughput.

- Increase the capacity of your backhauling infrastructure.
  - If using IPsec tunnels, provision traffic backhauling over your edge infrastructure that is capable of handling increased traffic load.
  - If using resource connectors, add additional connectors to resource connector groups to increase the ability to handle the traffic load.

Recovery Options

Describes Recovery Options in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

If your system crashes or becomes unavailable due to high traffic sent to a custom target, do the following:

- For public targets: The SaaS provider may block traffic that is sent from Cisco IP addresses. The traffic may mimic the characteristics of a distributed denial-of-service (DDoS) attack, potentially disrupting legitimate user access by overloading system resources. Contact Cisco support.
- For private targets: Seek assistance from your IT or network administration team.

Create HTTP Server Tests

Describes Create HTTP Server Tests in Cisco Secure Access. HTTP server tests measure the response time and generate the response code of a web server.

HTTP server tests measure the response time and generate the response code of a web server. They are compatible with VPN and ZTA destinations.

Prerequisites

- Endpoints must have requisite permissions to access the test's target application. For more information, see Manage Access Policies.
- Endpoints must meet testing capacity requirements. For more information, see Endpoint Agent Licensing.

Zero Trust Access prerequisites:

- Endpoints must meet Zero Trust Access posture-profile requirements. For more information, see Manage Zero Trust Access Posture Profiles.
- End users must be enrolled in Zero Trust Access and must be signed into their OS.
- **Strongly recommended:** When testing private resources, turn off the user-authentication interval to prevent end users from receiving unexpected notifications. You must turn off the user authentication globally and for the specific HTTP server test. For more information, see: Rule Defaults: Default Settings for Access Rules and Network Requirements for Zero Trust Access.
- Your ZTA version must be 5.17 or higher, as earlier versions lack the necessary telemetry support. Updating ensures full visibility into the secure access path for better monitoring and troubleshooting.

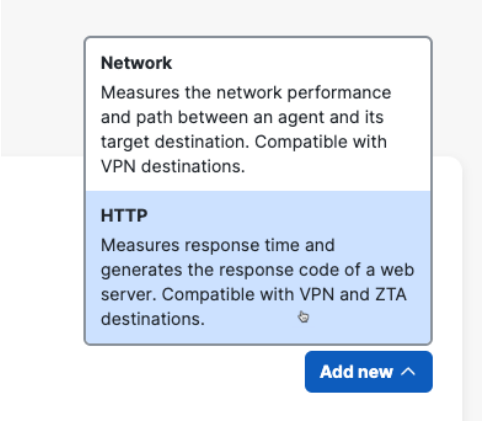
Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. Strongly recommended: Before running large-scale tests, run a test with a small subset of agents to ensure that your network can support the test traffic between Secure Access and your on-premise environment.

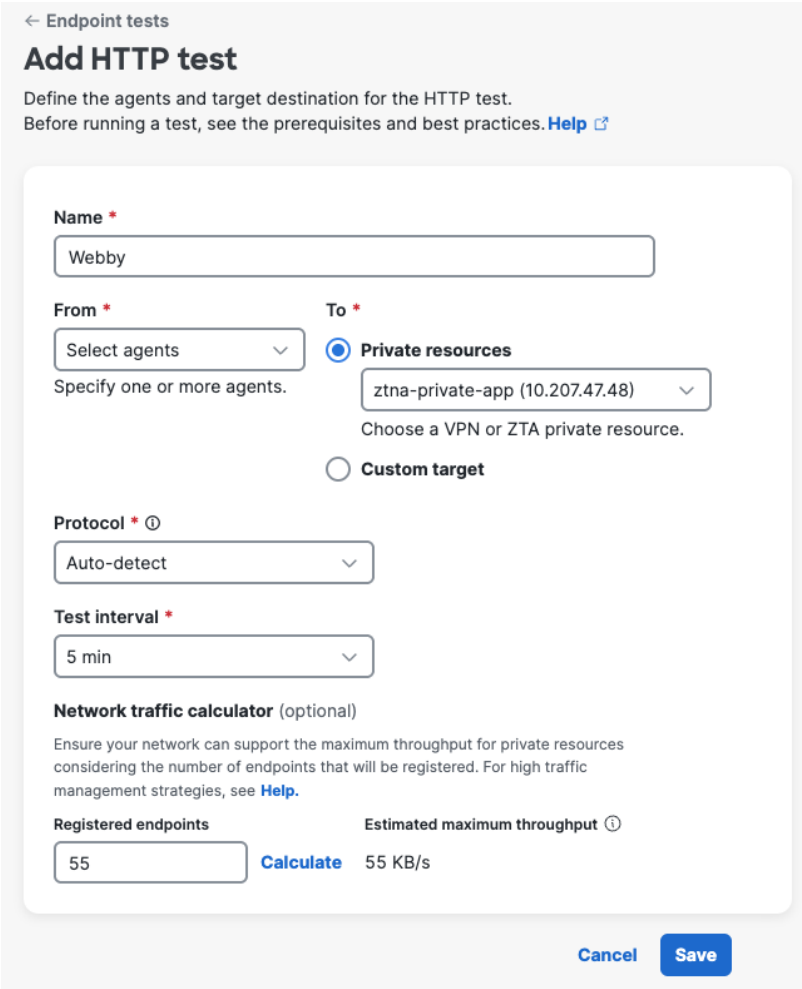
Strongly recommended: Before running large-scale tests, run a test with a small subset of agents to ensure that your network can support the test traffic between Secure Access and your on-premise environment.

Procedure

1. In Secure Access, navigate to **Experience Insights** > **Insights Management** > **Endpoint tests**.
2. Above the Endpoint tests table, click **Add new** > **HTTP**.



3. Define the agents and target destination under **Add HTTP test**.



- **Name** –Enter a name that identifies the agent-to-server test (such as target domain name or IP address).
- **From** –Specify by location, account groups, specific agents, or device type. You can also select between different account groups.
  - If you select all agents from a given location, the test will be associated with the agents that are currently present for that location.
  - If a new agent becomes available for the location when the test is run, the agent won't be included in the test. To add the new location, create a new test or clone the existing test.
  - Regardless of which group of agents you choose, the test itself will always be stored in your default account group for easy, centralized access.
  - Device type: Windows and macOS are supported.
  - A single synthetic test is limited to a maximum of 150,000 endpoint agents.
- **To**
  - **Private resource**: Choose an IP address from the drop-down. VPN and ZTA are supported.
  - **Custom target**: Specify a Web URL.
- **Protocol**:
  - **Auto-detect**–The default and recommended option. Auto-detect tries several probes to identify the best test method for the device's current network conditions.

- **ICMP**
- **ICMP + TCP Connect**–Enables a TCP connection with a 10-second timeout and closes the connection if it is unable to connect. Unsuccessful connections count towards the TCP-connection failures metric.
- **Prefer TCP (ICMP fallback)**
- **TCP**

- **Test interval**–Select the frequency of the test run.
- The **Network traffic calculator** is available to help you ensure your network can support the maximum throughput for private resources considering the number of endpoints that will be registered.
  - The calculator assumes all endpoints run the test at the same time. Actual testing may distribute network traffic over the test interval configured above.
  - For high traffic management strategies, see Estimate Peak Traffic to Custom Targets for Default Endpoint Tests.

4. Click **Save test**.

Important

Before running large-scale tests, run a test with a small subset of agents to ensure that your network can support the test traffic between Secure Access and your on-premise environment.

Create Network Tests

Describes Create Network Tests in Cisco Secure Access. Network synthetic tests measure the network performance and path between an agent and its target destination.

Network synthetic tests measure the network performance and path between an agent and its target destination. They are compatible with VPN destinations. The destination can be an IP address or a domain name.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. Endpoints must have requisite permissions to access the test's target application.

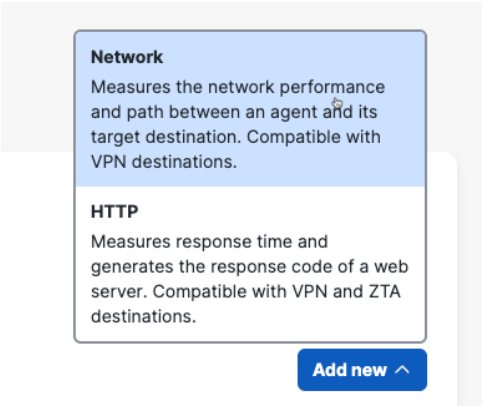
Before you begin

- Endpoints must have requisite permissions to access the test's target application. For more information, see Manage Access Policies.
- Endpoints must meet testing capacity requirements. For more information, see Endpoint Agent Licensing.

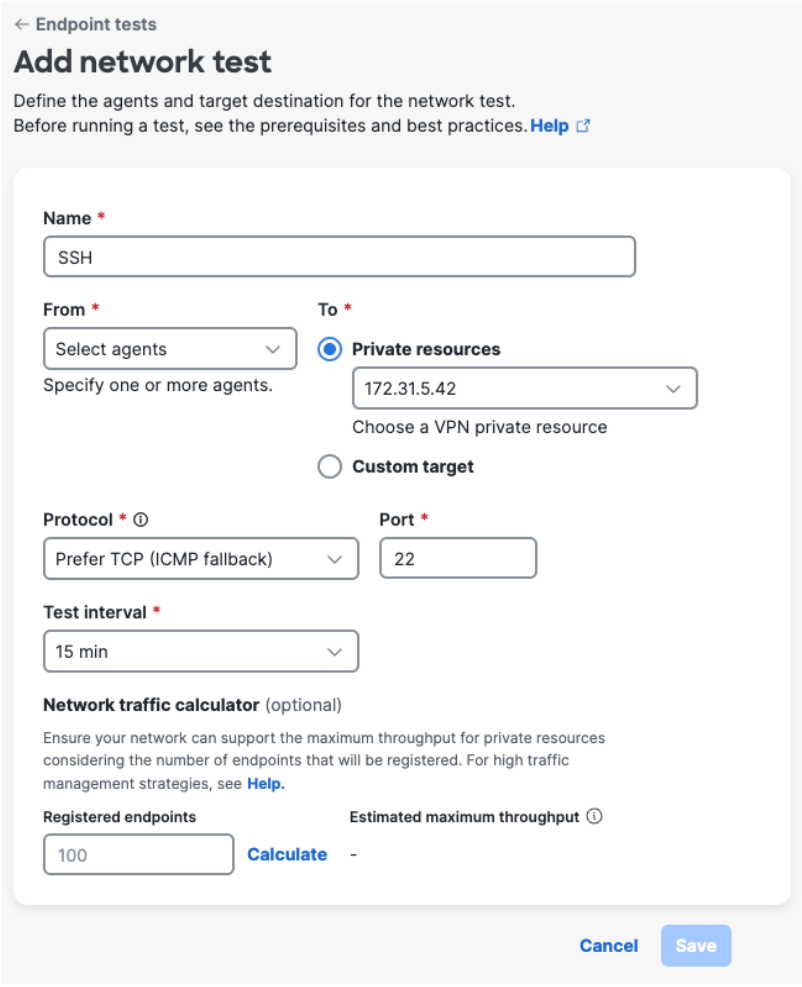
Procedure

---

1. In Secure Access, navigate to **Experience Insights** > **Insights Management** > **Endpoint tests**.
2. Above the Endpoint tests table, click **Add new** > **Network**.



3. Define the agents and target destination under **Add network test**.



- **Name**–Enter a name that identifies the agent-to-server test (such as target domain name or IP address).
- **From**–Specify by location, account groups, specific agents, or device type. You can also select between different account groups.
  - If you select all agents from a given location, the test will be associated with the agents that are currently present for that location.
  - If a new agent becomes available for the location when the test is run, the agent won't be included in the test. To add the new location, create a new test or clone the existing test.

- Regardless of which group of agents you choose, the test itself will always be stored in your default account group for easy, centralized access.
- Device type: Windows and macOS are supported.
- A single synthetic test is limited to a maximum of 150,000 endpoint agents.

- **To**
  - **Private resource**: Choose an IP address from the drop-down. Only VPN is supported.
  - **Custom target**: Specify an IP address or Web URL.
- **Protocol**:
  - **Auto-detect**–The default and recommended option. Auto-detect tries several probes to identify the best test method for the device's current network conditions.
  - **ICMP**
  - **ICMP + TCP Connect**–Enables a TCP connection with a 10-second timeout and closes the connection if it is unable to connect. Unsuccessful connections count towards the TCP-connection failures metric.
  - **Prefer TCP (ICMP fallback)**
  - **TCP**
- **Port**:
  - The field will auto-populate for configured ports. For non-configured resources and resources that have multiple ports, enter the port number(s).
  - If you entered a custom target, accept the default value or leave the field blank.
- **Test interval**–Select the frequency of the test run.
- The **Network traffic calculator** is available to help you ensure your network can support the maximum throughput for private resources considering the number of endpoints that will be registered.
  - The calculator assumes all endpoints run the test at the same time. Actual testing may distribute network traffic over the test interval configured above.
  - For high traffic management strategies, see Estimate Peak Traffic to Custom Targets for Default Endpoint Tests.

4. Click **Save test**.

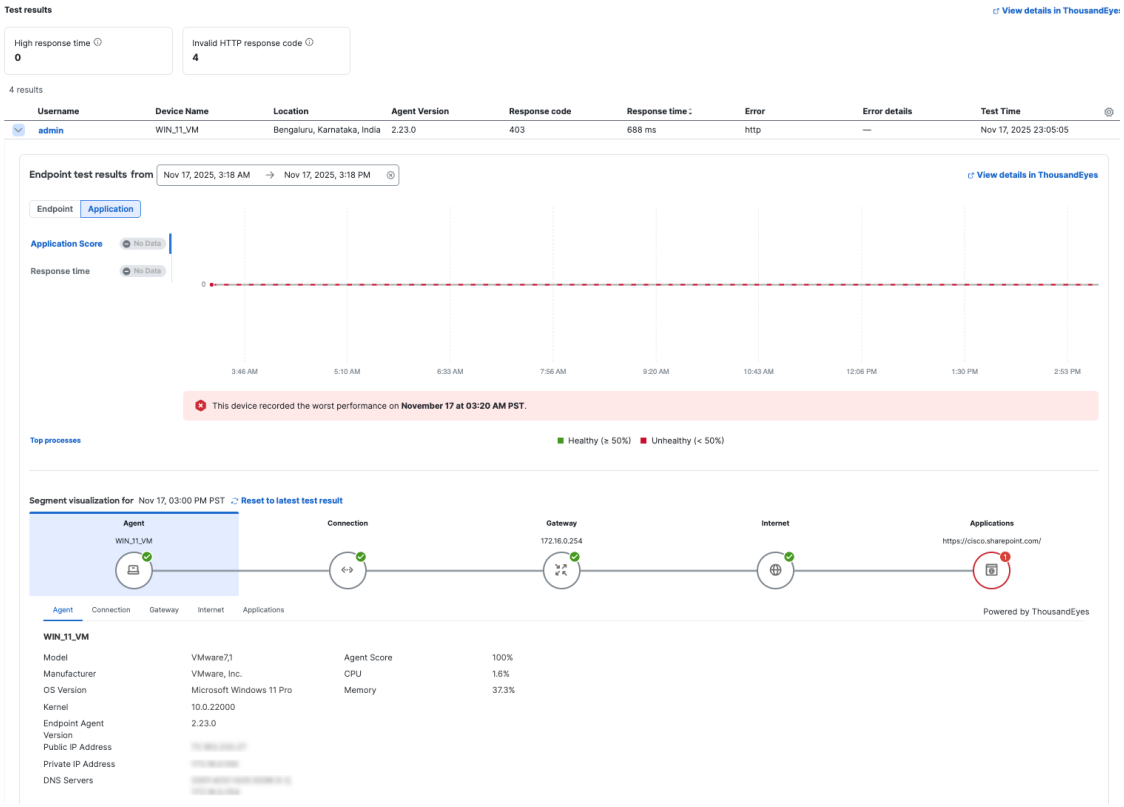
Important

Before running large-scale tests, run a test with a small subset of agents to ensure that your network can support the test traffic between Secure Access and your on-premise environment.

View HTTP server test results

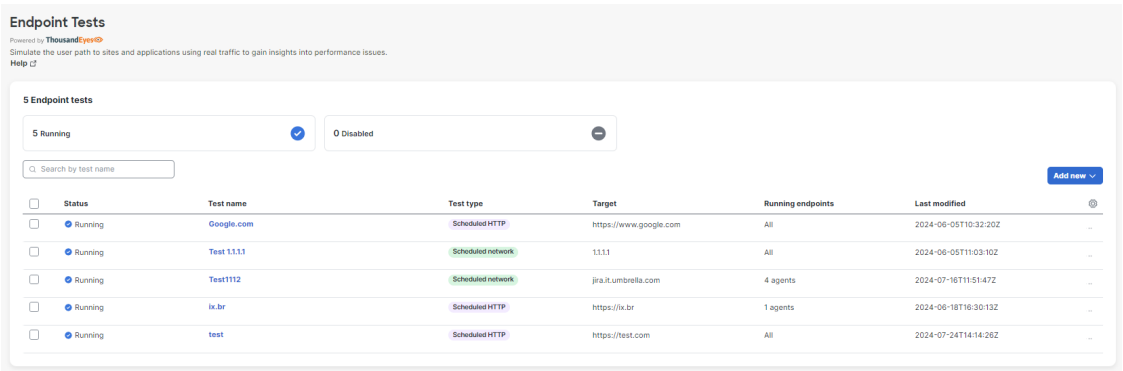
View response time, response code, and error details for scheduled HTTP server endpoint tests to help you monitor application availability and troubleshoot failures.

The **Endpoint Test Results** page displays the response time and response code for HTTP server tests, as well as error types and details for failed tests.

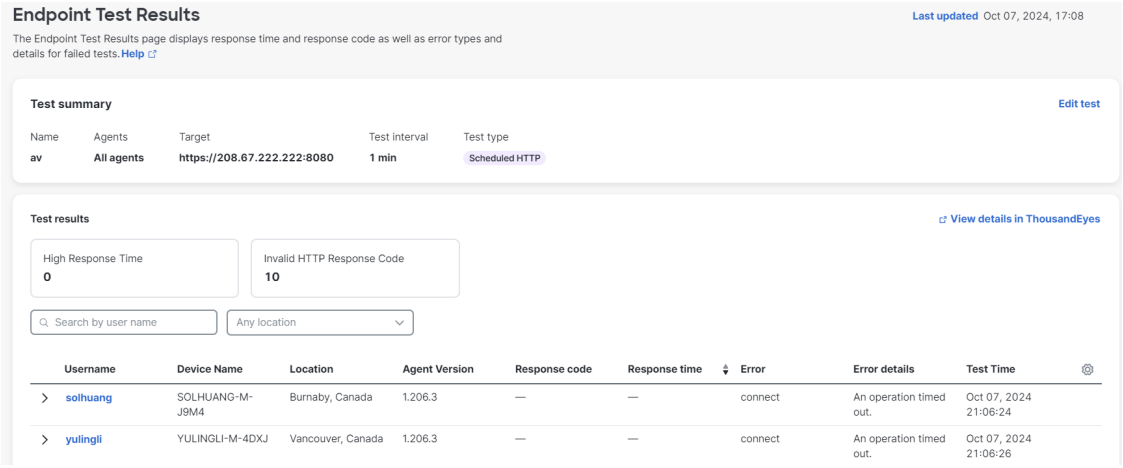


Procedure

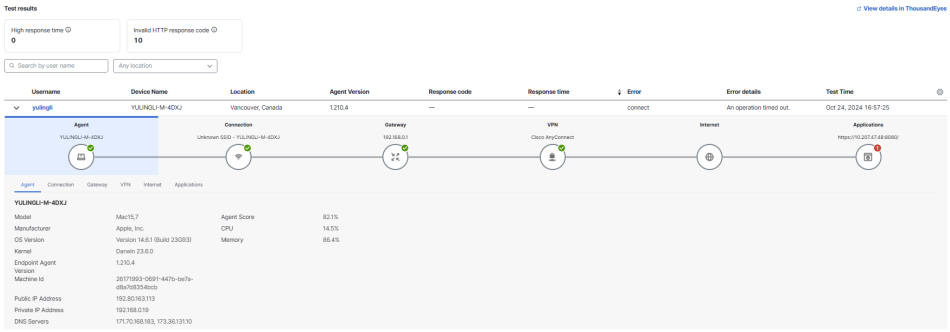
1. Go to **Experience Insights** > **Insights Management** > **Endpoint tests**.
2. On the **Endpoint Tests** page, click a scheduled HTTP server test (identified in the **Test type** column).



3. View the aggregated results for the test.
   - **Response code**–Indicates the interaction between the client and the server. A successful response code falls within the 200–299 range.
   - **Response time**–The time it takes for a request sent by the testing agent to receive a response from the target application server.



4. To view HTTP test results for a specific endpoint, click the down arrow next to the username to display the device path to the target destination.



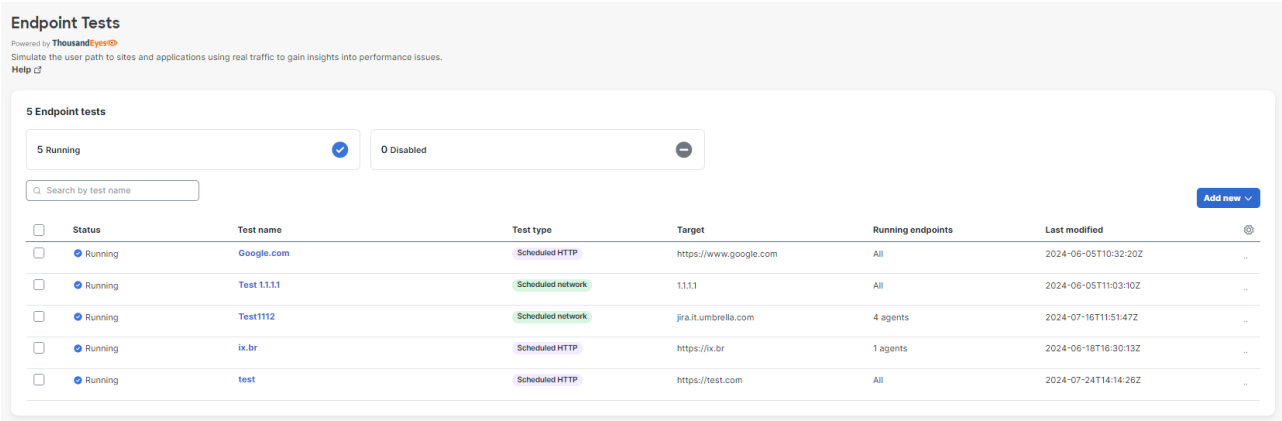
View Network Test Results

Provides instructions for completing the View Network Test Results workflow in Cisco Secure Access. The Endpoint Test Results page displays the quality of the test's network connection represented by key metrics including latency, packet loss, and jitter.

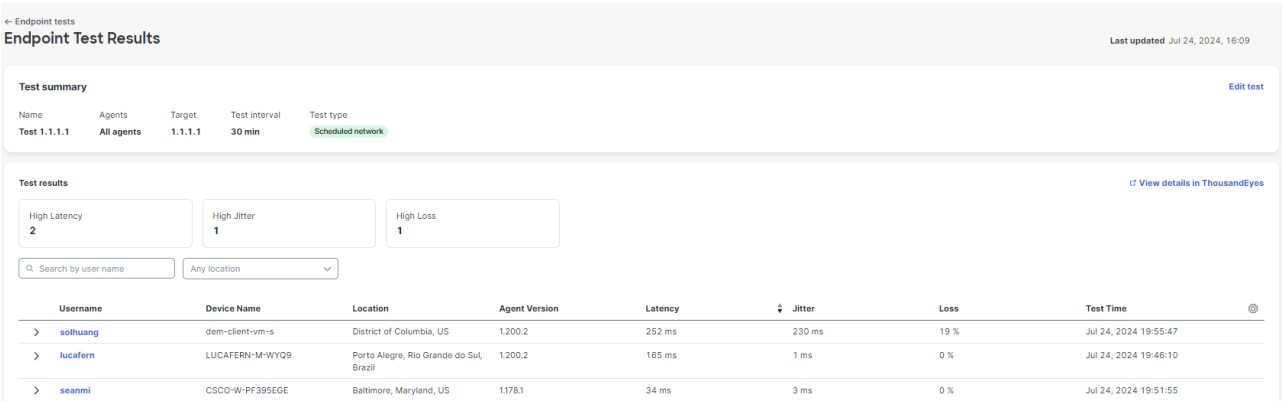
The Endpoint Test Results page displays the quality of the test's network connection represented by key metrics including latency, packet loss, and jitter.

Procedure

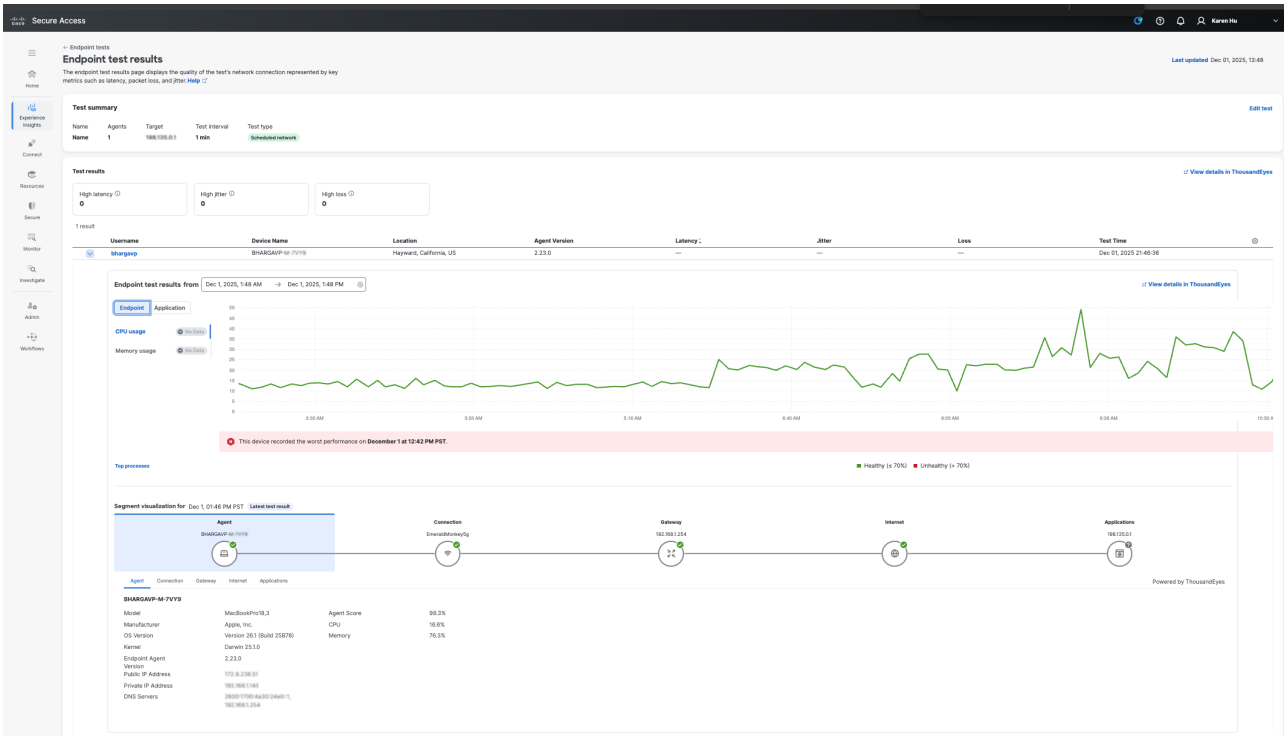
1. Navigate to: **Experience Insights** > **Endpoint tests**.
2. On the Endpoint Tests page, click a scheduled network test (denoted in the **Test type** field).



3. On the Endpoint Test Results page, view the results:
   - **Latency**–High network latency is 150ms or above.
   - **Jitter**–High jitter is 40ms or above.
   - **Loss**–High packet loss is 20 percent or above.



4. Click the down arrow next to a username to view the **Endpoint test results**, and **Segment visualization** for the device path to the target destination.


Secure Access
Endpoint test results
Test summary
Test results
Endpoint test results from
Segment visualization for
BHARGAVP-M-7VY9

68 Logging

Topics:

- Manage Logging
- Log Formats and Versioning

Provides an overview of Logging in Cisco Secure Access, including Manage Logging and Log Formats and Versioning. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Logging

Describes Manage Logging in Cisco Secure Access and explains Where are Logs Stored, Logging to the Secure Access Data Warehouse, and Logging to Amazon S3. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access allows for the logging of events and traffic. You can configure Secure Access to save these logs to either the United States or Europe. Logs can be saved to your own or a Cisco Managed S3 bucket.

Only event data is stored in a data warehouse. This is any data that might appear in a Secure Access report. Configuration data, such as audit logs and policy settings, remain stored by Cisco in California regardless of a change to the data warehouse's location.

Secure Access logs are CSV-formatted, compressed (gzip), and saved every 10 minutes. For more information, see Log Formats and Versioning.

Note

For Experience Insights, the process for managing ThousandEyes logs is not the same as the Secure Access logs. When you deploy the ThousandEyes agent, your account (that includes your logs) is provisioned by default to the data center in the United States. To move your account to the data center in Europe, contact support@thousandeyes.com.

Where are Logs Stored?

When you create a policy, activity logs are by default saved to the North America - California, US location of the Secure Access data warehouse. You can change the location of the data warehouse to Europe at any time. For more information, see Change the Location of Event Data Logs.

You can also optionally configure logging so that logs are also stored to an Amazon S3 bucket—either your own or one managed by Cisco.

Logging to the Secure Access Data Warehouse

The Secure Access data warehouse is the virtual location where your instance of Secure Access stores its event data logs. By default, Secure Access saves your event data logs to Cisco's California location; however, you can change the location of the data warehouse from North America to Europe at any time. For more information, see Change the Location of Event Data Logs.

Logging to Amazon S3

As well as storing logs to one of its data warehouses, Secure Access can store logs to an Amazon S3 bucket.

By having your logs uploaded to an S3 bucket, you can then automatically download logs so that you can keep them in perpetuity in backup storage outside of the Secure Access data warehouse storage system. Saving to an S3 bucket also gives you the ability to ingest logs through your SIEM or another security tool. This can help you determine if any security events in your Secure Access logs coincide with events in other security tools.

Secure Access Amazon S3 options:

- A self-managed bucket—You own the Amazon S3 bucket, including its configuration and management.
- A Cisco-managed bucket—Cisco Secure Access owns the bucket and sets the configuration and management of it.

Advantages and Disadvantages of Configuring a Cisco-Managed Bucket

- Easy to set up and manage.

- Secure Access supports the rotation of the S3 bucket key every 90 days.
- Included with your Secure Access license.
- You cannot add anything to your S3 bucket besides log files from Secure Access. You cannot use your Cisco-managed S3 bucket for any other application.
- Some SIEM integration types may require advanced privileges for the user accessing the S3 bucket (beyond the basic Read permissions) and as such, may not work with this feature.
- You cannot get support from Amazon directly for advanced configuration assistance, such as automation or help with the command line.
- Data can only be stored offline for a maximum of 30 days.

Enable Logging on a Rule in Access Policy

Provides instructions for completing the Enable Logging on a Rule in Access Policy workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

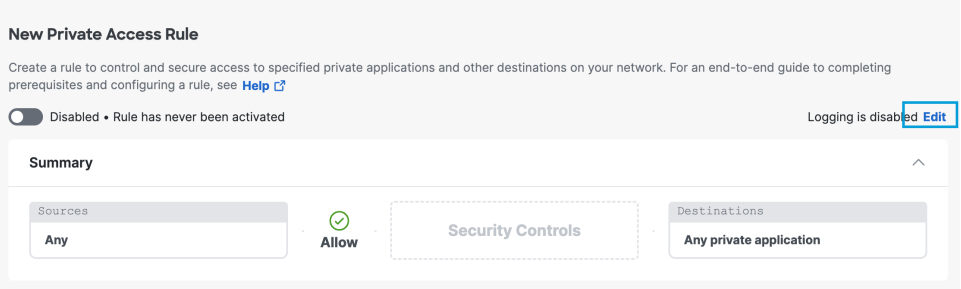
Configure the logging of events and traffic for an access rule in the Access policy. By default, logging is disabled. Logging can be enabled or disabled at any time for any rule.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

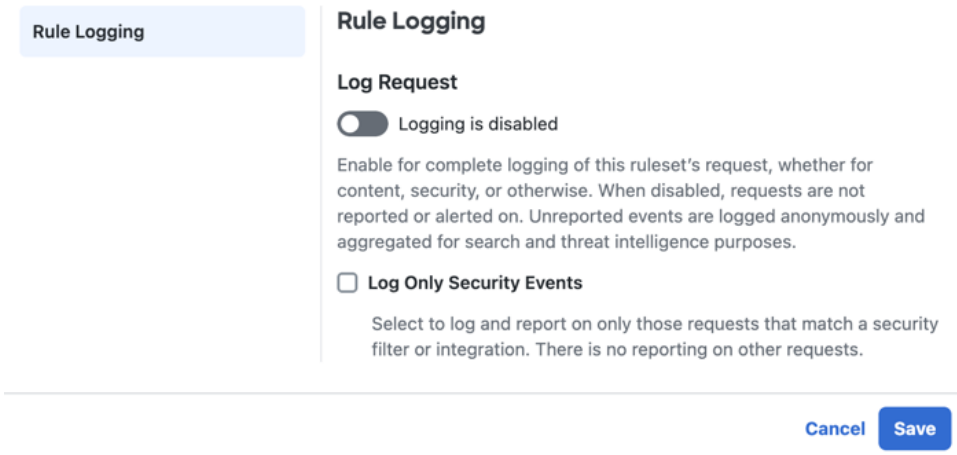
Procedure

1. Navigate to **Secure** > **Access Policy**.
2. Click **Add Rule** > **Private Access** or **Add Rule** > **Internet Access** , or in the access rules table, click the name of an access rule and then click **Edit**.



3. At the top of the page, navigate to **Logging is enabled** or **Logging is disabled**, and then click **Edit**.
   a) For **Log Request**, enable or disable logging for the access rule.
      Secure Access logs all events and requests from the sources to the destinations defined in the access rule.
   b) Click **Log Only Security Security Events**.
      Secure Access logs only the requests from the sources to the destinations defined in the access rule that match a security filter or integration.

> **Note**
>
> If you disable logging for an access rule, Secure Access cannot log the requests and other events to the Activity Search report.



Enable Logging to Your Own S3 Bucket

Describes Enable Logging to Your Own S3 Bucket in Cisco Secure Access. You can configure Secure Access to log events to an Amazon S3 bucket that you manage.

You can configure Secure Access to log events to an Amazon S3 bucket that you manage. To enable logging to a self-managed Amazon S3 bucket, follow the prerequisite steps to set up an AWS account and create an Amazon S3 bucket. Once you have created an S3 bucket in Amazon, configure Secure Access to use it for the storage of logs.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- A login to Amazon AWS service (http://aws.amazon.com/console/). If you don't have an account, Amazon provides free sign-up for S3.

> **Note**
>
> Amazon requires a credit card in case your usage exceeds free plan usage.

- A bucket configured in Amazon S3 to be used for storing logs. For more information, see Amazon's S3 documentation.

> **Note**
>
> Periods in S3 bucket names and Object Lock in S3 buckets are not supported.

JSON Bucket Policy

When you set up your Amazon S3 bucket, you must add a bucket policy that accepts uploads from Secure Access. Copy the following preconfigured JSON and substitute your S3 bucket name for `bucketname`. Then, paste the Secure Access S3 bucket policy into your Amazon S3 bucket policy.

```
{
  "Version": "2008-10-17",
  "Statement": \[
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucketname/*"
    },
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::bucketname/*"},
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::bucketname"
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::bucketname"
    }
  \]
}
```

Configure Your Own S3 Bucket

Provides instructions for completing the Configure Your Own S3 Bucket workflow in Cisco Secure Access. Navigate to Admin Log Management Set up cloud storage and click on the Amazon card.

> **Note**
>
> You must first configure a bucket in Amazon S3. For more information, see Amazon's S3 documentation.

Procedure

1. Navigate to **Admin** > **Log Management** > **Set up cloud storage** and click on the **Amazon** card.
2. In the **Amazon** field, type or paste the exact bucket name you created in Amazon S3 and click **Verify**.

   Secure Access verifies your bucket, connects to it, and saves a README_FROM_UMBRELLA.txt file to your bucket.
3. Open the `README_FROM_UMBRELLA.txt` file that Secure Access saved to your bucket, copy the token listed in it, paste it into the **Token Number** field, and click **Save**.
4. A summary page shows you the bucket name. Click **Done**.

   A pop-up window appears when verification is successful and your Amazon S3 bucket is now connected.

Integrate AWS S3 Bucket with Splunk App

Describes Integrate AWS S3 Bucket with Splunk App in Cisco Secure Access. You can integrate your self-managed AWS S3 bucket with the Cisco Cloud Security App for Splunk.

You can integrate your self-managed AWS S3 bucket with the Cisco Cloud Security App for Splunk. Use the data path to your AWS S3 bucket to set up the integration.

The S3 bucket data path consists of the following components:

```
<AWS S3 bucket name>-<AWS region>/<AWS S3 bucket directory prefix>
```

where,

- **AWS S3 bucket name and AWS region**–the name of your AWS S3 bucket, followed by a dash (-), and the **AWS region**.
- **AWS S3 bucket directory prefix**–the directory prefix (customer folder name) to the AWS S3 bucket.

Sample S3 Bucket Data Path

```
my_company_name-us-west-1/dnslogs
```

Use the data path to your self-managed S3 bucket to:

- Download log files using the AWS CLI.
- Integrate your AWS S3 bucket with the Cisco Cloud Security App for Splunk. The Cisco Cloud Security App for Splunk enables you to analyze your Secure Access logs that are stored in your AWS S3 bucket. For more information, see Cisco Cloud Security App for Splunk.

Download Files Locally From the S3 Bucket

Describes Download Files Locally From the S3 Bucket in Cisco Secure Access. You can use the Amazon Command Line Interface (CLI) to download files from a self-managed S3 bucket to your local directory.

You can use the Amazon Command Line Interface (CLI) to download files from a self-managed S3 bucket to your local directory.

Prerequisites

- Install the AWS CLI to your system.

To download files, run the following command. If you want to test the command without syncing files, add the `--dryrun` flag.

AWS CLI command syntax:

```
aws s3 sync s3://DATAPATH /path/to/local/directory/
```

Detailed sample command:

```
aws s3 sync s3://mycompany-us-west-1/dnslogs
/opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Enable Logging of DLP Violation Evidence to Your Own S3 Bucket

This concept explains the capability to log Data Loss Prevention (DLP) violation evidence files to an Amazon S3 Bucket.

Secure Access allows you to store Data Loss Prevention (DLP) violation evidence files in an Amazon S3 bucket you manage. This feature enables direct access to the actual files that triggered DLP violations. It helps you audit, investigate, and comply with regulatory requirements more easily. With this capability, you can view full violation files. The files are securely stored in your S3 bucket with a unique naming structure to avoid conflicts and ensure traceability.

Note

- This feature is available only for organizations using a custom certificate. Cisco Support must enable it on a per-organization basis. It is not supported for organizations using a shared certificate, due to potential security vulnerabilities.
  - A custom certificate is required only for logging Web DLP violation evidence to your own Amazon S3 bucket. Endpoint DLP, Email DLP, and SaaS API DLP violation events continue to be logged to your S3 bucket without a custom certificate.
  - Web DLP violation evidence logging is not supported for organizations using a shared certificate (Secure Access Root Cert), due to potential security vulnerabilities. Endpoint DLP, Email DLP, and SaaS API DLP violation events continue to be logged to your S3 bucket.
- You must grant the IAM role provided by Cisco Secure Access the necessary permissions for DLP violation evidence logging to access and write files to your S3 bucket.
- When enabling this feature, Secure Access verifies the connectivity of your S3 bucket by attempting to write a test file. If unsuccessful, an error message will be displayed in the UI.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- An AWS account. Sign up for free at http://aws.amazon.com/console/.

> **Note**
>
> Amazon requires a credit card if your usage exceeds the limits of the free plan.

- An Amazon S3 bucket configured for storing DLP violations. You must first configure a bucket in Amazon S3. For more information, see The Amazon S3 documentation.

> **Note**
>
> Periods are not supported in the names of S3 bucket and Object Lock settings.

Procedure

To enable logging of DLP violation evidence to your S3 bucket, perform these steps:

1. Configure the IAM policy for your S3 bucket
2. Configure your S3 bucket

Configure IAM Policy for S3 Bucket

Use this task to configure IAM Policy for an S3 Bucket by creating a production KMS key, setting permissions, and applying necessary encryption and access settings.

Set up your Amazon S3 bucket by adding a bucket policy that enables Secure Access for uploading violation files using the specific IAM role provided.

Grant the necessary permissions to the IAM role (dlp-evidence) provided by Cisco for Secure Access to verify and upload files to your bucket. Refer to the sample bucket policy in the documentation. Substitute your bucket name and account details.

Procedure

1. Create a production KMS key.

```
aws kms create-key --description "KMS key for bucket_name" --profile
[YOUR-PROFILE]
```

> **Note**
>
> Save the Key ID from the output, for example, `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.

2. Create a production KMS key alias.

```
aws kms create-alias --alias-name alias/[bucket_name] --target-key-id
[PROD-KMS-KEY-ID] --profile [YOUR-PROFILE]
```

3. Apply the production KMS key policy.
   Create the policy file at this location:

```
/tmp/prod-kms-policy.json
```

> **Note**
>
> You may use Amazon S3-managed encryption (SSE-S3). However, we strongly recommend using AWS KMS with a customer-managed key (CMK) for tighter access control and auditing.

The KMS key policy applies only when you use a CMK. It is not required for S3-managed encryption as shown below. In the KMS key policy, replace `YOUR-ACCOUNT-ID` with the customer account ID.

```
{
  "Version":  "2012-10-17",
  "Statement":  [
    {
      "Sid":  "Enable IAM User Permissions",
      "Effect":  "Allow",
      "Principal":  {
        "AWS":  [
            "arn:aws:iam::{YOUR-ACCOUNT-ID}:root",
        ]
      },
      "Action":  "kms:*",
      "Resource":  "*"
      },
      {
        "Sid":  "Allow DLP Violations Role to Encrypt",
        "Effect":  "Allow",
        "Principal":  {
            "AWS":  "arn:aws:iam::050208289548:role/dlp-evidence"
        },
        "Action":  [
          "kms:GenerateDataKey",
          "kms:Encrypt",
          "kms:DescribeKey",
          "kms:CreateGrant"
        ]
        "Resource":  "*"
      }
  ]
}
```

To apply the KMS key policy, execute the command:

```
aws kms put-key-policy --key-id [PROD-KMS-KEY-ID] --policy-name default
--policy file:///tmp/prod-kms-policy.json --profile [YOUR-PROFILE]
```

4. Create a production S3 Bucket.

```
aws s3api create-bucket --bucket [bucket_name] --region us-west-2
--create-bucket-configuration LocationConstraint=us-west-2 --profile
[YOUR-PROFILE]
```

5. Enable encryption on the production bucket using full key ARN.

```
aws s3api put-bucket-encryption --bucket [bucket_name]
--server-side-encryption-configuration
'{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"aws:kms","KMSMasterKeyID":"arn:aws:kms:us-west-2:[YOUR-ACCOUNT-ID]:key/[PRO-KMSKEY-ID]"}}]}'
 --profile [YOUR-PROFILE]
```

6. Enable versioning for the production bucket.

```
aws s3api put-bucket-versioning --bucket [bucket_name]
--versioning-configuration Status=Enabled --profile [YOUR-PROFILE]
```

7. Block public access to the production bucket.

```
aws s3api put-public-access-block --bucket [bucket_name]
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
 --profile [YOUR-PROFILE]
```

8. Apply the production bucket policy.

   Copy the following preconfigured JSON and replace `bucket_name` with your S3 bucket name and replace `YOUR_ACCOUNT_ID` with your account ID. Insert the Secure Access S3 bucket policy into your Amazon S3 bucket policy.

```
{
  "Version":  "2008-10-17",
  "Statement":  [
    {
      "Sid": "AllowRootAccountFullAccess",
      "Effect": "Allow",
      "Principal":  {
        "AWS":  "arn:aws:iam::[YOUR-ACCOUNT-ID]:root"
        },
      "Action":  "s3:*",
      "Resource":  [
          "arn:aws:s3:::{bucket_name}",
          "arn:aws:s3:::{bucket_name}/*"
        ]
      },
      {
        "Sid":  "AllowUploadLocationAndList",
        "Effect":  "Allow",
        "Principal":  {
          "AWS":  "arn:aws:iam::050208289548:role/dlp-evidence"
      },
      "Action":  [
          "s3:PutObject",
          "s3:DeleteObject",
          "s3:GetEncryptionConfiguration",
          "s3:GetBucketLocation",
          "s3:ListBucket",
          "s3:GetBucketAcl"
      ],
      "Resource":  [
          "arn:aws:s3:::{bucket_name}",
          "arn:aws:s3:::{bucket_name}/*"
      ]
    },
    {
      "Sid":  "DenyGetObjectFromViolationServiceRole",
```

```
      "Effect":  "Deny",
      "Principal":  {
        "AWS":  "arn:aws:iam::050208289548:role/dlp-evidence"
        },
      "Action":  "s3:GetObject",
      "Resource":  "arn:aws:s3:::{bucket_name}/*"
    }
  ]
}
```

To apply the bucket policy, execute the command:

```
aws s3api put-bucket-policy --bucket [bucket_name] --policy
file:///tmp/prod-bucket-policy.json --profile [YOUR-PROFILE]
```

9. Verify if the bucket policy is correctly applied by executing these commands:

```
aws s3api head-bucket --bucket [bucket_name] --profile [YOUR-PROFILE]
aws s3api get-bucket-policy --bucket [bucket_name] --profile [YOUR-PROFILE]
aws s3api get-bucket-encryption --bucket [bucket_name] --profile [YOUR-PROFILE]
```

Configure Your Own S3 Bucket

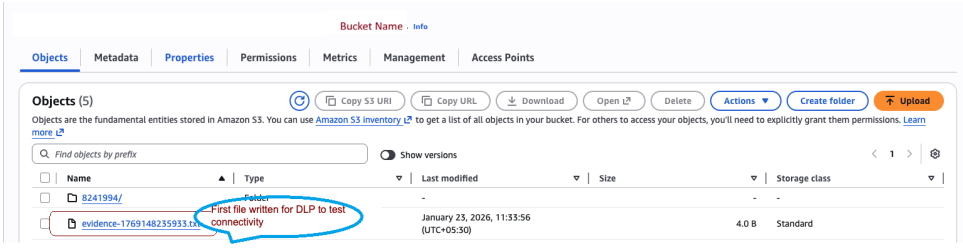
Use this procedure to set up your organization-managed S3 bucket for storing DLP violation evidence files.

Before you begin
Ensure that an Amazon S3 bucket has been created for your organization.

Procedure

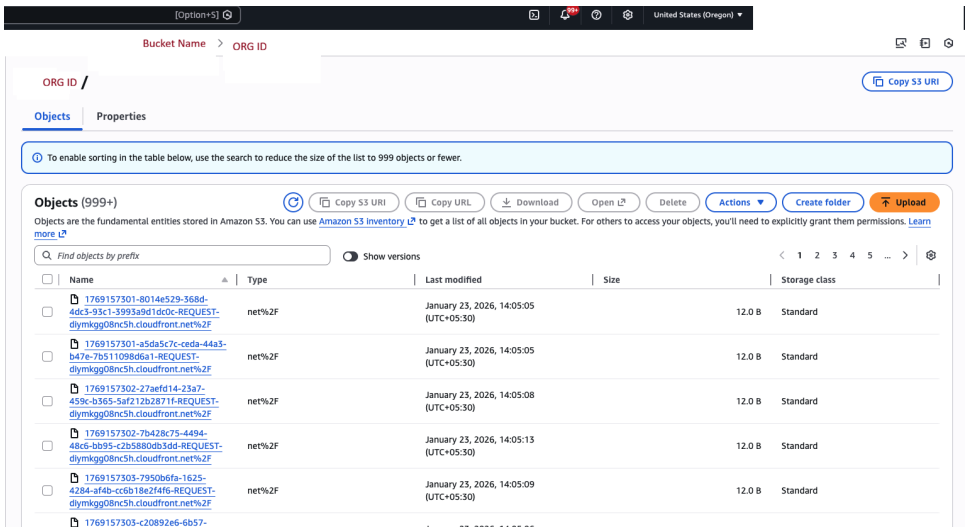
---

1. Navigate to **Admin** > **Log Management**. In the **DLP Violation Evidence** card, select **Configure**.
2. In the **Amazon S3 Bucket** field, enter the bucket name you created in Amazon S3 and click **Verify**.
   a. Secure Access attempts to verify and connect to your bucket.
   b. A test file is created in the S3 bucket to validate connectivity and permissions.



   c. After successful validation, a confirmation message will be displayed.

3. After successful verification, you can view the folder structure in your S3 bucket. The organization folder structure uses the org ID as a prefix to store DLP violation evidence files.



The S3 bucket is configured and validated to store DLP violation evidence files.

Integrate AWS S3 Bucket with Splunk App

This concept explains how to integrate AWS S3 bucket with the Splunk App.

Integrate your AWS S3 bucket with the Cisco Cloud Security App for Splunk using the S3 bucket data path.

Components of S3 Bucket Data Path

The components of the S3 bucket data path are:

```
<AWS S3 bucket name>-<AWS region>/<AWS S3 bucket directory prefix>
```

- **AWS S3 bucket name and AWS region**–the name of your AWS S3 bucket, followed by a dash and the **AWS region**.
- **AWS S3 bucket directory prefix**–the directory prefix (customer folder name) in the AWS S3 bucket.

Sample S3 Bucket Data Path

An example of a sample S3 bucket data path is:

```
my_company_name-us-west-1/dnslogs
```

Use the S3 bucket data path to:

- Download log files using the AWS CLI.
- Integrate your AWS S3 bucket with the Cisco Cloud Security App for Splunk. The Cisco Cloud Security App for Splunk enables you to analyze Secure Access logs stored in your AWS S3 bucket. For more information, see Cisco Cloud Security App for Splunk.

Download Files Locally From the S3 Bucket

This concept explains how to download files from an S3 bucket using the AWS CLI command.

You can use the Amazon Command Line Interface (CLI) to download files from a self-managed S3 bucket to your local directory.

Prerequisites

Before downloading files from the S3 bucket, ensure that AWS CLI is installed on your system.

To download files from the S3 bucket, run the AWS CLI command.

```
aws s3 sync s3://DATAPATH /path/to/local/directory/
```

> **Note**
>
> Use the `--dryrun` flag to test the command without syncing files.

An example of an AWS CLI command is:

```
aws s3 sync s3://mycompany-us-west-1/dnslogs
/opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Troubleshooting

This concept explains the error conditions and successful scenarios you may encounter during S3 bucket configuration for enabling the DLP Violation Evidence feature.

When you configure a S3 bucket to enable the DLP Violation Evidence feature, you may encounter one of these error conditions.

- **Bucket not found**

  When the S3 bucket cannot be found during configuration, the UI displays the message: "We are unable to find the bucket. Please check the bucket path and try again."

- **IAM permissions error**

  If the IAM permissions are not properly configured for write access, the UI displays the message: "IAM permissions are not properly configured for write access. Please check your bucket policy."

- **KMS key policy error**

  If the KMS key policy is not properly configured, the UI displays the message: "An unexpected error occurred during verification. Please try again or contact support."

- **Successful configuration**

  When the bucket is properly configured, the UI displays the message: "We are sending data to your Amazon S3 bucket storage."

Enable Logging to a Cisco-Managed S3 Bucket

Describes Enable Logging to a Cisco-Managed S3 Bucket in Cisco Secure Access. You can configure Cisco Secure Access to log events to an Amazon S3 bucket, which is managed by Cisco.

You can configure Cisco Secure Access to log events to an Amazon S3 bucket, which is managed by Cisco.

Cisco configures all Cisco-managed buckets to use Amazon Server-Side Encryption with S3-Managed Keys (SSE-S3, AES-256). The encryption and keys are managed by Amazon. Cisco and the Secure Access user account (customer) don't exchange keys, but the data is still encrypted at rest. More information about S3 buckets and encryption is available on the Amazon website by searching for "SSE-S3, AES-256".

Secure Access provides access to Cisco-managed S3 buckets using Amazon's IAM system. When the S3 bucket is provisioned, Secure Access provides the S3 bucket's key and secret in the **Admin** > **Log Management** page.

You must copy your S3 bucket key credentials to your environment. Secure Access does not store your keys during the generation process. If you lose your keys, you can not recover them. Instead, you must rotate the keys in Secure Access.

A Cisco user account can write files to the S3 bucket, and the customer IAM user can read from the S3 bucket. A customer IAM user can rotate their keys at any time.

> **Note**
>
> Customer logs are also encrypted in transit between Cisco's log management infrastructure and Amazon S3.

Best Practices for Rotating an S3 Bucket Key

Describes Best Practices for Rotating an S3 Bucket Key in Cisco Secure Access. Beginning on May 15, 2025, Secure Access organizations must rotate their IAM key credentials for a Cisco-managed S3 bucket every 90 days.

Beginning on May 15, 2025, Secure Access organizations must rotate their IAM key credentials for a Cisco-managed S3 bucket every 90 days. If a Cisco-managed S3 bucket key expires, Secure Access autorotates the IAM key and continues to log events to the S3 bucket. To access the S3 bucket, the organization must regenerate the IAM key for the Cisco-managed S3 bucket. For more information, see Rotate Keys on a Cisco-Managed S3 Bucket.

> **Note**
>
> Rotating IAM keys every 90 days only applies to Cisco-managed S3 buckets not self-managed S3 buckets.
>
> If your organization is unable to rotate the IAM key credentials for the Cisco-managed S3 bucket, we recommend that you use a self-managed S3 bucket.

About the Notifications for the IAM Key

- Secure Access provides periodic notifications to an organization when the IAM key for a Cisco-managed S3 bucket expires. Secure Access sends email notifications to the email account that was used during the initial purchase or renewal of your Cisco Secure Access license.
- An organization can view notifications about the expired IAM key on the **Overview** page in Secure Access. After the organization successfully rotates the IAM key for the Cisco-managed S3 bucket, Secure Access removes the IAM key notifications on the **Overview** page.

Configure a Cisco-Managed S3 Bucket

Provides instructions for completing the Configure a Cisco-Managed S3 Bucket workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

In Secure Access, create a Cisco-managed Amazon S3 bucket to store the event logs for the organization.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management** > **Set up cloud storage** > click **Cisco**.
2. Select a **Region** and a **Retention Duration**.
   - Select a **Region**–Regional endpoints are important to minimize latency when downloading logs to your servers.

The regions that are listed match those available in Amazon S3. Not all regions are available.

Pick a region that is closest to you. If you wish to change your region in the future, you will need to delete your current settings and start over.

- Select a **Retention Duration**–Select 7, 14, or 30 days. Beyond the selected time period, all data will be purged and cannot be retrieved.

  We recommend a smaller time period if your ingestion cycle is regular. The retention duration can be changed at any time.

3. Click **Save**.

   Secure Access activates its ability to export to an AWS S3 account. When activation is complete, the Amazon S3 Summary page appears.

4. Copy credentials from this page and store them in a safe place.

   This is the only time that the **Access** and **Secret** keys are made available to you. These keys are required to access your S3 bucket and download logs. If you lose these keys, they must be regenerated.

5. Once keys are copied and safe, click **Done**.

Rotate Keys on a Cisco-Managed S3 Bucket

Provides instructions for completing the Rotate Keys on a Cisco-Managed S3 Bucket workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Rotate the IAM keys on the Cisco-managed S3 bucket for the organization. For more information, see Best Practices for Rotating an S3 Bucket Key

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

---

1. In Secure Access, navigate to **Admin > Log Management**.
2. Click **Regenerate Keys**.
3. Click **Regenerate Keys** to confirm and update the IAM key on the Cisco-managed S3 bucket.
4. Copy the updated key and secret to your environment.

What to do next

> **Note**
>
> After you regenerate the IAM keys on the Cisco-managed S3 bucket, copy the S3 bucket keys to any systems that integrate with the event logs from the Cisco-managed S3 bucket.

Get the S3 Bucket Data Path

Provides instructions for completing the Get the S3 Bucket Data Path workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

The Secure Access Amazon S3 page provides a summary of the configured Cisco-Managed S3 bucket including the data path to your Amazon bucket.

Use the data path to your Cisco-managed S3 bucket to:

- Download log files with the AWS CLI.
- Set up your Cisco-managed S3 bucket with the Cisco Cloud Security App for Splunk. The Cisco Cloud Security App for Splunk enables you to analyze your Secure Access logs found in your AWS S3 bucket. For more information, see Cisco Cloud Security App for Splunk.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. In Secure Access, navigate to **Admin > Log Management**, click **Manage**.
2. Navigate to **Data Path**.

   The data path to your Amazon bucket is composed of several fields.

```
<AWS S3 bucket name>-<AWS region>/<AWS S3 bucket directory prefix>
```

   - **AWS S3 bucket name and AWS region**–the name of the AWS S3 bucket managed by Cisco (`cisco-managed`), a dash (-), and the **AWS region**.
   - **AWS S3 bucket directory prefix**–the directory prefix (customer folder name) to the Cisco-managed AWS S3 bucket.

   Sample S3 Bucket Data Path

```
cisco-managed-us-west-1/2069997_6ff2802af17337def701c2e7816cf14913zf848a
```

Verify Your Access to an S3 Bucket

Provides instructions for completing the Verify Your Access to an S3 Bucket workflow in Cisco Secure Access. To run the Amazon command-line interface (CLI) locally, install the AWS CLI in your environment.

To verify that you have access to a Cisco-managed S3 Bucket, you can configure the AWS CLI with your newly generated keys.

Before you begin

- To run the Amazon command-line interface (CLI) locally, install the AWS CLI in your environment. For information about installing the AWS CLI, see the Amazon S3 documentation.

Procedure

1. In a shell, run `aws configure`.

```
AWS Access Key ID [None]\: <Enter Your Generated Access Key>
AWS Secret Access Key [None]\: <Enter Your Generated Secret Key>
Default region name [None]\: <Enter Your S3-Bucket Region>
Default output format [None]\:
```

2. List one of the saved logs in your Cisco-managed S3-Bucket.

   For example, run:

```
aws s3 ls s3://cisco-managed-us-west-1/<org_id>/<s3-bucket-instance>/dnslogs
 -recursive
```

```
aws s3 ls s3://cisco-managed-us-west-1/<org_id>/<s3-bucket-instance>/auditlogs
 -recursive
```

Download Files Locally From the Cisco-Managed S3 Bucket

Describes Download Files Locally From the Cisco-Managed S3 Bucket in Cisco Secure Access. You can use the Amazon command-line interface (CLI) to download files from a Cisco-managed S3 bucket to your local directory.

You can use the Amazon command-line interface (CLI) to download files from a Cisco-managed S3 bucket to your local directory.

Run the AWS CLI to download your files from a Cisco-managed S3 bucket to your local directory. To run the AWS CLI command in test mode (without syncing files), use the `--dryrun` flag.

AWS CLI command syntax:

```
aws s3 sync s3://DATAPATH/ /path/to/local/directory/
```

> **Note**
>
> You must append a forward slash (**/**) to the `DATAPATH`.

Sample Command

```
aws s3 sync
s3://cisco-managed-us-west-1/2069997_6ff2802af17337def701c2e7816cf14913zf848a/
 /opt/splunk/etc/apps/TA-cisco_umbrella/data/
```

Best Practices: Download Files From the Cisco-Managed S3 Bucket

- When you download files from a Cisco-managed S3 bucket, ensure that you only download one copy of each log file. If you download log files multiple times, Cisco reserves the right to suspend the download of logs from a Cisco-managed S3 bucket (through the rotation of keys or other methods).
- Once files are downloaded to a local directory, you can delete the files. Only delete files that are older than the **Retention Duration** value configured in Secure Access. Otherwise, the next sync command will download the deleted files again.

Migrate From Cisco S3 Bucket to Your Own S3 Bucket

Provides instructions for completing the Migrate From Cisco S3 Bucket to Your Own S3 Bucket workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

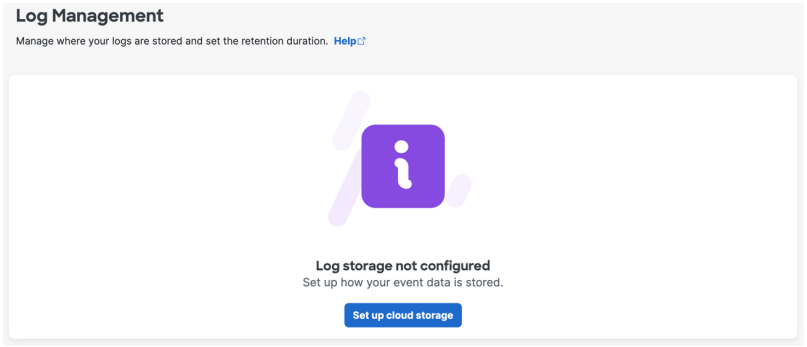
Migrate the logging of events from a Cisco-managed S3 bucket to your own Amazon S3 bucket.

Before you begin

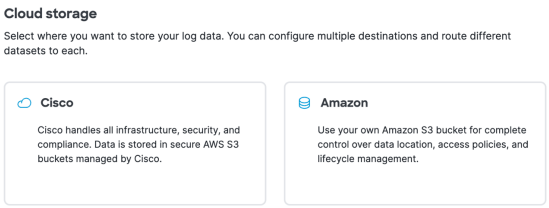
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**.
2. Download your log files in the Cisco-managed S3 bucket to your environment.
   For more information, see Download Files Locally From the Cisco-Managed S3 Bucket.
3. Stop logging events to the Cisco managed S3 bucket.
   For more information, see Stop Logging .
   a) Click **Stop Logging**.
   b) Click **Stop logging data** to confirm your request.
4. To remove the storage for the Cisco-managed S3 bucket, click **Delete Storage**.
5. Configure the logging of events to your own Amazon S3 bucket.
   For more information, see Enable Logging to Your Own S3 Bucket
   a) Navigate to **Admin** > **Log Management**.
   b) Click **Set up cloud storage**.



   c) Click **Amazon** and then configure your Amazon S3 bucket in Secure Access.



Change the Location of Event Data Logs

Provides instructions for completing the Change the Location of Event Data Logs workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

By default, Secure Access saves event data logs to its California data warehouse location. You can change the location of the data warehouse for your organization from North America to Europe at any time.

Only event data is stored in the data warehouse. This is any data that might appear in a Secure Access report. Configuration data, such as audit logs and policy settings, remain stored by Cisco in California regardless of a change to the data warehouse's location.

Implications When You Change Data Warehouse Locations

When you change the location of the data warehouse from North America to Europe or Europe to North America, the data that your reports use changes. Because Secure Access' reports use the data saved to logs that are stored to the data warehouse, only data from the data warehouse's current location is available to reports. Existing logs do not change locations. Data stored in North America stays in North America. Data stored in Europe stays in Europe. To generate reports using data from the previous data warehouse location, you must change the data warehouse location back to the previous location.

> **Caution**
>
> Although you can change back from the European data warehouse location to the North American data warehouse location, we do not recommend this procedure. Changing back and forth between data warehouse locations results in the splitting of your Secure Access event data between locations. This splitting lessens the accuracy of your Secure Access reports. We strongly recommend that once you change the location of your data warehouse from North America to Europe that you do not change back unless the change back is intended to be permanent.

> **Note**
>
> When you change the data warehouse's location, Secure Access' reporting functionality is temporarily suspended while the switchover to a new location occurs. For activity search data, the switchover period lasts only a few minutes; however, other reporting data may take several hours to begin appearing in reports.

Log Retention

Logs are deleted when the retention date expires as per the Secure Access Privacy Data Sheet.

Logs are not deleted when you change the data warehouse location.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**. In the **Data Storage** area, click **Change Location**.
2. Select a new location and click **Save**.
3. Confirm that you understand the consequences of changing the location where logs are physically stored and click **Confirm**.

   The data warehouse location is changed and Secure Access now stores event data logs to this new location. Logging to the old location stops.

   > **Note**
   >
   > Logs stored at the previous location are not deleted until the retention period expires—30 days for detailed data and two years for summary data.

Log export failures to Amazon S3

Describes Log export failures to Amazon S3 in Cisco Secure Access and explains Detection and notification, Export job pause policy, and Retry, retention, and deletion policy. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

A log export failure to Amazon S3 is a log delivery error that

- occurs when the Amazon S3 bucket configuration (including bucket name, path, access policy, or credentials) is invalid or inaccessible
- results in logs not being successfully transferred to the Amazon S3 destination
- triggers automatic retention, deletion, and notification policies in Secure Access

This policy replaces any previous S3 log export retention policy. Keeping S3 configurations valid and monitoring the Secure Access user interface helps prevent data loss.

Secure Access provides the capability to export logs to Amazon S3 buckets managed by either customers or Cisco. For successful log delivery, the S3 bucket configuration must remain valid and accessible. Export failures most commonly occur due to changes in the S3 bucket, access policies, or credentials.

Detection and notification

Secure Access continuously checks the status of Amazon S3 log exports. Export failures are detected when any of the following conditions occur:

- The S3 bucket or path is renamed or deleted
- The access policy is modified or removed
- S3 access credentials expire or become invalid

When an export failure is detected, Secure Access is unable to deliver log files to the configured S3 destination. The **Admin** > **Log Management** page displays **Last Sync** timestamp for reference. The job status will become **Not configured** once the job is paused. This behavior is applicable only for user-managed buckets, not for Cisco-managed buckets.

Export job pause policy

When an export failure is detected and persists for twenty-four hours, the S3 log export job is automatically paused. Secure Access stops attempting to upload logs until the configuration is corrected and the job is manually restarted.

Retry, retention, and deletion policy

When an export failure is detected:

- Secure Access tries to upload affected log files three times in immediate succession.
- If all upload attempts fail, the failed log files are retained for 24 hours from the initial failure. This retention window allows time to correct any misconfiguration and prevent data loss
- If the S3 export misconfiguration is not resolved within 24 hours, the retained log files are permanently deleted from Secure Access. These files cannot be recovered.

Log export recovery considerations

- After a misconfiguration is corrected, the S3 log export job becomes available to restart from **Admin** > **Log Management** > **Manage**click**Start Logging**. A success notification appears when you successfully start logging.
- Resolve any misconfiguration within 24 hours to prevent permanent loss of log data.

Data recovery considerations

- Logs deleted after the 24-hour retention window cannot be recovered through S3 export.
- Event data for the affected period may still be accessible through Secure Access reporting APIs within the standard data retention period, which is typically up to 90 days.

Frequently Asked Questions

Will I receive an email notification if my S3 export fails?

No. Email notifications are not sent for S3 export failures.

Can I recover logs deleted after a misconfiguration?

No. Deleted logs cannot be recovered through S3 export. However, event data may be available by using reporting APIs if it is still within the retention period.

How do I know if my S3 export is paused?

The **Admin** > **Log Management** page displays the current job status and timestamps for additional information.

Stop Logging

Provides instructions for completing the Stop Logging workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can stop logging at any time. When logging is stopped, Secure Access immediately stops sending logs to your S3 storage.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**.
2. Click **Stop Logging**.
3. **Do not** check the box to Delete all logs from S3.
   If you check the box, you are acknowledging that you are deleting all logs and to stop sending logs.
4. Click **Stop logging data** to confirm your request.

What to do next

To resume logging, click **Start logging**.

To delete storage, click **Delete Storage**.

Delete Logs

Provides instructions for completing the Delete Logs workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

You can delete previous log data when you stop logging. See Stop Logging.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management** > **Manage** > **Stop logging**.
2. Check the box to **Delete all logs from S3**.
3. Click **Stop logging data** to confirm your request.
   Logging of activity data stops, and all activity logs are deleted.

What to do next

You can restart logging at any time. Click **Start Logging** to resume logging.

Log Formats and Versioning

Describes Log Formats and Versioning in Cisco Secure Access. Secure Access stores zipped CSV log files in Cisco's managed AWS S3 bucket or your own AWS S3 bucket.

Secure Access stores zipped CSV log files in Cisco's managed AWS S3 bucket or your own AWS S3 bucket. Each log file displays multiple columns of information that are extracted from your Secure Access logs. A log file may have additional fields that are not shown in the Secure Access reports.

To identify the current version of the Secure Access log format, refer to Find your log schema version.

> **Note**
>
> Logs are not always chronological and are not always in the specific time bucket based on the timestamp of the log event.

Prerequisites

- Full Admin user role. For more information, see Manage Accounts.
- Configure logging to an Amazon S3 bucket. See Enable Logging to Your Own S3 Bucket or Enable Logging to a Cisco-managed S3 Bucket.

Log File Name Formats

Describes Log File Name Formats in Cisco Secure Access. Logs are uploaded in 10-minute intervals from the Secure Access log queue to the AWS S3 bucket.

Logs are uploaded in 10-minute intervals from the Secure Access log queue to the AWS S3 bucket. Within the first two hours after a completed configuration, you should receive your first log upload to your AWS S3 bucket.

> **Note**
>
> To check if everything is working, the **Last Sync** time in Secure Access should update and logs should begin to appear in your AWS S3 bucket. The logs appear in a GZIP format with the following file name format. The files will also be sorted into date-stamped folders.

- **Admin Audit logs** - `auditlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Cloud Firewall traffic** - `firewalllogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **DLP traffic** - `dlplogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **DNS traffic** - `dnslogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **File Events traffic** - `fileeventlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **IPS traffic** - `intrusionlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Network Connectivity logs** - `ntglogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Remote Access VPN traffic** - `ravpnlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Web traffic** - `proxylogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Zero Trust Network Access Enrollment traffic** - `ztnaenrollmentlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Zero Trust Network Access traffic** - `ztnalogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`
- **Zero Trust Access flow traffic** - `ztnaflowlogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz`

Subfolders

Logs are uploaded to AWS S3 buckets in the appropriate subfolder with the following naming format.

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

Secure Access names a log subfolder (`<subfolder>`) with one of the following folder names:

- `dnslogs`
- `proxylogs`
- `firewalllogs`
- `fileeventlogs`

- `intrusionlogs`
- `auditlogs`
- `dlplogs`
- `ntglogs`
- `ravpnlogs`
- `ztnaenrollmentlogs`
- `ztnalogs`
- `ztnaflowlogs`

The **<xxxx>** segment of the log GZIP file name is a random string of four alphanumeric characters, which prevents duplicate file names from being overwritten.

Example: `dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz`

Find Your Log Schema Version

Describes Find Your Log Schema Version in Cisco Secure Access. Depending on the Secure Access subscription that you have, and depending on the type of AWS S3 bucket you configure, there are different versions of the log schemas available.

Depending on the Secure Access subscription that you have, and depending on the type of AWS S3 bucket you configure, there are different versions of the log schemas available. Once your system is configured to log to an AWS S3 bucket you can view the log schema version in use.

Log Schema Versions

- **v1**–For customers who have configured their own S3 bucket *before* November 2017.

> **Note**
>
> To upgrade from **v1** to a higher version of the Secure Access log format, you must remove your existing S3 bucket, disable the integration, and then recreate a new bucket. For all other versions, you can upgrade from the Log Management screen of the Secure Access dashboard by clicking **Upgrade**.

- **v2**–For customers who have configured their own S3 bucket *after* November 2017, or are using a Cisco-managed bucket. This version is inclusive of everything in version 1.
- **v3**– The same as version 2, but adds two new fields: Most Granular Identity Type and Identity Types for DNS logs.
- **v4**–The same as version 3, but adds the Blocked Categories field for DNS and Proxy logs.
- **v5**–The same as version 4, but adds three new fields: all Identities, all Identity Types, and Request Method for Proxy logs.
- **v6**–The same as version 5, but adds the following fields to Proxy logs: Certificate Errors, Destination Lists IDs, DLP Status, File Name, Rule ID, and Ruleset ID.
- **v7**–The same as version 6, but adds the DLP file label field.
- **v8**–The same as version 7, but adds fields to the Proxy, DLP, and Firewall logs.
  - Proxy logs–Adds the Isolate Action, File Action, and Warn Status fields.

  - DLP logs–Changes the Event Type field. The event type is either `Real Time` or `SaaS API`.
  - Firewall logs–Adds the FQDNs and Destination List IDs fields.

- **v9**–The same fields as version 8, but the v9 log format adds fields to the IPS and Web logs.
  - Adds new fields to the **Intrusion Prevention System (IPS)** logs: **operation mode**, **policy resource ID**, **direction**, **firewall rule ID**, **IPS config type**, **AWS region**.
  - Adds new fields to the **Web** logs: **forwarding method** and **producer**.
  - Adds **File Events** logs.
  - Adds **Remote Access Virtual Private Network** logs.
  - Adds **Zero Trust Network Access** logs.

- **v10**–The same fields as version 9, but the v10 log format adds the following fields:
  - **Cloud Firewall** logs: **app id**, **private resource id**, **private app group id**, **private flow**, **posture id**, **casi category ids**, **traffic source**, **content category ids**, **content category list ids**, **organization id**.
  - **Data Loss Prevention (DLP)** logs: **application category name**, **traffic direction**, **private resource name**, **private resource group name**, **destination protocol**, **destination ip**, **destination port**, **organization id**.
  - **DNS** logs: **rule id**, **destination countries**, **organization id**.
  - **IPS** logs: **application id**, **casi category ids**, **data center**, **organization id**.
  - **Remote Access VPN** logs: **asa syslog id**, **device id**, **machine id**, **public ipv6**, **assigned ipv6**, **security group tag**, **dap record name**, **dap connection type**, **failed reasons**.
  - **Web** logs: **msp organization id**, **geo location**, **blocked destination countries**, **application ids**, **hostname**, **data center**, **egress**, **server name**, **time based rule**, **security overridden**, **detected response file type**, **warn categories**, **organization id**.
  - **Zero Trust Access** logs: **transaction id**, **block reason**, **application port**, **application protocol**, **tunnel type**, **secure client version**, **possible match ruleset id**, **possible match rule id**, **possible match posture**, **source process id**, **source process name**, **source process hash**, **source process user name**, **organization id**, **ad joined id**.
  - Adds **Zero Trust Access Flow** logs.

- **v11**–The same fields as version 10, but the v11 log format adds two new fields : Application Entity Name, and Application Entity Category to Web logs.
- **v12**–The same fields as version 11, but the v12 log format adds the following fields:
  - **Cloud Firewall** logs: **egress ip**, **egress**.
  - **File Events** logs: **enforced by**, **ftd enforcement id**, **ftd enforcement name**.
  - **IPS** logs: **egress ip**, **egress**, **enforced by**, **ftd enforcement id**, **ftd enforcement name**.
  - **Remote Access VPN** logs: **log message**, **asa syslog severity**, **asa syslog class**, **asa syslog descriptor**.
  - **Web** logs: **egress ip**.
  - **Zero Trust Access** logs: **enforced by**, **ftd enforcement id**, **ftd enforcement name**, **mdm source**, **mdm device id**, **mdm is managed**, **mdm is compliant**, **mdm last updated**.

  - **Zero Trust Access Flow** logs: **enforced by**, **ftd enforcement id**, **ftd enforcement name**.

- **v13**–The same fields as version 12, but the v13 log format introduces **Zero Trust Access Enrollment** logs and adds the following new fields to the existing logs:
  - **Web** logs: **ai model name**, **ai supply chain categories**.
  - **Zero Trust Access** logs: **applied trusted network**, **detected, trusted network**, **zta profile id**, **egress ip**.
  - **Zero Trust Access Enrollment** logs: **timestamp**, **identity email**, **identity labels**, **identity type labels**, **organization id**, **msp organization id**, **enrollment id**, **event type**, **enrollment method**, **event detail**, **os type & version**, **zta client version**, **event status**, **device id, public ip**.

- **v14**–The same fields as version 13, but the v14 log format adds the following new fields to the existing logs:
  - **Web** logs: **event correlation id**.
  - **Cloud Firewall** logs: **event correlation id.**
  - **IPS** logs: **event correlation id**.
  - **Zero Trust Access** logs: **transaction id**. The Transaction ID serves as the event correlation mechanism in ZTNA, unifying related events across security services (Firewall, SWG, ZTNA) to provide an end-to-end view of a single traffic flow.

- **v15**–The same fields as version 14, but the v15 log format introduces **Network Connectivity** logs and adds the following new fields:
  - **Network Connectivity** logs: **timestamp**, **identity labels**, **identity type labels**, **organization id**, **msp organization id**, **network tunnel group id**, **tunnel id**, **service name**, **level**, **message**, **region**, **datacenter ip**, **datacenter**, **ike auth id**, **ike customer address**, **ike customer port**, **ike spi**, **bgp peer ip**.

- **v16**–The same fields as version 15, but the v16 log format adds the following new fields to the existing logs:
  - **Web** logs: **isolateProfileId**.
  - **Cloud Firewall** logs: **destinationSGTOriginId** and **fwBlockReason**.

- **v17**–The same fields as version 16, but the v17 log format introduces **Data Loss Prevention (DLP)** logs and adds the following new fields to the existing logs:
  - **Cloud Firewall** logs: **source country**.
  - **DLP** logs: **taac tenant id**, **taac profile id**, **match excerpts**, **match violation starts**, **match violation ends**, **email sender**, **email recipients**, **email attachments**, **email id**, and **email vendor id**.
  - **Web** logs: **source country**.

View Your Log Schema Version and Last Sync Time

Provides instructions for completing the View Your Log Schema Version and Last Sync Time workflow in Cisco Secure Access. To view the Schema version, navigate to Admin Log Management Manage System information .

Procedure

1. To view the **Schema** version, navigate to **Admin** > **Log Management** > **Manage** > **System information**.
2. To view the **Last sync** navigate to **Admin** > **Log Management**.

- The **Last sync** field indicates the date and time when your logs were last synced to Amazon S3.
- If your S3 log export job is paused due to a misconfiguration (for example, invalid bucket, deleted bucket, or access policy changes), the **Last sync** time will not update until the issue is resolved and syncing resumes.
- When the job is paused, the **Start logging** located in **Admin** > **Log Management** > **Manage** page becomes active. After correcting the misconfiguration, you can use this button to manually resume log export.

The default schema version is **v10**. When a new schema version is available, it will be displayed as a green label (for example, **v12 Available**) indicating that an upgrade is available.

> **Note**
>
> You cannot undo a schema upgrade or return to a previous schema version after completing the upgrade.

What to do next

There are two ways to upgrade to the latest schema version:

1. Navigate to **Admin** > **Log Management** > **Upgrade from v<number>**.
2. Navigate to **Admin** > **Log Management** > **Manage** > **Upgrade**.

When the upgrade is successful, the new version (for example, v12) will be displayed in the Schema Version field.

Include Headers

Describes Include Headers in Cisco Secure Access. By default, AWS S3 log exports do not include a header row with field names.

By default, AWS S3 log exports do not include a header row with field names.

To enable a header row with field names in your AWS S3 log exports, navigate to **Admin** > **Log Management** > **Manage** > **Include Optional Log headers in S3 Export** > **Save**.

This setting applies to all log files. Changes to this setting will take effect with the next export.

Log File Fields

Describes Log File Fields in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Each type of Secure Access log contains various log fields. Not all field values are available in every log record. When a field does not have a value, Secure Access sets the field to the empty string (""). For information about the formats of the Secure Access reports, see Reports and CSV Formats.

- Admin Audit Log Formats
- Cloud Firewall Log Formats
- DLP Log Formats
- DNS Log Formats
- File Events Log Formats
- IPS Log Formats
- Network Connectivity Log Formats
- Remote Access VPN Log Formats
- Web Log Formats
- Zero Trust Network Access Log Formats
- Zero Trust Access Flow Log Formats

Estimate the Size of a Log

Describes Estimate the Size of a Log in Cisco Secure Access. The size of your S3 logs depends on the number of events that occur and the volume of the traffic in your organization.

The size of your S3 logs depends on the number of events that occur and the volume of the traffic in your organization.

1. Download one of your Secure Access log files. The Secure Access log file is a comma-separated values (CSV) file.
2. Count the number of rows in the CSV file minus one for the header row.

   The number of rows is equivalent to the number of events in the twenty-four hour period.
3. Multiply the number of rows of data by the number of bytes of data listed in a single row in the file.

   The result is the estimate of the size of the event log recorded for one day.

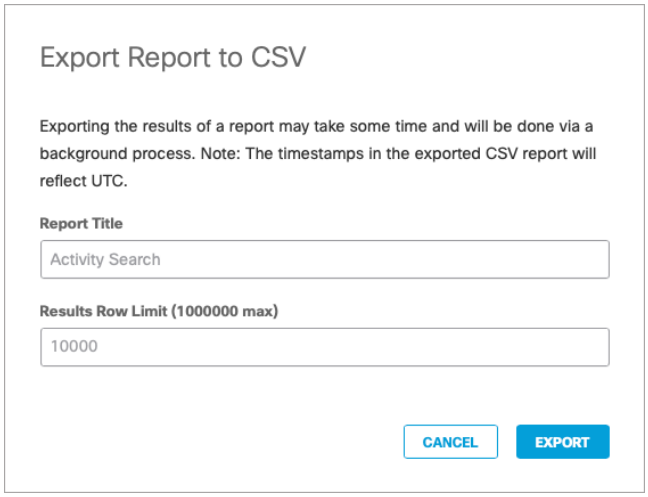
Estimate the Size of an Exported Report

Provides instructions for completing the Estimate the Size of an Exported Report workflow in Cisco Secure Access. The size of an exported report depends on the number of events that occur, which is dependent on the volume of your traffic.

The size of an exported report depends on the number of events that occur, which is dependent on the volume of your traffic. The size of each log line varies based on a number of items–for example, the length of the domain name or the number of categories. Assuming each log line is 220 bytes, a million requests would be 220 MB.

Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. For Filters, run a report for the last 24 hours and then click the **Export CSV** icon.



3. Open the downloaded CSV file. The number of rows (minus one for the header) is the number of queries per day. Multiply the number of rows by the number of bytes in one row to get the estimate for one day.

Reports and CSV Formats

Describes Reports and CSV Formats in Cisco Secure Access. Cisco Secure Access has various reports that you can download from Secure Access in the comma-separated values (CSV) format.

Cisco Secure Access has various reports that you can download from Secure Access in the comma-separated values (CSV) format. For information about the size of a report, see Estimate the Size of an Exported Report.

Here is the list of reports that you can download from Cisco Secure Access:

- Activity Search Report
- Top Categories Report
- Top Destinations Report
- Top Resources Report

Activity Search Report

Describes Activity Search Report in Cisco Secure Access. You can export the results of the Activity Search Report to a CSV format.

You can export the results of the Activity Search Report to a CSV format. For more information, see Export Report Data to CSV and Activity Search Report.

Fields in the Activity Search Report:

- **Type**–The type of request made, such as DNS.
- **Date**–The date the request was made.
- **Time**–The time the request was made, in UTC.
- **Action**–Whether the request was Allowed or Blocked.
- **Errors**–Any certificate or protocol errors in the request.
- **Ruleset ID**–The ID number assigned to the ruleset.
- **Ruleset Name**–The ruleset that was applied.
- **Rule ID**–The ID number assigned to the rule.
- **Rule Name**–The rule that was applied.
- **Destination List IDs**–The ID number assigned to a destination list.
- **Signature List ID**–The unique ID assigned to a Default or Custom Signature List.
- **IPS Signature**–The threat detected in our IPS/IDS protection.
- **IPS Signature Severity**–The severity of the IPS Signature.
- **IPS Signature CVE**–Common vulnerabilities and exposures related to the IPS Signature.
- **Identities**–All tunnel identities associated with this request.
- **Identity Types**–The types of identity that were associated with the request. For example, Roaming Computers or Networks.
- **Policy or Ruleset Identity**–The identity that made the request.
- **Policy or Ruleset Identity Type**–The type of the identity that made the request.
- **Forwarding Method**–The method used to forward the identity of the client to the proxy.
- **Internal IP**–The internal IP address that made the request.
- **External IP**–The external IP address that made the request.
- **Source IP**–The IP of the computer making the request.
- **Destination IP**–The destination IP requested.

- **Source Port**–The port the request was made on.
- **Destination Port**–The destination port the request was made on.
- **Destination**–The domain of the request.
- **Hostname**–The name of the host.
- **Categories**–The content categories, if any, that matched against the destination IP address or port requested.
- **Integrations**–Integration categories you set.
- **Blocked Categories**–The category that resulted in the destination being blocked.
- **Application**–The application associated with the request.
- **Application Category**–The categories for any applications associated with the request.
- **Query Type**–The type of DNS request that was made.
- **Content Type**–The type of web content; typically text or html.
- **Protocol**–The actual protocol of the traffic. For example, TCP, UDP, or ICMP.
- **Filename**–The name of the file.
- **File Action (Remote Browser Isolation)**–The action taken on a file during a Remote Browser Isolation session.
- **Total Size in Bytes**–The total size in bytes.
- **Request Size**–Request size in bytes.
- **Response Size**–Response size in bytes.
- **Packet Size**–Packet size in bytes.
- **Referrer**–The referring domain or URL.
- **User Agent**–The browser agent that made the request.
- **Status Code**–The HTTP status code.
- **Direction**–The direction of the packet. It is directed either towards the internet or to the customer's network.
- **Threats**–Any threats associated with the request.
- **Threat Types**–The types of threats associated with the request.
- **SHA256 Hash**–The hex digest of the response content.
- **Cisco AMP Result**–The malware detected by AMP.
- **Cisco AMP Disposition**–What action was taken on the file download.
- **Cisco AMP Score**–The risk score associated with the downloaded file. This field returns blank unless the verdict is Unknown, in which the value will be 0.
- **Antivirus Result**–Threats detected by the antivirus.
- **Potentially Unwanted Applications**–A list of all potentially unwanted application (PUA) results for the proxied file as returned by the antivirus scanner.
- **Detected Response File Type**–The file type of the response, as detected by the file type control that blocked the request based on factors such as URL or content type header.
- **Isolated State**–Whether the Remote Browser Isolation state was isolated or not.
- **Data Loss Prevention State**–Whether the DLP status was allowed or blocked.

- **Tenant Controls**–Whether the request is Tenant Application Access Control protected.

Zero Trust Access Activity Search Fields

Describes Zero Trust Access Activity Search Fields in Cisco Secure Access. The Activity Search report displays the Zero Trust Access event details.

The Activity Search report displays the Zero Trust Access event details.

Field Name	Reports Section	Description
Ingress Region	Event Details	The geographic region of the data center where Secure Access received the incoming traffic.
Resource Connector Group	Event Details	The ID of the resource connector group that provides access to the private resource.
Tunnel Type	Event Details	The type of traffic supported by the network tunnel, which the endpoint established with the proxy. The transport protocol on the tunnel is either **HTTP** or **HTTP3**.
Transaction ID	Event Details	The unique ID associated with the Zero Trust request. Use the transaction ID to correlate and troubleshoot connection issues.
Block Reason	Block Details	Secure Access provides an explanation for blocking access to the private resource.
Associated Rule	Block Details	When access was blocked for not meeting access or posture requirements, Secure Access reports the closest matched policy rule that would have allowed access.
Associated Posture	Block Details	The posture profile that is configured for the associated rule.
Endpoint Application	Endpoint Details	The name of the endpoint application, which initiated the connection.
Application Signature	Endpoint Details	The SHA256 signature of the endpoint application process.
Endpoint Username	Endpoint Details	The username that is associated with the endpoint application process.

Top Categories Report

Describes Top Categories Report in Cisco Secure Access. You can export the results of the Top Categories Report to a CSV format.

You can export the results of the Top Categories Report to a CSV format. For more information, see Export Report Data to CSV and Top Categories Report.

Fields in the Top Categories Report:

- **Category**–A content category in which a request was made. See Manage Content Categories.
- **Count**–The number of requests made for the category.

Top Destinations Report

Describes Top Destinations Report in Cisco Secure Access. You can export the results of the Top Destinations Report to a CSV format.

You can export the results of the Top Destinations Report to a CSV format. For more information, see Export Report Data to CSV and Top Destinations Report.

Fields in the Top Destinations Report:

- **Domain**–The domain that was requested.
- **Query Count**–The number of requests for the domain.
- **Categories**–The content categories that matched against the destination requested. See Manage Content Categories.

Top Resources Report

Describes Top Resources Report in Cisco Secure Access. You can export the results of the Top Resources Report to a CSV format.

You can export the results of the Top Resources Report to a CSV format. For more information, see Export Report Data to CSV.

Fields in the Top Resources Report:

- **Identity**–The identity making requests.
- **Query Count**–The number of requests made by the identity.

Admin Audit Log Formats

Describes Admin Audit Log Formats in Cisco Secure Access. The Cisco Secure Access Admin Audit logs show the administrative changes to your organization's Secure Access settings.

The Cisco Secure Access Admin Audit logs show the administrative changes to your organization's Secure Access settings. For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of an Admin Audit log event:

```
id,timestamp,email,user,type,action,logged in from,before,after
"123","2024-07-22
10:46:45","[user@domain.com](mailto:user@domain.com)","","logexportconfigurations","update","209.165.200.227","version:
 4","version: 5"
```

Order of Fields in Admin Audit Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"ID","Time","Email","User","Type","Action","Logged in from","Before","After"
```

> **Note**
>
> The last two fields, "Before" and "After," may contain line breaks if the previous or updated value spans multiple lines.

Log Format

The CSV fields in the header row of the Admin Audit log.

```
id,timestamp,email,user,type,action,logged in from,before,after
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
id	A unique identifier of the audit event.	v4
timestamp	The date and time of the administrative change event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note**: Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v4
email	The email of the user that triggered the event.	v4
user	The account name of the user who created the change.	v4
type	Where the change was made, such as settings or a policy.	v4
action	The type of change made, such as Create, update, or Delete.	v4
logged in from	The user's IP source.	v4
before	The policy or setting before the change was made.	v4

Field name	Description	Release version
after	The policy or setting after the change was made.	v4

Cloud Firewall Log Formats

Describes Cloud Firewall Log Formats in Cisco Secure Access. Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall.

Cloud firewall logs show traffic that has been handled by Secure Access cloud-delivered firewall. For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of a Cloud Firewall log:

```
timestamp,origin IDs,identities,identity type,direction,protocol,packet
size,source IP,source port,destination IP,destination port,data center,rule
ID,action,fqdns,destination list IDs,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event
id,destination country,aws region,app id,private app group id,private
flow,posture id,casi category ids,traffic source,content category ids,content
 category list ids,organization id,egress IP,egress, event correlation id,
destination SGT Origin Id, fw Block Reason
id, source country
"2024-06-14 18:59:57","\[211039844\]","Passive Monitor", "CDFW Tunnel Device",
 "OUTBOUND", "1", "84", "172.17.3.4", "60951", "146.112.255.129",
"443","ams1.edc", "12", "ALLOW", "google.com,apple.com", "44,66", "1718391597",
 "1718391597", "3", "3", "1108", "755", "39-42", "", "", "", "", "", "", "[]",
 "", "", "", "2204063", "3.3.3.4", "TRUE", "8dd4e2a7c2dba7d1", "10",
"policy_violation", "us"
```

Order of Fields in the Cloud Firewall Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Origin IDs","Identities","Identity
Types","Direction","Protocol","Packet Size","Source IP","Source
Port","Destination IP","Destination Port","Data Center","Rule
ID","Action","FQDNS","Destination List IDs","First Packet Timestamp","Last
Packet Timestamp","Packets Sent","Packets Received","Bytes Sent","Bytes
Received","FW Event ID","Destination Country","AWS Region","App ID","Private
App ID","Private Flow","Posture ID","CASI Category IDs","Traffic
Source","Content Category IDs","Content Category List IDs","Organization
ID","Egress IP","Egress","Event Correlation ID","Destination SGT Origin ID",
"Fw Block Reason", "Source Country"
```

Log Format

The CSV fields in the header row of the Cloud Firewall logs.

```
timestamp,origin ids,identities,identity type,direction,protocol,packet
size,source ip,source port,destination ip,destination port,data center,rule
id,action,fqdns,destination list ids,first packet timestamp,last packet
timestamp,packets sent,packets received,bytes sent,bytes received,fw event
id,destination country,aws region,app id,private app group id,private
flow,posture id,casi category ids,traffic source,content category ids,content
 category list ids,organization id,egress IP,egress,event correlation id,
destinationSGTOriginId, fwBlockReason, sourcecountry
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the cloud-delivered firewall traffic event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note**: Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v1
origin ids	The unique identity of the network tunnel.	v1
identities	The names of the network tunnel.	v5
identity type	The type of identity that made the request. Should always be `CDFW Tunnel Device`.	v5
direction	The direction of the packet. It is destined either towards the internet or to the customer's network.	v1
protocol	The actual protocol of the traffic. Valid values are: `TCP`, `UDP`, or `ICMP`.	v1
packet size	The size in bytes of the packet sent to the CDFW.	v1
source ip	The internal IP address of the user-generated traffic towards the CDFW. If the traffic goes through NAT before it comes to CDFW, it will be the NAT IP address.	v1
source port	The internal port number of the user-generated traffic towards the CDFW.	v1
destination ip	The destination IP address of the user-generated traffic towards the CDFW.	v1
destination port	The destination port number of the user-generated traffic towards the CDFW.	v1

Field name	Description	Release version
data center	The name of the data center that processed the user-generated traffic.	v1
rule id	The ID of the rule that processed the user traffic.	v1
action	The final verdict whether to allow or block the traffic based on the rule.	v1
fqdns	The fully qualified domain names (FQDNs) that match the request.	v8
destination list ids	The destination list IDs that Secure Access applied in the rule.	v8
first packet timestamp	The timestamp when the first packet of the session was received in UTC in seconds. Populated only for traffic handled by Cisco Secure Firewall.	v9
last packet timestamp	The timestamp when the last packet of the session was received in UTC in seconds. Populated only for traffic handled by Cisco Secure Firewall.	v9
packets sent	The number of packets sent during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
packets received	The number of packets received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
bytes sent	The number of bytes sent during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
bytes received	The number of bytes received during the session. Populated only for traffic handled by Cisco Secure Firewall.	v9
fw event id	The ID of the firewall event. Populated only for traffic handled by Cisco Secure Firewall.	v9
destination country	The ISO-3166 alpha-2 two-character identifier of the country associated with the destination IP.	v10
aws region	The AWS region that stores your VPN logs.	v10
app id	The unique application ID identified for the current session.	v10
private app group id	The unique ID of the private resource group ID that the private resource belongs to.	v10

Field name	Description	Release version
private flow	`TRUE` if Secure Access applied a private access rule to the user-generated traffic, and `FALSE` if Secure Access applied an internet access rule.	v10
posture id	The unique ID of the endpoint posture profile.	v10
casi category ids	Name of the Application category to which the App ID belongs.	v10
traffic source	The source of the user-generated traffic. Valid values are `0 - Unknown`, `1 - VPN`,`2 - ZTNA`, `3 - Network Tunnel`.	v10
content category ids	ID of one or more content categories matched by the rule.	v10
content category list ids	ID of one or more content category lists that include categories matched by the rule.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID .	v10
egress IP	The public IP address assigned to a session as it exits the Secure Access ZTA infrastructure en route to the destination application.	v12
egress	`TRUE`indicates that the egress IP was a reserved IP.	v12
event correlation id	A unique identifier generated for each network request, the Event Correlation ID stitches together all related events across various security services (Firewall, SWG, ZTNA) to provide a unified, end-to-end view of a single traffic flow.	v14
destination SGT origin Id	The Security Group Tag (SGT) ID associated with the destination resource. This identifies the security group classification of the traffic destination.	v16
fw block reason	The specific reason why the firewall blocked the traffic. Common values include policy_violation, malicious_domain, protocol_mismatch, or access_denied.	v16
source country	The ISO 3166 alpha 2 two character identifier of the country associated with the source IP.	v17

Data Loss Prevention (DLP) Log Formats

Describes Data Loss Prevention (DLP) Log Formats in Cisco Secure Access. The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred.

The Cisco Secure Access DLP logs show information about DLP events where data identifiers were triggered and a violation occurred. DLP logs are available in all log format versions. For information about the size of a log file, see Estimate the Size of a Log.

> **Note**
>
> A single DLP event can present in multiple rows of the logs when different data identifiers and file labels are triggered for the same content. Rows related to the same content or event have the same Unique Event ID.

Example

This is an example of a DLP log event:

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file
label,application category name,traffic direction,private resource name,private
 resource group name,destination protocol,destination ip,destination
port,organization id, taac tenant id, taac profile id, match excerpts, match
violation starts, match violation ends, email sender, email recipients, email
 attachments, email id, email vendor id
"2022-02-15 12:05:45","Real
[illegible]
 PCI Classification","Credit Card Number -
Strict","text/html","48","abbd2352c3cfea8846871928bf99ca24dc3a6f162170926649381a6d968869ab",

"Confidential","","","dlpprivateresource","","https","127.0.0.1","443","8247177","tenant
 12345","profile 67890","masked card: **** 4242, masked SSN: *** **
1234","12,48","23,64","sender@example.com","alice@example.com,
bob@example.com","invoice.pdf, contract.docx","email 2026 0001","m365"
```

Order of Fields in the DLP Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Event Type","Unique Event
ID","Severity","Identities","Owner","Name","Application","Destination","Action","Rule
 Name","Data Classification","Data Identifier","Content Type","File
Size","SHA256 Hash","File Label","Application Category Name","Traffic
Direction","Private Resource Name","Private Resource Group Name","Destination
 Protocol","Destination IP","Destination Port","Organization ID", "TAAC Tenant
 ID", "TAAC Profile ID", "Match Excerpts", "Match Violation Starts", "Match
```

```
Violation Ends", "Email Sender", "Email Recipients", "Email Attachments",
"Email ID", "Email Vendor ID"
```

Log Formats

The CSV fields in the header row of the DLP logs.

```
timestamp,event type,unique event
id,severity,identity,owner,name,application,destination,action,rule,data
classification,data identifier,content type,file size,sha 256 hash,file
label,application category name,traffic direction,private resource name,private
 resource group name,destination protocol,destination ip,destination
port,organization id, taac tenant id, taac profile id, match excerpts, match
violation starts, match violation ends, email sender, email recipients, email
 attachments, email id, email vendor id
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the DLP event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v6
event type	The type of event that matched a data identifier. `Real Time` denotes a proxy-based DLP event triggered by a Real Time rule and `SaaS API` denotes a DLP event triggered by any of the SaaS API rules.	v8
unique event id	The unique identifier for the event. There can be multiple violation matches in one event.	v6
severity	The severity of the rule: `Low/Info`, `Medium/Warn`, `High/Alert`, or `Critical`.	v6
identity	The source that triggered the violation.	v6
owner	The owner of the file.	v6
name	The name of the file.	v6
application	The application of the request.	v6
destination	The domain of the request.	v6
action	If the violation was `Blocked` or `Monitored`.	v6

Field name	Description	Release version
rule	The DLP rule name.	v6
data classification	The data classification whose data identifier matched on the violation.	v6
data identifier	The data identifier that matched on the request.	v6
content type	The mime type of the file that matches the data identifier.	v6
file size	The size of the file in bytes.	v6
sha 256 hash	The hex digest of the response content.	v6
file label	The file name label that matched on the file properties.	v7
application category name	The category of the requested web application. For more information, see Application Categories.	v10
traffic direction	Direction of traffic. (Applies only to some applications, such as OpenAI API and OpenAI ChatGPT.)	v10
private resource name	The name of the private resource.	v10
private resource group name	The private resource group name if the matched rule destination was a private resource group.	v10
destination protocol	The protocol of the destination.	v10
destination ip	The IP address of the destination.	v10
destination port	The port of the destination.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID .	v10
taac tenant id	The unique identifier for the Cisco Secure Access tenant within the TAAC platform.	v17
taac profile id	The unique identifier for the TAAC configuration profile.	v17
match excerpts	Comma separated masked excerpts containing classifier matches.	v17
match violation starts	Comma separated zero based start offsets for the matches.	v17
match violation ends	Comma separated exclusive end offsets for the matches.	v17
email sender	The sender address for email scan events.	v17
email recipients	Comma separated list of recipient addresses.	v17

Field name	Description	Release version
email attachments	Comma separated list of attachment file names.	v17
email id	A unique identifier for the email message.	v17
email vendor id	The identifier for the email vendor or integration provider.	v17

DNS Log Formats

Describes DNS Log Formats in Cisco Secure Access. The Cisco Secure Access DNS logs show your organization's traffic through the Secure Access DNS resolvers.

The Cisco Secure Access DNS logs show your organization's traffic through the Secure Access DNS resolvers. For information about the size of a log file, see Estimate the Size of a Log.

Examples

This is an example of a DNS Log of an Allowed Action event:

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories,rule id,destination countries,organization id
"2024-09-11 18:46:00","Active Directory User (adusername@example.net)","Active
 Directory User
(adusername@example.net),WIN11-SNG01-Example","10.10.1.100","24.123.132.133","Allowed","1
 (A)","NOERROR","domain-visited.com.","Software/Technology,Business
Services,Allow List,Infrastructure and Content Delivery Networks,SaaS and
B2B,Application","AD Users","AD Users,Anyconnect Roaming
Client","","506165","","8234970"
```

This is an example of a DNS Log of a Blocked Action event with Blocked Categories:

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories,rule id,destination countries,organization id
"2024-09-11 18:46:00","Active Directory User (adusername@example.net)","Active
 Directory User
(adusername@example.net),WIN11-SNG01-Example","10.10.1.100","24.123.132.133","Blocked","1
 (A)","NOERROR","domain-visited.com.","Chat,Social Networking","AD Users","AD
 Users,Anyconnect Roaming Client","Social Networking","506165","","8234970"
```

Order of Fields in the DNS Log

Note

Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Most Granular Identity","Identities","Internal IP","External
IP","Action","Query Type","Response Code","Domain","Categories","Most Granular
 Identity Type","Identity Types","Blocked Categories","Rule ID","Destination
Countries","Organization ID"
```

Log Formats

The CSV fields in the header row of the DNS logs.

```
timestamp,most granular identity,identities,internal ip,external ip,action,query
 type,response code,domain,categories,most granular identity type,identity
types,blocked categories,rule id,destination countries,organization id
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the DNS event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v8
most granular identity	The first identity matched with this request in order of granularity.	v8
identities	All identities associated with this request.	v5
internal ip	The internal IP address that made the request.	v8
external ip	The external IP address that made the request.	v8
action	Whether the request was allowed or blocked.	v8
query type	The type of DNS request that was made.	v8
response code	The DNS return code for this request.	v8
domain	The domain that was requested.	v8
categories	The security or content categories that the destination matches. For category definitions, see Manage Threat Categories and Manage Content Category Lists.	v8

Field name	Description	Release version
most granular identity type	The first identity type matched with this request in order of granularity.	v3
identity types	The type of identity that made the request, for example: Roaming Computer, Network.	v3
blocked categories	The categories that resulted in the destination being blocked.	v4
rule id	The ID of the access rule when the DNS request is matched by a policy.	v10
destination countries	The two-character country identifier of the domain that was requested.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10

File Events Log Formats

Describes File Events Log Formats in Cisco Secure Access. The Cisco Secure Access File Events log shows your organization's traffic events involving file access that match private access rules with File Inspection or File Type Control enabled.

The Cisco Secure Access File Events log shows your organization's traffic events involving file access that match private access rules with File Inspection or File Type Control enabled. For more information, see Get Started With Private Access Rules, Manage File Inspection and File Analysis, and Manage File Type Controls.

For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of the File Events log:

```
timestamp,organization id,retention policy in days,aws region,firewall
eventid,file action,disposition,sha256,direction,threat name,filestatic
analysis,threat score,filetype id,filename,filesize,archive filename,archive
filedepth,archive sha,dlp status,enforced by,ftd enforcement id,ftd enforcement
 name
"2024-09-04
```

Order of Fields in the File Events Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Organization ID","Retention Policy In Days","AWS Region","Firewall
 Event ID","File Action","Disposition","SHA256 Hash","Direction","Threat
Name","File Static Analysis","Threat Score","File Type ID","File Name","File
Size","Archive File Name","Archive File Depth","Archive SHA","DLP
Status","Enforced By","FTD Enforcement ID","FTD Enforcement Name"
```

Log Format

The CSV fields in the header row of the File Events log.

```
timestamp,organization id,retention policy in days,aws region,firewall
eventid,file action,disposition,sha256,direction,threat name,filestatic
analysis,threat score,filetype id,filename,filesize,archive filename,archive
filedepth,archive sha,dlp status,enforced by,ftd enforcement id,ftd enforcement
 name
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The timestamp of the request transaction in UTC (e.g., 2024-01-16 17:48:41).	v9
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v9
retention policy	The number of days that AWS S3 stores your Secure Access File Events log.	v9
aws region	The AWS region where Secure Access stores your logs.	v9
firewall event id	The ID of the firewall event. Populated only for traffic handled by Cisco Secure Firewall.	v9
file action	The action taken on a file in a remote browser isolation session. Valid values are: **UNKNOWN**, **DETECT**, **BLOCK**, **MALWARE_CLOUD_LOOKUP**, **MALWARE_WHITELIST**, **CLOUD_LOOKUP_TIMEOUT**, **CUSTOM_DETECTION**, **CUSTOM_DETECTION_BLOCK**, **ARCHIVE_BLOCK_DEPTH_EXCEEDED**, **ARCHIVE_BLOCK_ENCRYPTED**, **ARCHIVE_BLOCK_FAILED_TO_INSPECT**, **TID_BLOCK**	v9
disposition	The status of the files proxied and scanned by Cisco Advanced Malware Protection (AMP) as part of the File Inspection feature. Valid values are: **CLEAN**, **MALWARE**, **UNKNOWN**.	v9
sha256	The SHA-256 checksum hash of the file.	v9

Field name	Description	Release version
direction	The traffic direction of the file event. Valid values are: **UNKNOWN**, **UPLOAD**, **DOWNLOAD**.	v9
threat name	Name of the threat identified for files with **MALWARE** disposition.	v9
file static analysis	The status of the file static sample analysis. For more information, see Cisco Secure Malware Analytics (formerly Threat Grid) Details. Valid values are: **UNKNOWN**, **NOT_ANALYZED**, **ANALYSIS_COMPLETE_NO_VIRUS**, **ANALYSIS_FAILED**, **ANALYSIS_COMPLETE_MALWARE_DETECTED**	v9
threat score	The threat score most recently associated with this file. This is a value from 0 to 100.	v9
file type id	The type of file. For example, PDF or MSEXE.	v9
file name	The name of the file involved with the activity.	v9
file size	The size of the file in bytes.	v9
archive file name	The name of the archive file involved with the activity.	v9
archive depth	The level (if any) at which the file was nested in an archive file.	v9
archive sha	The SHA-256 checksum hash of the archive file.	v9
dlp status	The verdict of the DLP scanning service. For more information, see Manage the Data Loss Prevention Policy. Valid values are: **FW_FILE_DLP_NONE**, **FW_FILE_DLP_SENT**, **FW_FILE_DLP_SUCCESS**, **FW_FILE_DLP_FAIL_ON_MIN_FILESIZE**, **FW_FILE_DLP_FAIL_ON_MAX_FILESIZE**, **FW_FILE_DLP_FAIL_ON_MEMCAP**, **FW_FILE_DLP_FAIL_ON_FULL_QUEUE**, **FW_FILE_DLP_FAIL_ON_SEND**, **FW_FILE_DLP_FAIL_ON_NO_RESPONSE**, **FW_FILE_DLP_FAIL_ON_CLOUD_SEND**, **FW_FILE_DLP_VERDICT_FAIL**, **FW_FILE_DLP_VERDICT_UNKNOWN**, **FW_FILE_DLP_VERDICT_CLEAN**, **FW_FILE_DLP_VERDICT_DATA_LEAK**, **FW_FILE_DLP_VERDICT_MALICIOUS**, **FW_FILE_DLP_VERDICT_TIMEOUT**	v9

Field name	Description	Release version
enforced by	The Secure Access component or service that enforced the policy or control related to this event (e.g., Firewall, Web Proxy).	v12
ftd enforcement id	The unique identifier of the enforcement action taken by a Firepower Threat Defense (FTD) device integrated with Secure Access.	v12
ftd enforcement name	The name or type of enforcement action taken by a FTD device integrated with Secure Access (e.g., Malware Block, URL Category Block).	v12

IPS Log Formats

Describes IPS Log Formats in Cisco Secure Access. The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System.

The Cisco Secure Access IPS logs show the traffic, events, and possible threats detected by the Secure Access Intrusion Prevention System. For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of an IPS log:

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region,application id,casi category ids,data center,organization
 id,egress ip,egress,enforced by,ftd enforcement id,ftd enforcement name, event
 correlation id
"2024-09-11 23:17:13","Firewall Tunnel Name","Network
Tunnels","1","16606","SERVER-ORACLE BEA WebLogic Server Plug-ins Certificate
overflow attempt","50516","HIGH","Attempted User Privilege
Gain","cve-2009-1016","TCP","12345","123.123.123.123","80","1.1.1.1","40762","Would

Block","IDS","50516","S2C","21171","PROFILE","eu-central-2b","","","","8151514","3.3.3.4","TRUE","FTD","12321321312","","e846afe0f3c8a87f"
```

Order of Fields in the IPS Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Identities","Identity Types","Generator ID","Signature
ID","Signature Message","Signature List ID","Severity","Attack
```

```
Classification","CVEs","IP Protocol","Session ID","Source IP","Source
Port","Destination IP","Destination Port","Action","Operation Mode","Policy
Resource ID","Direction","Firewall Rule ID","IPS Config Type","AWS
Region","Application ID","CASI Category IDs","Data Center","Organization
ID","Egress IP","Egress","Enforced By","FTD enforcement ID","FTD Enforcement
Name","Event Correlation ID"
```

Log Format

The CSV fields in the header row of the IPS log.

```
timestamp,identities,identity types,generator id,signature id,signature
message,signature list id,severity,attack classification,cves,ip
protocol,session id,source ip,source port,destination ip,destination
port,action,operation mode,policy resource id,direction,firewall rule id,ips
config type,aws region,application id,casi category ids,data center,organization
 id,egress IP,egress,enforced by,ftd enforcement id,ftd enforcement name,event
 correlation id
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the IPS detection event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v8
identities	All tunnel identities that are associated with this request.	v8
identity types	The type of identity that is associated with this request.	v8
generator id	Unique ID assigned to the part of the IPS that generated the event.	v8
signature id	Used to uniquely identify signatures.	v8
signature message	A brief description of the signature.	v8
signature list id	Unique ID assigned to a Default or Custom Signature List.	v8
severity	The severity level of the rule. Valid values are: `High`, `Medium`, `Low`, and `Very Low`.	v8

Field name	Description	Release version
attack classification	The category of attack detected by a rule that is part of a more general type of attack class. Valid values are: `trojan-activity`, `attempted-user`, and `unknown`.	v8
cves	A list of information about security vulnerabilities and exposures.	v8
ip protocol	The actual protocol of the traffic, such as `TCP`, `UDP`, `ICMP`.	v8
session id	The unique identifier of a session, which is used to group the correlated events between various services.	v8
source ip	The IP of the computer making the request.	v8
source port	The port number of the request.	v8
destination ip	The port number of the request.	v8
destination port	The destination port number of the request.	v8
action	The action performed when criteria meets a rule, for example: `block`, `warn`, and `would_block`.	v8
operation mode	The mode of operation of the IPS, either detection or prevention. Valid values are: `IDS`, `IPS`, and `UNKNOWN`.	v9
policy resource id	The ID of the IPS policy resource. An example of a policy resource is: signature list.	v9
direction	The direction of the packet that matches the signature. Valid values are: `S2C`, `C2S`, and `UNKNOWN`.	v9
firewall rule id	The ID of the rule that matches the firewall session.	v9
ips config type	The type of the IPS configuration. Valid values are: `CONFIG`, `PROFILE`, and `UNKNOWN`.	v9
aws region	The AWS region where Secure Access stores your logs.	v9
application id	The ID of the destination application.	v10
casi category ids	The name of the Application category to which the App ID belongs.	v10
data center	The name of the data center that processed the user-generated traffic.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID .	v10

Field name	Description	Release version
egress ip	The public IP address assigned to a session as it exits the Secure Access ZTA infrastructure en route to the destination application.	v12
egress	`TRUE` indicates that the egress IP was a reserved IP.	v12
enforced by	The Secure Access component or service that enforced the policy or control related to this event (e.g., Firewall, Web Proxy).	v12
ftd enforcement id	The unique identifier of the enforcement action taken by a Firepower Threat Defense (FTD) device integrated with Secure Access.	v12
ftd enforcement name	The name or type of enforcement action taken by a FTD device integrated with Secure Access (e.g., Malware Block, URL Category Block).	v12
event correlation id	A unique identifier generated for each network request, the Event Correlation ID stitches together all related events across various security services (Firewall, SWG, ZTNA) to provide a unified, end-to-end view of a single traffic flow.	v14

Network Connectivity Log Formats

This concept explains how Cisco Secure Access Network Connectivity logs are exported in CSV format to Amazon Simple Storage Service (Amazon S3) buckets for long-term retention and centralized management. The log format enables compliance, analytics, and event correlation with detailed event fields.

The Cisco Secure Access Network Connectivity logs display the export data logs or reports to an Amazon S3 bucket, which can be either customer-owned or Cisco-managed. The S3 export facilitates long-term event retention and centralized management of log and report data. This is typically used for compliance, event correlation, or analytics purposes. For more information, see Estimate the Size of a Log.

Example

This is an example of a Network Connectivity log event:

```
"2017-10-02 23:52:53","Canary 1","Network Tunnel
Hub","1234567","5678912","610610610","132412","BGP","ERROR","BGP Peer failed
to
connect","us-west-2","10.10.10.10","stg-aws-usw2","TestTunnel@111111-61106956.cisco.com","12.11.54.16","3000","53a5eed7de8fnet","1.1.1.1"
```

Order of Fields in Network Connectivity Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
<timestamp><identity label><identity type label><organization id><msp
organization id><network tunnel group id><tunnel id><service
name><level><message><region><datacenter ip><datacenter><ike auth id><ike
customer address><ike customer port><ike spi><bgp peer ip>
```

Log Format

The CSV fields in the header row of the Network Connectivity log.

```
Timestamp, Identity Label, Identity Type Label, Organization ID, MSP
Organization ID, Network Tunnel Group ID, Tunnel ID, Service Name, Level,
Message, Region, Datacenter IP, Datacenter, IKE Auth ID, IKE Customer Address,
 IKE Customer Port, IKE SPI, BGP Peer IP
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The UTC time the event occurred in milliseconds. (e.g., `2017-10-02 23:52:53`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v15
identity labels	The list of labels for the identity.	v15
identity type labels	The label of the identity type.	v15
organization id	The Secure Access organization ID.	v15
msp organization id	ID of the MSP organization.	v15
network tunnel group id	Identifier of a network tunnel group.	v15
tunnel id	Identifier of an established tunnel instance.	v15
service name	Name of the service reporting the event. Options are BGP, IKE, ORCH, UNDEFINED.	v15

Field name	Description	Release version
level	The level of this log entry. Options are INFO, WARNING, ERROR.	v15
message	Description of the log entry.	v15
region	Deployment region where datacenters are located, in which the log entry was generated.	v15
datacenter ip	IP address of the datacenter where the message was produced.	v15
datacenter	Name of the datacenter handling the tunnel termination in which this log entry was generated.	v15
ike auth id	Tunnel identity configured by the customer.	v15
ike customer address	Public customer side address of incoming IKEv2 packets.	v15
ike customer port	Public port of incoming IKEv2 packets.	v15
ike spi	A unique identifier per IKEv2 Security Association.	v15
bgp peer ip	The customer-side BGP peer IP address.	v15

Remote Access VPN Log Formats

Describes Remote Access VPN Log Formats in Cisco Secure Access. The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services.

The Cisco Secure Access remote access virtual private network (VPN) logs show the VPN session connection events, which are managed by the Secure Access VPN services. Some relevant fields to aid debugging and trouble-shooting VPN sessions include:

- Display Username for Failed Events – Significantly improves how quickly issues can be tracked and addressed.
- ASA Syslog Message ID Extraction Support – Offers detailed insights by identifying the specific sys-log messages used in the remote access logs.
- Device ID – Includes the device ID with every event, providing critical help to network administrators in numerous ways.
- Failed Events for Posture – Provides vital information for effective triage during failed connection attempts.

For information about the size of a log file, see Estimate the Size of a Log.

Examples

This is an example of Secure Access VPN log of a **CONNECTED** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons,log message,asa syslog severity,asa syslog class,asa syslog
```

```
 description
"2024-09-11
21:40:51","hostname","user-1","CONNECTED","[296958]","7","sample-uid","2368","35","us","","48","TK2","CiscoSecureAccessVPN","24.23.32.23","10.10.1.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","[]","AAA
 Marking param1 server param2 as FAILED","5","INFORMATION","AAA-ERROR"
```

This is an example of Secure Access VPN log of a **DISCONNECTED** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons,log message,asa syslog severity,asa syslog class,asa syslog
 description
"2024-09-11
22:25:21","hostname","user-1","DISCONNECTED","[296958]","7","sample-uid","2368","35","us","","48","TK2","CiscoSecureAccessVPN","24.23.32.23","10.10.1.10","2024-09-11 19:40:51","User
 Requested","Mac OS X
14.6.1","5.0.05040","ASA-4-113019","DEVICE-M-F1PG","","n/a","n/a","10","","","[]","AAA
 Marking param1 server param2 as FAILED","5","INFORMATION","AAA-ERROR"
```

This is an example of Secure Access VPN log of a failed **AUTHORIZATION-CHECK** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons,log message,asa syslog severity,asa syslog class,asa syslog
 description
"2024-09-11
21:40:51","hostname","user-1","FAILED","[296958]","7","sample-uid","2368","35","us","","48","TK2","CiscoSecureAccessVPN","24.23.32.23","10.10.1.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","\["AUTHORIZATION-CHECK"\]","AAA
 Marking param1 server param2 as FAILED","5","INFORMATION","AAA-ERROR"
```

This is an example of Secure Access VPN log of a failed **CERT-AUTH-CHECK** event:

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons,log message,asa syslog severity,asa syslog class,asa syslog
 description
"2024-09-11
21:40:51","hostname","user-1","FAILED","[296958]","7","sample-uid","2368","35","us","","48","TK2","CiscoSecureAccessVPN","24.23.32.23","10.10.1.10","","","Mac
 OS X
14.6.1","5.1.2.42","ASA-5-109201","DEVICE-M-L9XH","","n/a","n/a","10","","","\["CERT-AUTH-CHECK"\]","AAA
 Marking param1 server param2 as FAILED","5","INFORMATION","AAA-ERROR"
```

Order of Fields in the RAVPN Log

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Host Name","AWS Region","Event Type","Origin IDs","Origin
Type","User ID","Organization ID","Retention Days","Storage Location","MSP
Organization ID","Session ID","Session Type","VPN Profile","Public IP","Assigned
 IP","Connected At","Disconnection Reason","OS Version","Any Connect
Version","ASA Syslog ID","Device ID","Machine ID","Public IPv6","Assigned
IPv6","Security Group Tag","DAP Record Name","DAP Connection Type","Failed
Reasons","AAA Marking param1 server param2 as
FAILED","5","INFORMATION","AAA-ERROR"
```

Log Format

The CSV fields in the header row of the RAVPN logs.

```
timestamp,hostname,aws region,event type,origin ids,origin type,user
id,organization id,retention days,storage location,msp organization id,session
 id,session type,vpn profile,public ip,assigned ip,connected at,disconnection
 reason,os version,anyconnect version,asa syslog id,device id,machine id,public
 ipv6,assigned ipv6,security group tag,dap record name,dap connection
type,failed reasons,log message,asa syslog severity,asa syslog class,asa syslog
 description
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the RAVPN event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.'	v9
hostname	The name of the node on the Cisco headend side where user VPN connections are established and events are generated.	v9
aws region	The AWS region that stores your VPN logs.	v9

Field name	Description	Release version
event type	The label that describes the type of event. Valid values are: `CONNECTED`, `DISCONNECTED`, `FAILED`, or `UNKNOWN`.	v9
origin ids	The internal IP address of the device that connected to the Secure Access remote VPN services.	v9
origin type	The type of device connected to the Secure Access VPN services.	v9
user id	The ID of the VPN user. The ID is the email address associated with the user account.	v9
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID .	v9
retention days	The number of days that AWS S3 stores your Secure Access VPN log.	v9
storage location	The two-character label that identifies the location of your Cisco-managed VPN logs. Configure the storage location on Secure Access for your organization. The storage location options are: eu or us.	v9
msp organization id	The Secure Access managed organization ID.	v9
session id	The unique ID of the VPN session.	v9
session type	The protocol used by the device with the VPN session, for example: `TLS`.	v9
vpn profile	The name of the VPN connection profile that establishes a VPN session.	v9
public ip	The public IP address of the device with the Cisco Secure Client and VPN module.	v9
assigned ip	The IP address assigned to the device with the Cisco Secure Client and VPN module.	v9
connected at	The date and time of the start of the initial `CONNECTED` VPN event for a `DISCONNECTED` event expressed in milliseconds as a UTC-formatted string.	v9
disconnection reason	The description of the VPN disconnected event. The value is `null` for other event types.	v9
os version	The type and version of the user device's operating system.	v9

Field name	Description	Release version
anyconnect version	The version of the Cisco Secure Client with the VPN module.	v9
asa syslog id	The ID of the Cisco ASA syslog used to generate this log event.	v10
device id	The ID of the device with the Cisco Secure Client and VPN module.	v10
machine id	The ID of the client machine used for authentication.	v10
public ipv6	The public IP v6 address of the device with the Cisco Secure Client and VPN module.	v10
assigned ipv6	The IP v6 address assigned to the device with the Cisco Secure Client and VPN module.	v10
security group tag	Security group tag matched as a source by a rule.	v10
dap record name	The posture profile assessed by Cisco Secure Client HostScan.	v10
dap connection type	The RAVPN session connection type.	v10
failed reasons	The error codes for failed remote connection requests.	v10
log message	Log message details communications between devices involved in 802.1X port-based network access. This message is used to troubleshoot issues with authentication, authorization, and accounting (AAA) processes, including RADIUS servers.	v12
asa syslog severity	The severity level of the event. Syslog severity levels range from 0 (Emergency) to 7 (Debug), with lower numbers indicating higher severity. The levels are: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7).	v12
asa syslog class	The syslog message class categorizes syslog messages by type, representing a device's feature or function. For example, the 'auth' class denotes user authentication. You can use syslog message classes to specify an output location for an entire category of syslog messages or to create a message list that specifies the message class.	v12

Field name	Description	Release version
asa syslog descriptor	The syslog message format typically includes a timestamp, a hostname or IP address, facility code, severity level, and the actual log message content, all of which are used for system logging and analysis.	v12

Web Log Formats

Describes Web Log Formats in Cisco Secure Access. The Cisco Secure Access Web logs show your organization's traffic through the Secure Access proxy.

The Cisco Secure Access Web logs show your organization's traffic through the Secure Access proxy. For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of a Web log event:

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer,msp
organization id,geo location of blocked destination countries,application
ids,hostname,data center,egress,server name,time based rule,security
overridden,detected response file type,warn categories,organization
id,application entity name,application entity category, egress iP, ai model
name, ai supply chain categories, event correlation id, isolation profile id,
 source country
"2025-01-06
13:39:24","SIG-Server","10.XXX","10.XXX","10.XXX","","ALLOWED","https://example.com/","","","200","157","641","","","Software/Technology,Allow
 List,Computers and Internet","","","","","","Network
Tunnels","","SIG2-EX,RTO-XXXX-SIG","Network Tunnels,Internal
Networks,Unknown","","","","","","
```

```
 Hash","Categories","AV Detections","PUAs","AMP Disposition","AMP Malware
Name","AMP Score","Policy Identity Type","Blocked
Categories","Identities","Identity Types","Request Method","DLP
Status","Certificate Errors","File Name","Ruleset ID","Rule ID","Destination
List IDs","Isolate Action","File Action","Warn Status","Forwarding
Method","Producer","MSP Organization ID","Geo Location Of Blocked Destination
 Countries","Application IDs","Host Name","Data Center","Egress","Server
Name","Time Based Rule","Security Overridden","Detected Response File
Type","Warn Categories","Organization ID","Application Entity Name","Application
 Entity Category", "Egress IP","AI Model Name","AI Supply Chain
Categories","Event correlation ID", "Isolation profile ID", "source country"
```

Log Format

The CSV fields in the header row of the Web log.

```
timestamp,policy identity label,internal client ip,external client
ip,destination ip,content type,action,url,referer,user agent,status code,request
 size,response size,response body size,sha—sha256,categories,av
detections,puas,amp disposition,AMP malware name,amp score,policy identity
type,blocked categories,identities,identity types,request method,dlp
status,certificate errors,file name,ruleset id,rule ID,destination list
ids,isolate action,file action,warn status,forwarding method,producer,msp
organization id,geo location of blocked destination countries,application
ids,hostname,data center,egress,server name,time based rule,security
overridden,detected response file type,warn categories,organization
id,application entity name,application entity category, egress ip,ai model
name,ai supply chain categories,event correlation id,isolation profile id,source
 country
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the Web traffic event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v1
policy identity label	The identity that made the request.	v1
internal client ip	The internal IP address of the computer making the request.	v1
external client ip	The egress IP address of the network where the request originated.	v1
destination ip	The destination IP address of the request.	v1

Field name	Description	Release version
content type	The type of web content, typically `text/html`.	v1
action	Whether the request was allowed, blocked, or trusted.	v1
url	The URL requested.	v1
referer	The referring domain or URL.	v1
user agent	The browser agent that made the request.	v1
status code	The HTTP status code; should always be `200` or `201`.	v1
request size	Request size in bytes.	v1
response size	Response size in bytes.	v1
response body size	Response body size in bytes.	v1
sha–sha256	The hex digest of the response content.	v1
categories	The security categories for this request, such as `Malware`.	v1
av detections	The detection name according to the antivirus engine used in file inspection.	v1
puas	A list of all potentially unwanted application (PUA) results for the proxied file as returned by the antivirus scanner.	v1
amp disposition	The status of the files proxied and scanned by Cisco Advanced Malware Protection (AMP) as part of the File Inspection feature; can be `Clean`, `Malicious` or `Unknown`.	v1
amp malware name	If Malicious, the name of the malware according to AMP.	v1
amp score	The score of the malware from AMP. This field returns blank (`""`) unless the verdict is Unknown, in which the value will be `0`.	v1
policy identity type	The first identity type that made the request. Examples: `Roaming Computer`, `Network`.	v1
blocked categories	The category that resulted in the destination being blocked.	v4
identities	All identities associated with this request.	v5
identity types	The type of identities that were associated with the request. Examples: `Roaming Computer`, `Network`.	v5

Field name	Description	Release version
request method	The HTTP request method. Examples: `GET`, `POST`, `HEAD`, `PUT`, `DELETE`.	v5
dlp status	If the request was Blocked for DLP.	v6
certificate errors	Any certificate or protocol errors in the request.	v6
file name	The name of the file.	v6
ruleset id	The ID number assigned to the ruleset.	v6
rule id	The ID number assigned to the rule.	v6
destination list ids	The ID number assigned to a destination list.	v6
isolate action	The remote browser isolation state associated with the request.	v8
file action	The action taken on a file in a remote browser isolation session. Valid values are: `UNKNOWN`, `DETECT`, `BLOCK`, `MALWARE_CLOUD_LOOKUP`, `MALWARE_WHITELIST`, `CLOUD_LOOKUP_TIMEOUT`, `CUSTOM_DETECTION`, `CUSTOM_DETECTION_BLOCK`, `ARCHIVE_BLOCK_DEPTH_EXCEEDED`, `ARCHIVE_BLOCK_ENCRYPTED`, `ARCHIVE_BLOCK_FAILED_TO_INSPECT`, `TID_BLOCK`	v8
warn status	The Warn page's state associated with the request.	v8
forwarding method	The method used to forward the proxy events. Example: `Secure Web Appliance`.	v9
producer	The producer of the proxy events.	v9
msp organization id	The Secure Access parent organization ID.	v10
geo location of blocked destination countries	The ISO-3166 IDs of one or more countries where destination IPs blocked by policy are located.	v10
application ids	The ID of the destination application.	v10
hostname	The hostname of the user device.	v10
data center	The name of the data center that processed the user-generated traffic.	v10
egress	`TRUE` indicates that the egress IP was a reserved IP.	v10

Field name	Description	Release version
server name	The name of the server according to the TLS protocol server name indication (SNI), if present, or from the server's SAN certificate common name (CN).	v10
time based rule	`TRUE` indicates that a the rule was applied due to a time condition.	v10
security overridden	`TRUE` indicates that security filtering was explicitly overridden and not applied during enforcement.	v10
detected response file type	The file type that resulted in a blocked response. Examples: `exe`, `avi`.	v10
warn categories	The ID of one or more content categories in lists matched for a Warn action by the rule.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10
application entity name	The specific name of an application entity within the system. This field is used exclusively for YouTube Tenant Control.	v11
application entity category	The classification grouping of application entities based on shared characteristics. This field is used exclusively for YouTube Tenant Control.	v11
egress ip	The public IP address assigned to a session as it exits the Secure Access ZTA infrastructure en route to the destination application.	v12
ai model name	Indicates the name of the AI model involved in the transaction or event.	v13
ai supply chain categories	The list of AI supply chain categories associated with the event. Valid values are: `PROHIBITED SUPPLIERS`, `CODE EXECUTION`, and `COPYLEFT LICENSE`	v13
event correlation id	A unique identifier generated for each network request, the Event Correlation ID stitches together all related events across various security services (Firewall, SWG, ZTNA) to provide a unified, end-to-end view of a single traffic flow.	v14

Field name	Description	Release version
isolation profile id	The unique identifier for the isolation profile applied to the session. This profile determines the specific browser isolation policies enforced for the user's web traffic.	v16
source country	The ISO 3166 alpha 2 two character identifier of the country associated with the source IP.	v17

Zero Trust Access Log Formats

Describes Zero Trust Access Log Formats in Cisco Secure Access. The Cisco Secure Access Zero Trust Access logs show your organization's traffic through the Secure Access Zero Trust Access services.

The Cisco Secure Access Zero Trust Access logs show your organization's traffic through the Secure Access Zero Trust Access services. ZTA logs include traffic events that take place at the time of ZTA session authentication for both client-based and browser-based ZTA sessions. For logs that show traffic events that take place after successful ZTA session authentication, see Zero Trust Access Flow Log Formats.

For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of a Zero Trust Access log event:

```
timestamp,identity email,identity labels,identity type
labels,hostname,verdict,client os,client browser,client geo location,client
ip,ruleset id,rule id,private app group id,private app id,private resource
id,private resource group id,step up auth type,step up auth result,step up
auth token life,posture id,requested id fqdn,resolved ip,app connector group
id,headend type,duo device id,duo device id string,system password,client
firewall,disk encryption,anti malware agents,transaction id,block
reason,application port,application protocol,tunnel type,secure client
version,possible match ruleset id,possible match rule id,possible match
posture,source process id,source process name,source process hash,source process
 user name,organization id,ad joined id,enforced by,ftd enforcement id,ftd
enforcement name,mdm source,mdm device id,mdm is managed,mdm is compliant,mdm
 last updated,applied trusted network,detected trusted network,zta profile
id,egress ip
"2017-10-02 23:52:53","network@example.com","Network. AD
Computer","Networks","ts-auto.com","ALLOW","Mac OS 10.9.5","Chrome
99","aaa","10.10.1.5","1.2.3.4","US","CA","SAN JOSE","37.3387","-121.8853","1.1.1.1","5","TA","2a4e2e68a0e4e9","aaa[10]","SS","HRAY","cisco
 1.20.0.877, windows-defender
1.0.87","e2a4e2e68a0e4e9","8","TP","HP","","","","","","","","8554","ED","123132","AF","23432","ue","ue","1674653","Sw24","Sw42",
 Verizon6","12345","2.2.2.2"
```

Order of Fields in Zero Trust Access Logs

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Identity Email","Identity Labels","Identity Type Labels","Host
Name","Verdict","Client OS","Client Browser","Client Geolocation","Client
IP","Ruleset ID","Rule ID","Private App Group ID","Private App ID","Private
Resource ID","Private Resource Group ID","Step Up Auth Type","Step Up Auth
Result","Step Up Auth Token Life","Posture ID","Requested ID FQDN","Resolved
IP","App Connector Group ID","Headend Type","Duo Device ID","Duo Device ID
String","System Password","Client Firewall","Disk Encryption","Anti Malware
Agents","Transaction ID","Block Reason","Application Port","Application
Protocol","Tunnel Type","Secure Client Version","Possible Match Ruleset
ID","Possible Match Rule ID","Possible Match Posture","Source Process
ID","Source Process Name","Source Process Hash","Source Process User
Name","Organization ID","Ad Joined ID","Enforced By", "FTD enforcement ID",
"FTD Enforcement Name", "MDM Source", "MDM Device ID", "MDM Is Managed", "MDM
 Is Compliant", "MDM Last Updated", "Applied Trusted Network", "Detected Trusted
 Network", "ZTA Profile ID", "Egress IP"
```

Log Format

The CSV fields in the header row of the Zero Trust Access log.

```
timestamp,identity email,identity labels,identity type
labels,hostname,verdict,client os,client browser,client geo location,client
ip,ruleset id,rule id,private app group id,private app id,private resource
id,private resource group id,step up auth type,step up auth result,step up
auth token life,posture id,requested id fqdn,resolved ip,app connector group
id,headend type,duo device id,duo device id string,system password,client
firewall,disk encryption,anti malware agents,transaction id,block
reason,application port,application protocol,tunnel type,secure client
version,possible match ruleset id,possible match rule id,possible match
posture,source process id,source process name,source process hash,source process
 user name,organization id,ad joined id,enforced by,ftd enforcement id,ftd
enforcement name,mdm source,mdm device id,mdm is managed,mdm is compliant,mdm
 last updated,applied trusted network,detected,trusted network,zta profile
id,egress ip
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the ZTA event, expressed as a UTC-formatted string (e.g., `2024-01-16 17:48:41`). **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v9
identity email	The email address of the Active Directory user.	v9
identity labels	The list of labels for the identity.	v9
identity type labels	The label of the identity type.	v9
hostname	The hostname of the user device.	v9
verdict	Whether the user has access to a resource.	v9
client os	The operating system of the user device.	v9
client browser	The name of the browser on the user device.	v9
client geo location	The regional location of the user device.	v9
client ip	The IP address of the user device.	v9
ruleset id	The ID of the ruleset.	v9
rule id	The ID of the access rule.	v9
private app group id	The ID of the private application group.	v9
private app id	The ID of the private application.	v9
private resource id	The ID that Secure Access assigns to the customer-defined private application.	v9
private resource group id	The ID if the rule matched is based on the private application group.	v9
step up auth type	The type of authentication. Valid values are: `SAML_SSO`, `MFA`, or `NONE`.	v9
step up auth result	The result of the authentication. Valid values are: `SUCCESS` or `FAILURE`.	v9
step up auth token life	The time in seconds between when you generated the token and used the token.	v9
posture id	ID of the matching posture profile.	v9

Field name	Description	Release version
requested id fqdn	The IP or FQDN of the requested application.	v9
resolved ip	The IP of the application returned by the proxy.	v9
app connector group id	The group ID of the App Connector.	v9
headend type	The type of the headend. Valid values are: `CLAP` or `BAP`.	v9
duo device id	The ID of the Duo App on the device.	v9
duo device id string	The ID label of the Duo App on the device.	v9
system password	Whether the system password is enabled with its timeout in seconds.	v9
client firewall	The client system firewall. Valid values are `SYS` or `NONE`.	v9
disk encryption	The client Disk Encryption Type. Valid values are: `SYS`, `NONE` or `THIRD PARTY`.	v9
anti malware agents	The clients' anti malware agents.	v9
transaction id	A unique identifier generated by the Secure Client for each network request. The Transaction ID serves as the event correlation mechanism in ZTNA, unifying related events across security services (Firewall, SWG, ZTNA) to provide an end-to-end view of a single traffic flow. For a browser-based connection, the authorization, establishment, and termination records share the same Transaction ID. In Events, use the Event ID to display these records. **Note** The Event Correlation ID is not used in ZTNA, as its functionality is covered by the Transaction ID field. Note:	v10
block reason	The reason for the transaction being blocked. (e.g., `Android OS not allowed`)	v10
application port	The port of the destination application.	v10

Field name	Description	Release version
application protocol	The type of protocol used for transactions. (e.g., `TCP`)	v10
tunnel type	The type of tunnel used to connect to the ZTA proxy. Valid values are: `HTTP2`, `HTTP3`	v10
secure client version	The version of the Cisco Secure Client on the endpoint device accessing a private resource.	v10
possible match ruleset id	For a block event, the ID of the ruleset that could have allowed the transaction if not for the block reason.	v10
possible match rule id	For a block event, the ID of the rule within the ruleset that could have allowed the transaction if not for the block reason.	v10
possible match posture	For a block event, the posture that could have allowed the transaction if not for the block reason.	v10
source process id	The ID of the source process that initiated the transaction from the client side.	v10
source process name	The name of the source process that initiated the transaction from the client side (e.g., `chrome.exe`).	v10
source process hash	The hash of the source process that initiated the transaction from the client side.	v10
source process user name	The user name associated with the source process that initiated the transaction from the client side.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10
ad joined id	ID of the device if it is joined to an Active Directory domain.	v10
enforced by	The Secure Access component or service that enforced the policy or control related to this event (e.g., Firewall, Web Proxy).	v12
ftd enforcement id	The unique identifier of the enforcement action taken by a Firepower Threat Defense (FTD) device integrated with Secure Access.	v12

Field name	Description	Release version
ftd enforcement name	The name or type of enforcement action taken by a Cisco Secure Firewall Threat Defense device that is integrated with Secure Access, for example, Malware Block and URL Category Block.	v12
mdm source	The specific Mobile Device Manager (MDM) platform integrated with Secure Access providing device management and compliance information (e.g. Cisco Meraki Systems Manager)	v12
mdm device id	The unique identifier assigned to the device by the integrated MDM platform, enabling Secure Access to track and manage the device's access privileges.	v12
mdm is managed	Indicates whether the device is currently under active management by the integrated MDM platform: `TRUE` or `FALSE`	v12
mdm is compliant	Indicates whether the device meets the compliance policies defined within the integrated MDM platform: `TRUE` or `FALSE`	v12
mdm last updated	The date and time that Secure Access last received updated device information from the integrated MDM platform.	v12
trusted network	The trusted network that was applied during policy enforcement.	v13
detected trusted networks	A list of trusted networks that were detected by the client during the event.	v13
zta profile id	The unique identifier of the applicable ZTA profile associated with the event.	v13
egress ip	The public IP address assigned to a session as it exits the Secure Access ZTA infrastructure toward the destination application. For network tunnel backhauls, the destination network sees this address as the source IP address of the connection. For Resource Connector backhauls, this field does not represent the source IP address seen by the destination network.	v13

Zero Trust Access Flow Log Formats

Describes Zero Trust Access Flow Log Formats in Cisco Secure Access. The Cisco Secure Access Zero Trust Access (ZTA) flow logs show your organization's traffic through the Secure Access ZTA services.

The Cisco Secure Access Zero Trust Access (ZTA) flow logs show your organization's traffic through the Secure Access ZTA services.

ZTA flow logs show traffic after successful authentication for clientbased and browserbased sessions. For browserbased access, each TCP connection has establishment and termination records. Match Transaction IDs to correlate these records with authorization logs. One application session can use several connections. Use log format version 10 or later. For information about the size of a log file, see Estimate the Size of a Log.

Example

This is an example of a Zero Trust Access flow log event:

```
timestamp,identity email,identity labels,identity type labels,organization
id,msp organization id,hostname,transaction ID,private resource id,private
resource group id,app connector id,app connector group id,ruleset id,rule
id,connection status,connection failure reason,headend type,event
type,rxbytes,txbytes,egress ip,egress port,nt group id,zta source port,enforced
 by,ftd enforcement id,ftd enforcement name
"2026-08-28
12:34:56","alice@example.com","alice@example.com","managed-device-123","AD
Users","Managed
Devices","1001","","zta-host","txn-abc-123","99","88","77","66","55","44","TERMINATED","Test","CA","CONCLUDE","124","248","10","43","33","80","Enforcement
 Point","ftd-123","FTD Device"
```

Order of Fields in Zero Trust Access Flow Logs

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header.

```
"Timestamp","Identity Email","Identity Labels","Identity Type
Labels","Organization ID","MSP Organization ID","Host Name","Transaction
ID","Private Resource ID","Private Resource Group ID","App Connector ID","App
 Connector Group ID","Ruleset ID","Rule ID","Connection Status","Connection
Failure Reason","Headend Type","Event Type","Rx Bytes","Tx Bytes","Egress
IP","Egress Port","NT Group ID","ZTA Source Port","Enforced By", "FTD
enforcement ID", "FTD Enforcement Name"
```

Log Format

The CSV fields in the header row of the Zero Trust Access flow log.

```
timestamp,identity email,identity labels,identity type labels,organization
id,msp organization id,hostname,transaction ID,private resource id,private
resource group id,app connector id,app connector group id,ruleset id,rule
id,connection status,connection failure reason,headend type,event
type,rxbytes,txbytes,egress ip,egress port,nt group id,zta source port,enforced
 by,ftd enforcement id,ftd enforcement name
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the ZTA event, expressed as a UTC-formatted string (e.g., `2025-01-16 17:48:41`). For browser-based flow records, the timestamp identifies establishment or termination according to Connection Status. Termination is not necessarily application logout. **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v10
identity email	The email address of the Active Directory user.	v10
identity labels	The list of labels for the identity.	v10
identity type labels	The label of the identity type.	v10
organization id	The Secure Access organization ID. For more information, see Find Your Organization ID.	v10
msp organization id	The Secure Access organization ID of the parent managed service provider.	v10
hostname	The hostname of the user device.	v10
transaction id	Universally unique identifier (UUID) of the transaction associated with the event.	v10
private resource id	The ID that Secure Access assigns to the customer-defined private application.	v10
private resource group id	The ID if the rule matched is based on the private application group.	v10
app connector id	The ID of the App Connector.	v10
app connector group id	The group ID of the App Connector.	v10
ruleset id	The ID of the ruleset.	v10
rule id	The ID of the access rule.	v10
connection status	The status of the request to connect to the private resource. Valid values are: `Connected`, `Reset`, `Terminated`, or `Unknown`. For browser-based ZTA, Connected marks establishment; Terminated marks closure.	v10

Field name	Description	Release version
connection failure reason	The error codes for failed connection requests.	v10
headend type	The type of the headend. Valid values are: `CLAP` or `BAP`.	v10
event type	The type of flow event. Valid values are: DNS_FAILURE_CONNECTIVITY, DNS_FAILURE_RESOLUTION, CONN_FAILURE, CONN_SUCCESS, APP_INVALID_DESTINATION, APP_PORT_MISMATCH, APP_PROTOCOL_MISMATCH	v10
rxbytes	The number of bytes received during the session. For browserbased ZTA, final totals are available at termination.	v10
txbytes	The number of bytes transmitted or sent during the session. For browser-based ZTA, final totals are available at termination.	v10
egress ip	The egress IP address is not included in the flow logs and appears as empty. However, it can be found in the ZTA logs using the same transaction ID.	
egress port	The egress port number of the network where the request originated.	v10
nt group id	The tunnel ID associated with this request.	v10
zta source port	The port number used by the Zero Trust proxy service to connect to an unmanaged device requesting a connection to a private resource.	v10
enforced by	The Secure Access component or service that enforced the policy or control related to this event (e.g., Firewall, Web Proxy).	v12
ftd enforcement id	The unique identifier of the enforcement action taken by a Firepower Threat Defense (FTD) device integrated with Secure Access.	v12
ftd enforcement name	The name or type of enforcement action taken by a FTD device integrated with Secure Access (e.g., Malware Block, URL Category Block).	v12
source ip	The source IP address of the client endpoint for the Zero Trust Access flow.	v18
destination ip	The destination IP address for the flow.	v18

Field name	Description	Release version
application protocol	The application layer protocol used by the flow. Example: `HTTPS`.	v18

Zero Trust Access Enrollment Log Formats

Describes Zero Trust Access Enrollment Log Formats in Cisco Secure Access. The Cisco Secure Access Zero Trust Access (ZTA) flow logs provide a detailed account of events relating to ZTA services.

The Cisco Secure Access Zero Trust Access (ZTA) flow logs provide a detailed account of events relating to ZTA services. From version 13, Secure Access introduces a new log format specifically designed for ZTA enrollment events. These logs capture the details of enrollment and unenrollment transactions, enabling administrators to monitor the enrollment process and troubleshoot potential issues effectively.

Example

This is an example of a ZTA enrollment log event:

```
timestamp,identity email,identity labels,identity type labels,organization
id,msp organization id,enrollment id,event type,enrollment method,event
detail,os type & version,zta client version,event status,device id,public ip
"2017-10-02 23:52:53","tom@abc.com","tom@abc.com", "Network". "AD
Computer","Networks","ts-auto.com","1234567","1234567","Gd2o4Dr9PBERUpCvvAneaKoBqA6Di4Io","ENROLL","SAML","Failed
 to enroll","Mac OS 10.9.5","5.1.0.0","Successfully enrolled","12345","1.1.1.1"
```

Order of Fields in ZTA Enrollment Logs

> **Note**
>
> Not all the fields that are listed are found in most or all requests. When a field does not have a value, Secure Access sets the field to the empty string ("") in the log.

Optional Log Header Format

The CSV fields in the header row of the Optional Log header are as follows:

```
"Timestamp","Identity Email","Identity Labels","Identity Type
Labels","Organization ID","MSP Organization ID","Enrollment ID","Event
Type","Enrollment Method","Event Detail","OS Type & Version","ZTA Client
Version","Event Status","Device ID","Public IP"
```

Log Format

The CSV fields in the header row of the ZTA enrollment log are as follows:

```
timestamp,identity email,identity labels,identity type labels,organization
id,msp organization id,enrollment id,event type,enrollment method,event
detail,os type & version,zta client version,event status,device id,public ip
```

The following table describes each field and the log version in which it was released across all supported versions. For more information about log versions, see Find Your Log Schema Version.

Field name	Description	Release version
timestamp	The date and time of the ZTA enrollment event, displayed as a UTC-formatted string, for example, `2026-01-16 17:48:41`. **Note** Unlike the Secure Access dashboard and reports, Secure Access logs do not convert the timestamp to your local timezone.	v13
identity email	The email address of the Active Directory user initiating the enrollment or unenrollment.	v13
identity labels	The list of labels associated with the identity.	v13
identity type labels	The label specifying the identity type.	v13
organization id	The unique identifier for the Secure Access organization. For more information, see Find Your Organization ID.	v13
msp organization id	The Secure Access organization ID of the parent-managed service provider.	v13
enrollment id	The unique transaction ID for the enrollment or unenrollment process.	v13
event type	The type of enrollment event. Valid values are: `ENROLL` or `UNENROLL`.	v13
enrollment method	The authentication method used for enrollment. Valid values are: `SAML`, `CERTIFICATE`, or `BOTH`.	v13
event detail	Additional context for the event, including reasons for enrollment failure.	v13
os type & version	The operating system name and version of the client device.	v13
zta client version	The version of the ZTA client installed in the device.	v13
event status	The status of the enrollment event, for example, successfully enrolled or failure status details.	v13
device id	The unique identifier assigned to the enrolled or unenrolled device.	v13
public ip	The public IP address of the client device.	v13

69 Monitor with Alert Rules

Topics:

- Monitor Secure Access with Alert Rules

Provides an overview of Monitor with Alert Rules in Cisco Secure Access, including Monitor Secure Access with Alert Rules. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Monitor Secure Access with Alert Rules

Describes Monitor Secure Access with Alert Rules. Cisco Secure Access Alert Rules assist you with the task of actively monitoring Secure Access resources.

Cisco Secure Access Alert Rules assist you with the task of actively monitoring Secure Access resources.

You can monitor:

- IPsec tunnels in Network Tunnel Groups.
- The usage of your Secure Access API keys and the Secure Access API.
- Interactions of end users in the organization with online applications.
- Changes to the internet and private access rules in the organization's Access policy.

Guidelines

- Secure Access supports at most 100 Alert Rules.
- Secure Access supports the configuration of 50 email recipients in an Alert Rule.

Get Started

To get started, add an Alert Rule in Secure Access and set up a Secure Access Webhook, or configure email recipients to receive the alert messages.

A Secure Access Webhook sends notifications to a target HTTP service deployed in the organization's on-premises or cloud environment.

When an event occurs and a condition is met for the configured Alert Rule, Secure Access raises an alert and sends a notification.

- Add and Edit Alert Rules for API Anomalies
- Add and Edit Alert Rules for Behavior Analytics
- Add and Edit Alert Rules for Tunnel Connectivity
- Add and Edit User Access Alerts
- Add and Edit Alert Rules for Resource Connectors on page 2378
- Manage Alert Rules for Destination Lists

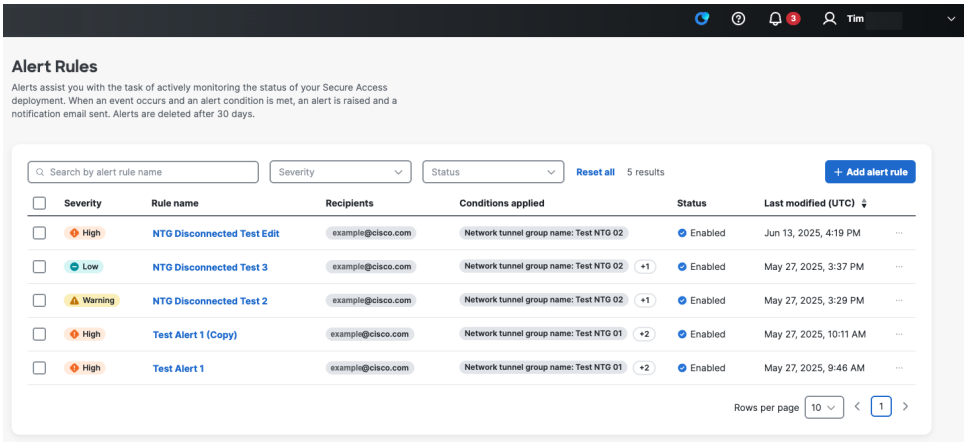
Manage Alert Rules

Provides instructions for completing the Manage Alert Rules workflow in Cisco Secure Access. Manage, create, and modify alert rules from the Alert Rules table.

Manage, create, and modify alert rules from the **Alert Rules** table.

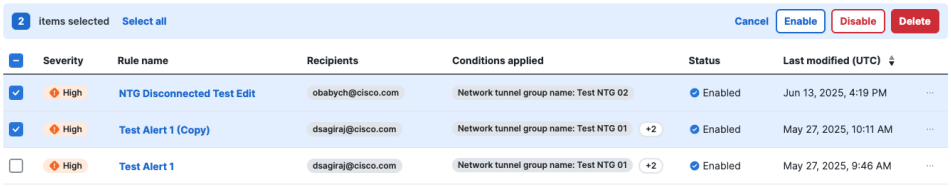
Procedure

1. Navigate to **Monitor** > **Alert Rules**.

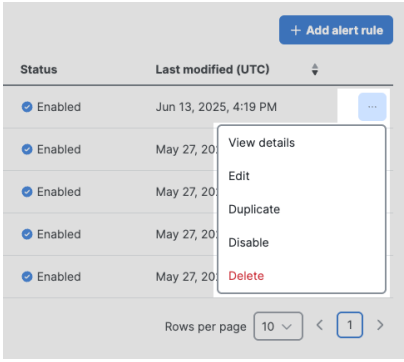


The **Alert Rules** table includes these controls:

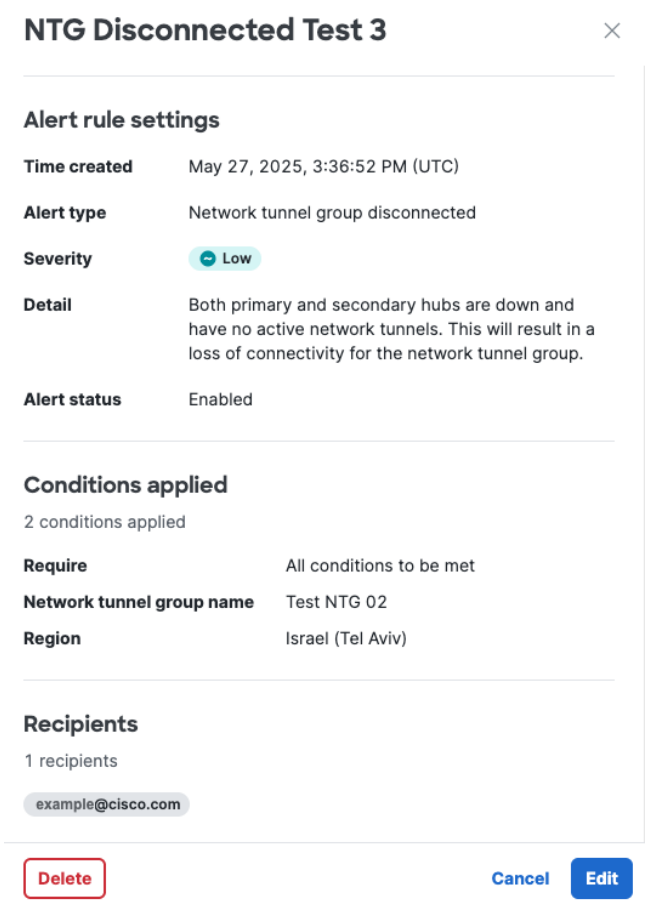
- Search by alert rule name.
- Filter by **Severity**: High, Warning, or Low.
- Filter by **Status**: Enabled or Disabled.
- Add new alert rules.
- Use the checkboxes to select, enable, disable, or delete one or more alert rules.



2. Click a rule's ellipsis icon (...) to view details or edit, duplicate, enable, disable, or delete the rule.



3. Click on an entry under **Rule name** to view more details about an alert rule.



- **Alert rule settings**–Shows when the rule was created and the alert type, severity, detail, and status.
- **Conditions applied**–Shows any conditions configured for this alert rule.
- **Recipients**–Lists the email addresses configured to receive email notifications for this alert.

4. Click **Delete** or **Edit** to manage the alert rule.

Add and Edit Alert Rules for API Anomalies

Add and edit alert rules for API anomalies.

Add an alert rule for a specific condition on the usage of your Secure Access API keys or the Secure Access API.

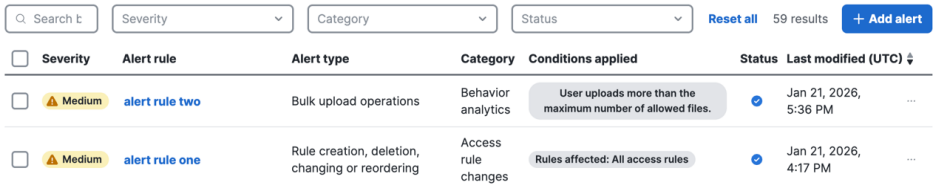
> **Note**
>
> When you edit an alert rule, Secure Access will dismiss any active alerts for that rule.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Alert Rules**.

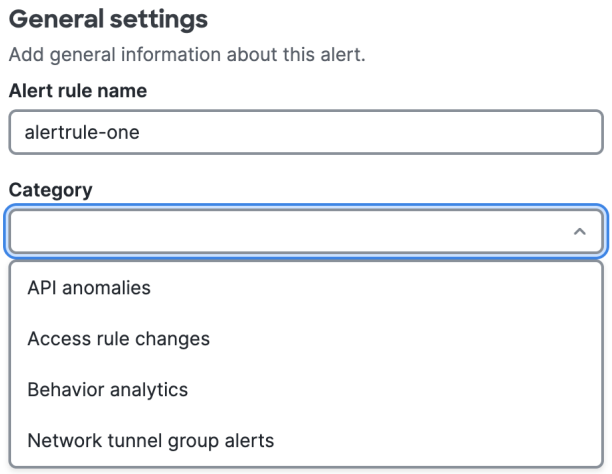


2. On **Alert Rules**, click **+ Add alert** or edit an existing alert rule.

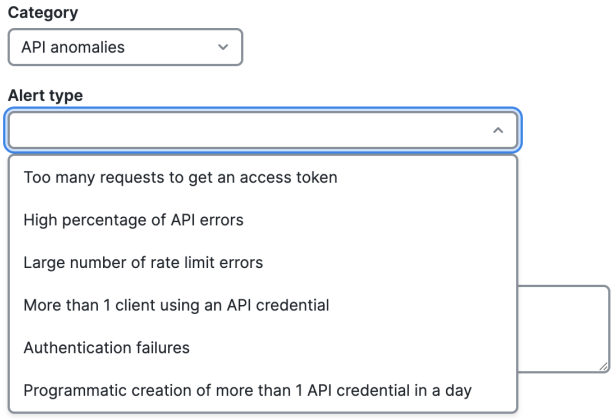
> **Note**
>
> On **General Settings**, you must configure the alert rule name, category, and alert type.

- Alert rule name–The name of the alert.
- Category–The category of the alert.
- Alert type–The type of the alert in the alert category.
- Severity level–The level of severity associated with the alert.
- Description–A meaningful description of the alert.

3. For the **Alert rule name**, enter a sequence of 3-254 alphanumeric, parentheses, and hyphen characters. Choose a meaningful name that begins with an alphanumeric character.

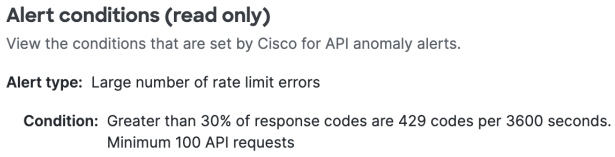


4. For **Category**, choose **API anomalies**.
5. For **Alert type**, choose from the list of alert types for the category.



6. For **Severity level**, choose one of the severity levels for the alert.
   - **High**
   - **Medium**
   - **Low**
   - **Info**
7. For **Description**, enter a sequence of 1-150 characters that describe the alert rule.
8. Click **Next**.

   Secure Access provides the details about the conditions that must be met for the alert to occur.

9. Click **Next**.
10. On **Notifications**, enable the notifications for the alert rule. You can enable **Webhook notifications** and **Email notifications**.

    Secure Access always enables in-product notifications. For more information about in-product notifications, see Monitor Alerts from Secure Access.

    a) Choose **Web notifications** to configure push notifications to a third-party product or service.

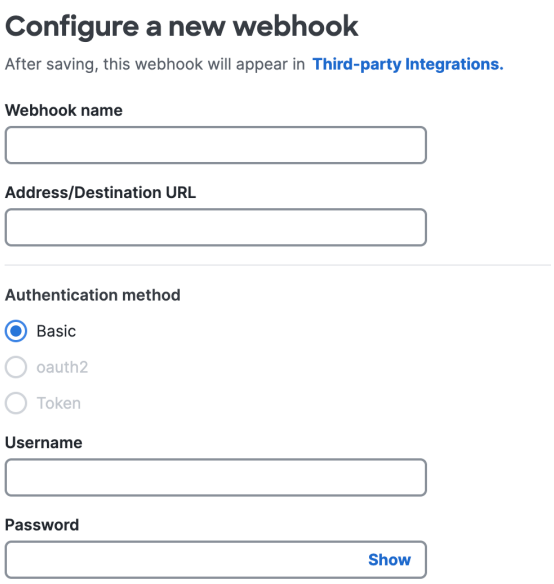
    You can choose from a list of configured webhooks or add a new webhook.

    b) Click on the **Select a webhook** drop-down menu and then choose a webhook from the list of configured webhooks.

    c) Click **+ Configure a new webhook**. After you complete the configuration of the new webhook, click **Save**.

    Complete the configuration of the webhook and add the webhook in the organization. You can add at most 10 webhooks.

    For information about webhooks, see Manage Webhooks for Third-Party Integrations.

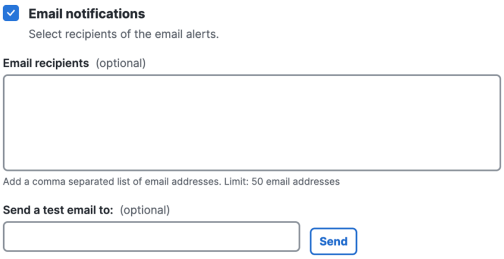


d) Click **Email notifications** to configure notifications to a list of email recipients.

You can configure and send a test notification to the list of email recipients.

e) Add a comma-separated list of email addresses.

> **Note**
>
> You are limited to 50 email addresses.

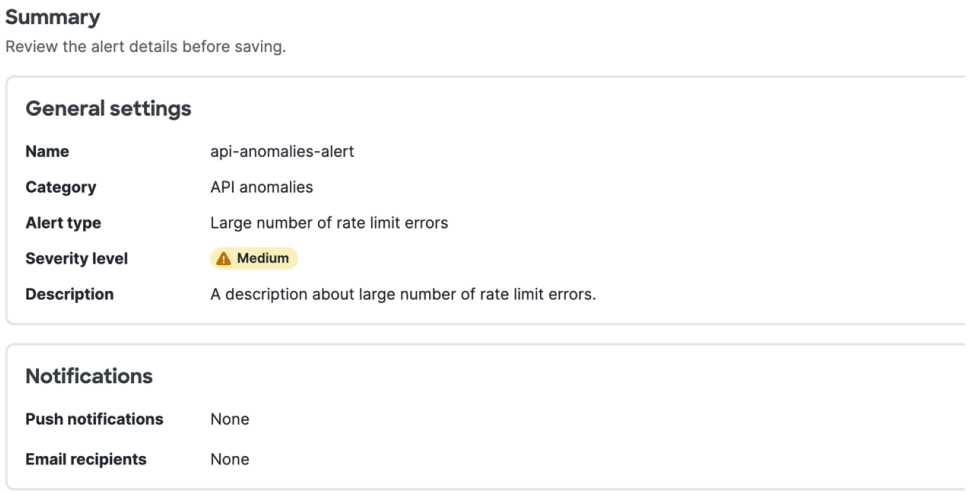


f) (Optional) Enter an email address, and then click **Send**.

Secure Access sends a test alert to evaluate that the email address receives the alert.

11. Click **Next**.

12 On **Summary**, review the **General Settings** and **Notifications**.



13. Click **Save**.

Add and Edit Alert Rules for Changes on Access Rules

Add and edit alert rules to monitor the changes to the access rules in the Access policy.

You can add alert rules in Secure Access to monitor the changes on the internet and private access rules in the Access policy.

After you add an alert rule, Secure Access begins to monitor the conditions defined for the alert. You can view the alerts generated by Secure Access for the alert rules in the organization. For information about viewing alerts in Secure Access, see Monitor Alerts From Secure Access.

Secure Access monitors these changes on access rules:

- The priority of an access rule in the Access policy.
- Additions to the access rules in the Access policy.
- Modifications to the access rules in the Access policy.
- Deletions to the access rules in the Access policy.

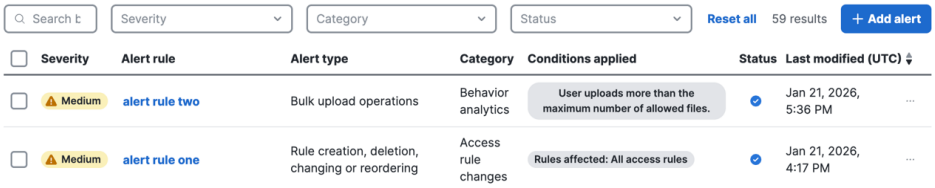
When you edit an alert rule, Secure Access will dismiss any active alerts for that alert rule.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Alert Rules**.



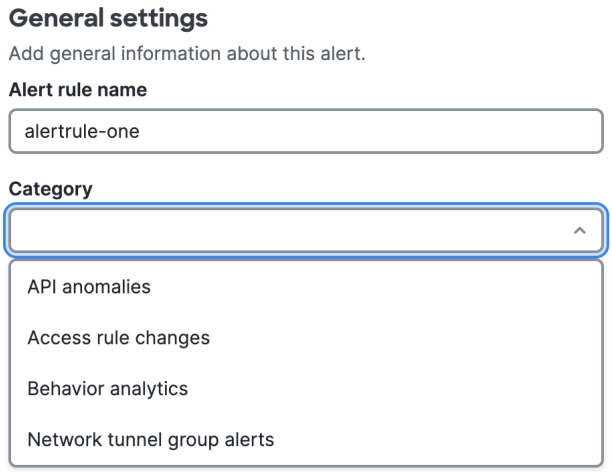
2. On **Alert Rules**, click **+ Add alert** or edit an existing alert rule.

> **Note**
>
> On **General Settings**, you must configure the alert rule name, category, and alert type.

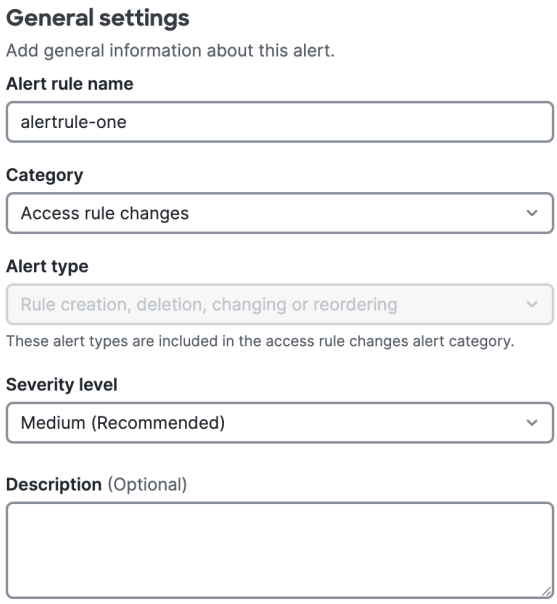
- Alert rule name–The name of the alert.
- Category–The category of the alert.
- Alert type–The type of the alert in the alert category.
- Severity level–The level of severity associated with the alert.
- Description–A meaningful description of the alert.

3. For the **Alert rule name**, enter a sequence of 3-254 alphanumeric, parentheses, and hyphen characters.

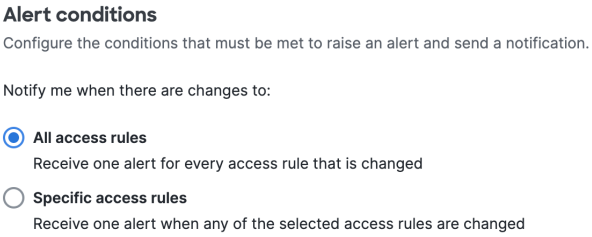
   Choose a meaningful name that begins with an alphanumeric character.



4. For **Category**, choose **Access rule changes**.
5. For **Alert type**, Secure Access enables the monitoring of rule creation, deletion, modifications, and changes to the priority of the internet and private access rules.

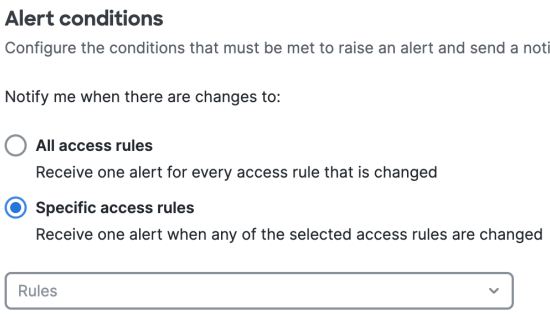


6. For **Severity level**, choose one of the severity levels for the alert.
   - **High**
   - **Medium**
   - **Low**
   - **Info**
7. For **Description**, enter a sequence of 1-150 characters that describe the alert rule.
8. Click **Next**.
9. On **Alert conditions**, choose the conditions that cause the system to create the alert.



   a) Choose **All access rules** to receive an alert every time an internet or private access rule changes.
   b) Choose **Specific access rules**, and then in the **Rules** drop-down menu, choose the access rules.

      For each selected access rule, Secure Access sends an alert to the organization any time the access rule changes.



10. Click **Next**.
11. On **Notifications**, enable the notifications for the alert rule. You can enable **Webhook notifications** and **Email notifications**.

    Secure Access always enables in-product notifications. For more information about in-product notifications, see Monitor Alerts from Secure Access.

    a) Choose **Web notifications** to configure push notifications to a third-party product or service.

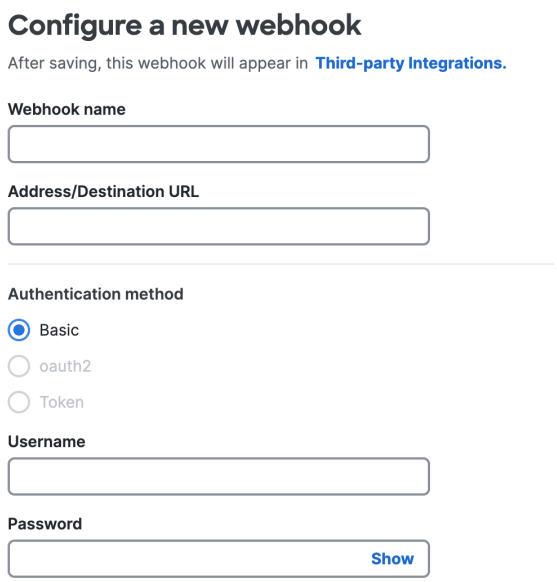
    You can choose from a list of configured webhooks or add a new webhook.

    b) Click on the **Select a webhook** drop-down menu and then choose a webhook from the list of configured webhooks.

    c) Click **+ Configure a new webhook**. After you complete the configuration of the new webhook, click **Save**.

    Complete the configuration of the webhook and add the webhook in the organization. You can add at most 10 webhooks.

    For information about webhooks, see Manage Webhooks for Third-Party Integrations.

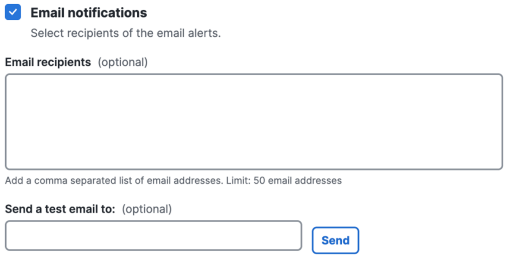


    d) Click **Email notifications** to configure notifications to a list of email recipients.

    You can configure and send a test notification to the list of email recipients.

    e) Add a comma-separated list of email addresses.

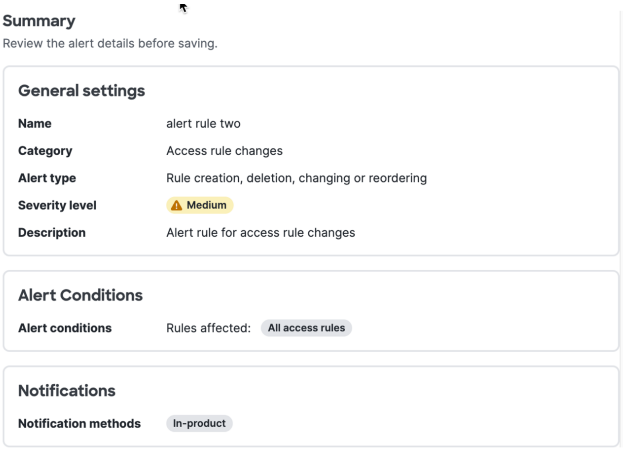
> **Note**
>
> You are limited to 50 email addresses.



f) (Optional) Enter an email address, and then click **Send**.

Secure Access sends a test alert to evaluate that the email address receives the alert.

12. Click **Next**.
13. On **Summary**, review the **General Settings** and **Notifications**.



14. Click **Save**.

Add and Edit Alert Rules for Behavior Analytics

Add and edit alert rules for monitoring end-user behaviors in the organization.

You can add alert rules in Secure Access to monitor the interactions of end users in the organization with internet and private applications. Once you add an alert rule, you can edit or delete the alert rule. Secure Access monitors these activities from end users:

- Anomalous MCP activity
- DLP violation spike
  - DLP rule violation spike
  - DLP classification violation spike
- Failed Private Resource Access Attempts

- Unseen location activities
- File operations
  - Bulk delete operations
  - Bulk download operations
  - Bulk upload operations
- High-risk country file activities
  - Upload to high-risk countries
  - Download from high-risk countries
- Impossible travel
- Traffic spike and destination monitoring
  - TOR traffic spike
  - Destination traffic spike

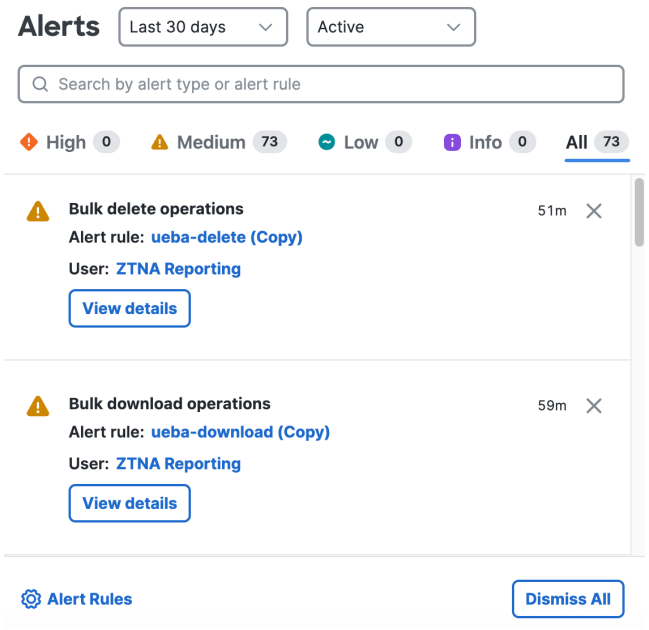
When you edit an alert rule, Secure Access will dismiss any active alerts for that alert rule.

After you add an alert rule, Secure Access begins to monitor the conditions defined for the alert. You can view the alerts generated by Secure Access for the Behavior analytics alert rules in the organization.

In Secure Access, navigate to the toolbar at the top of your browser window.



Click the bell icon to open the Alerts drop-down menu. Secure Access displays the alerts generated for the configured alert rules. For information about viewing alerts in Secure Access, see Monitor Alerts From Secure Access .



Important

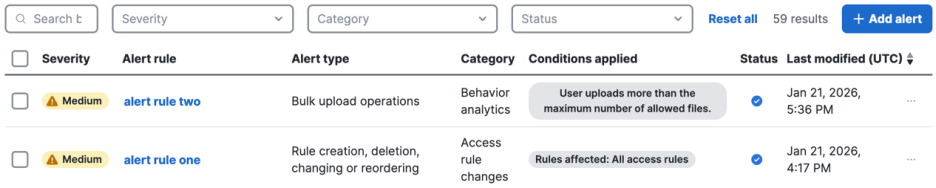
In Secure Access, you can add or duplicate alert rules that have the same alert type. However, for Behavior analytics alert rules, Secure Access generates only 25 alerts in an hour for the first alert rule created for each alert type. For example, if you add an alert rule with the alert type of **Bulk upload operations**, any subsequent alert rules that you add in the organization with the **Bulk upload operations** alert type do not generate duplicate or additional alerts.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Alert Rules**.



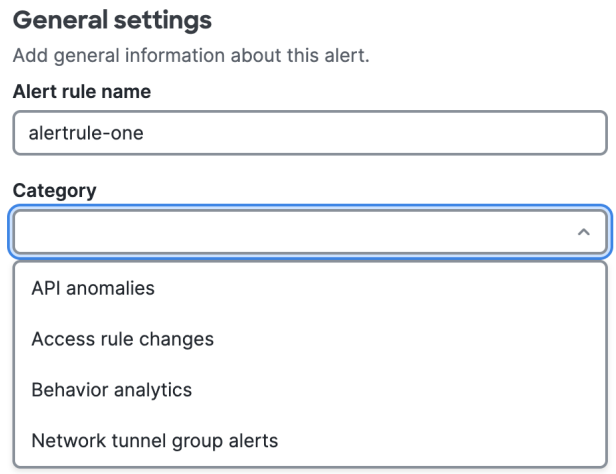
2. On **Alert Rules**, click **+ Add alert** or edit an existing alert rule.

> **Note**
>
> On **General Settings**, you must configure the alert rule name, category, and alert type.

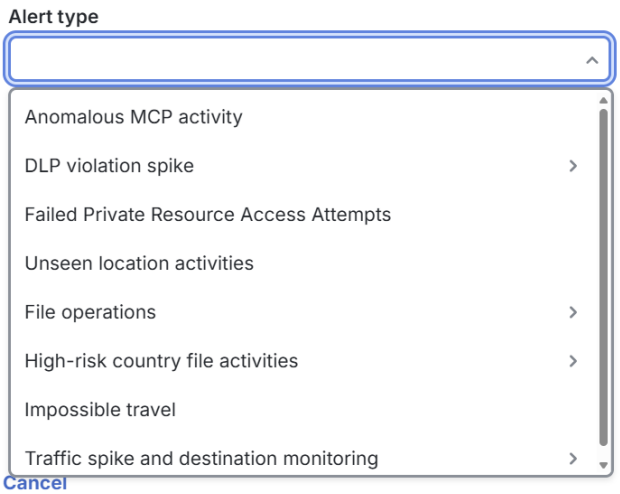
   - Alert rule name–The name of the alert.
   - Category–The category of the alert.
   - Alert type–The type of the alert in the alert category.
   - Severity level–The level of severity associated with the alert.
   - Description–A meaningful description of the alert.

3. For the **Alert rule name**, enter a sequence of 3-254 alphanumeric, parentheses, and hyphen characters.

   Choose a meaningful name that begins with an alphanumeric character.



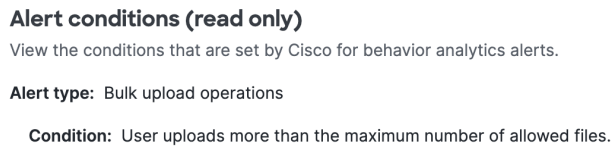
4. For **Category**, choose **Behavior analytics**.
5. For **Alert type**, choose one of the end-user behaviors monitored by Secure Access.
   - **Anomalous MCP activity**–Alert on unusual Model Context Protocol (MCP) activity.
   - **DLP violation spike** – Alert on exceeding the threshold for specific DLP violations based on predefined rules or classifications.
   - **Failed Private Resource Access Attempts** – Alert when an end user makes an unusually high number of failed attempts to access private resources through client-based ZTNA.
   - **Unseen location activities** – Alert on user activity from a city or source IP address that was not observed for that user during the previous 60 days.
   - **File operations**–Alert on unusual bulk file uploads, downloads, and deletions.
   - **High-risk country file activities**–Alert on file uploads to, or downloads from, countries that you designate as high-risk.
   - **Impossible travel** –Alert on end-user activity that occurs in geographic locations that are distant from one another and within unrealistic timeframes.
   - **Traffic spike and destination monitoring** – Alert on unusual increase in requests to a specific destination or to any TOR relay.



6. For **Severity level**, choose one of the severity levels for the alert.

- **High**
- **Medium**
- **Low**
- **Info**

7. For **Description**, enter a sequence of 1-150 characters that describe the alert rule.
8. Click **Next**.
9. On **Alert conditions**, Secure Acess describes the selected alert type and the conditions that cause the type of alert.



10. Click **Next**.
11. On **Notifications**, enable the notifications for the alert rule. You can enable **Webhook notifications** and **Email notifications**.

    Secure Access always enables in-product notifications. For more information about in-product notifications, see Monitor Alerts from Secure Access.

    a) Choose **Web notifications** to configure push notifications to a third-party product or service.

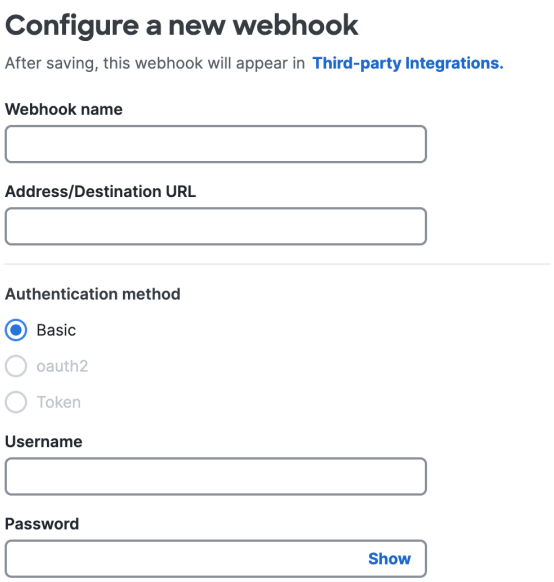
    You can choose from a list of configured webhooks or add a new webhook.

    b) Click on the **Select a webhook** drop-down menu and then choose a webhook from the list of configured webhooks.

    c) Click **+ Configure a new webhook**. After you complete the configuration of the new webhook, click **Save**.

    Complete the configuration of the webhook and add the webhook in the organization. You can add at most 10 webhooks.

    For information about webhooks, see Manage Webhooks for Third-Party Integrations.

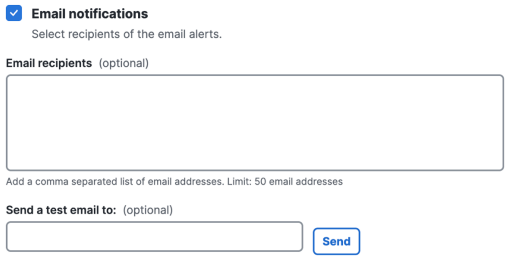


    d) Click **Email notifications** to configure notifications to a list of email recipients.

You can configure and send a test notification to the list of email recipients.

e) Add a comma-separated list of email addresses.

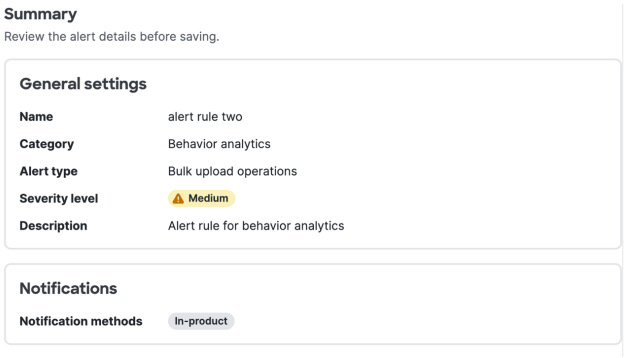
> **Note**
>
> You are limited to 50 email addresses.



f) (Optional) Enter an email address, and then click **Send**.

Secure Access sends a test alert to evaluate that the email address receives the alert.

12. Click **Next**.
13. On **Summary**, review the details in the **General Settings** and **Notifications**.



14. Click **Save**.

Add and Edit Alert Rules for Tunnel Connectivity

Provides instructions for completing the Add and Edit Alert Rules for Tunnel Connectivity workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access checks the status of network tunnel groups at regular intervals. When a network tunnel group is disconnected or a hub is down and these meet alert conditions, Secure Access will delay the alert for eight minutes. If alert conditions are still met after eight minutes, then Secure Access raises the alert. This delay avoids unnecessary alerts caused by short-lived issues and tunnel flapping.

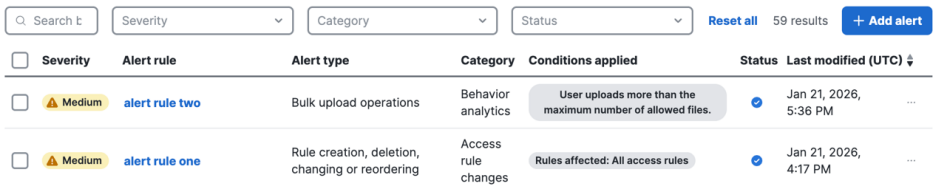
> **Note**
>
> When you edit an alert rule, Secure Access dismisses any active alerts for that rule.

Before you begin

- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Alert Rules**.

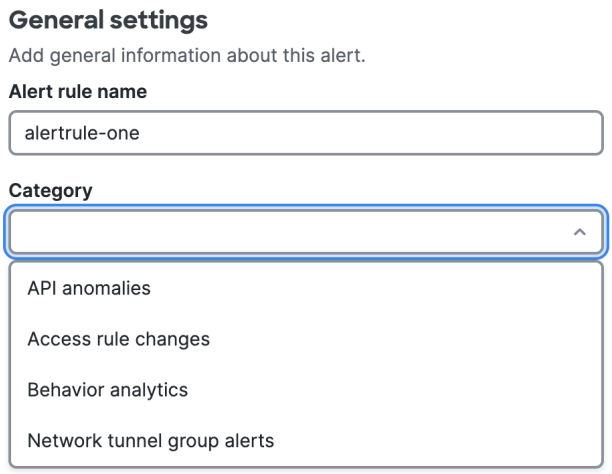


2. On **Alert Rules**, click **+ Add alert** or edit an existing alert rule.

> **Note**
>
> On **General Settings**, you must configure the alert rule name, category, and alert type.

   - Alert rule name–The name of the alert.
   - Category–The category of the alert.
   - Alert type–The type of the alert in the alert category.
   - Severity level–The level of severity associated with the alert.
   - Description–A meaningful description of the alert.

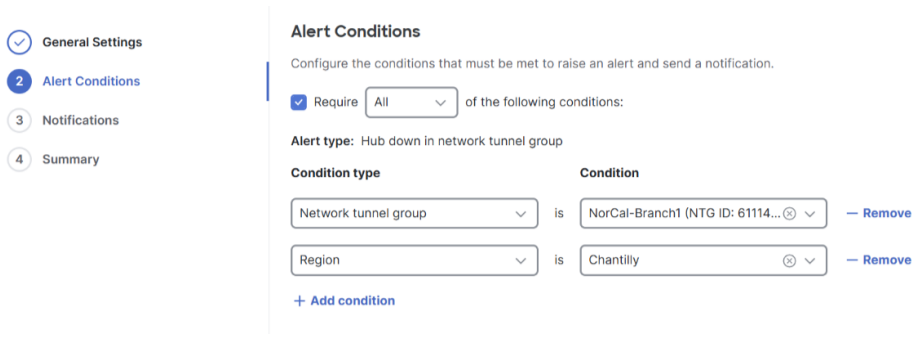
3. For the **Alert rule name**, enter a sequence of 3-254 alphanumeric, parentheses, and hyphen characters. Choose a meaningful name that begins with an alphanumeric character.



4. For **Category**, choose **Network tunnel group alerts**.
5. For **Alert type**, choose from the list of alerts conditions.
   - **Network tunnel group disconnected**–Both primary and secondary hubs are down and have no active network tunnels. This will result in a loss of connectivity for the network tunnel group.
   - **Hub down in network tunnel group**–One of the hubs of the network tunnel group is down and has no active tunnels. This will result in reduced failover and redundancy capabilities, and increased load on the remaining hub.

   Each **Alert type** displays the **Alert impact**–the impact of the event that triggers the alert.
6. For **Severity level**, choose the severity of the alert.

   Each **Alert type** has a recommended **Severity**:
   - **Network tunnel group disconnected**–High severity is recommended.
   - **Hub down in network tunnel group**–Warning severity is recommended.
7. For **Alert Conditions**, configure the conditions that must be met to raise an alert and send a notification.
   a) Click **Require** to select all or any of the conditions.
   b) Chose a **Condition type** and **Condition**.
      - **Condition type** and **Condition**–Specify a combination of network tunnel group name or region conditions that will trigger this alert.



8. Click **Next**.
9. On **Notifications**, enable the notifications for the alert rule. You can enable **Webhook notifications** and **Email notifications**.

Secure Access always enables in-product notifications. For more information about in-product notifications, see Monitor Alerts from Secure Access.

a) Choose **Web notifications** to configure push notifications to a third-party product or service.

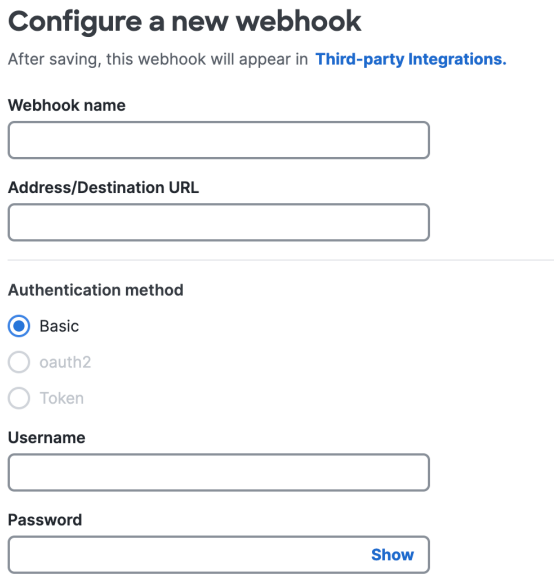
You can choose from a list of configured webhooks or add a new webhook.

b) Click on the **Select a webhook** drop-down menu and then choose a webhook from the list of configured webhooks.

c) Click **+ Configure a new webhook**. After you complete the configuration of the new webhook, click **Save**.

Complete the configuration of the webhook and add the webhook in the organization. You can add at most 10 webhooks.

For information about webhooks, see Manage Webhooks for Third-Party Integrations.

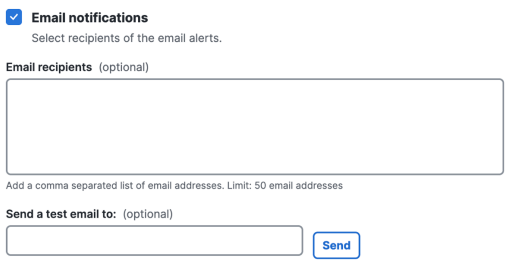


d) Click **Email notifications** to configure notifications to a list of email recipients.

You can configure and send a test notification to the list of email recipients.

e) Add a comma-separated list of email addresses.

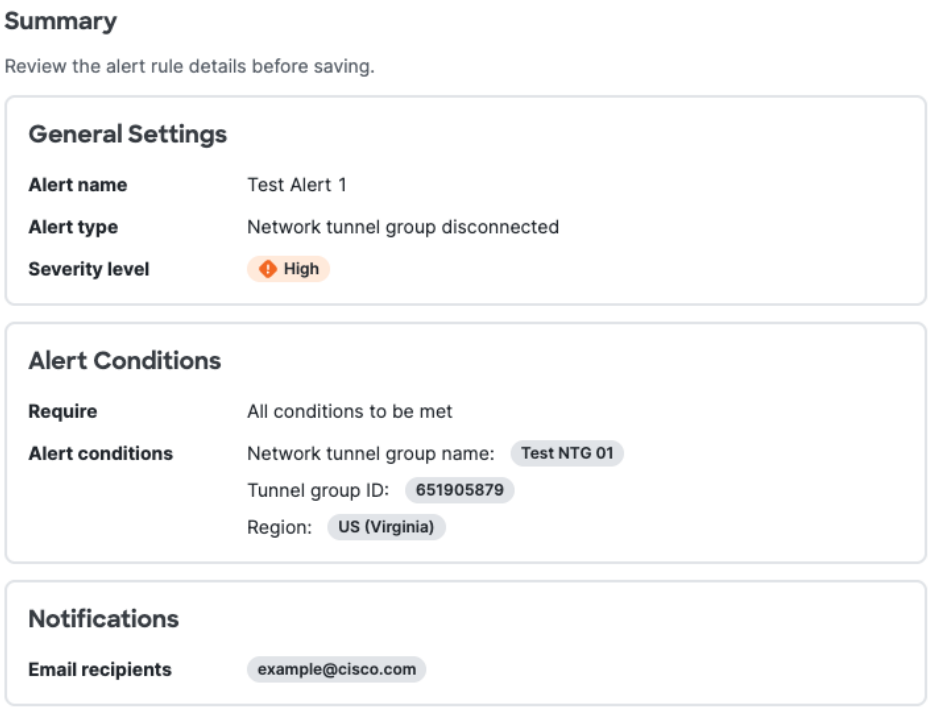
> **Note**
>
> You are limited to 50 email addresses.



f) (Optional) Enter an email address, and then click **Send**.

Secure Access sends a test alert to evaluate that the email address receives the alert.

10. Click **Next**.
11. On **Summary**, review the alert rule details, then click **Save**.



What to do next

Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** to investigate the network tunnel group identified by the alert. For more information, see Manage Network Tunnel Groups.

Add and Edit User Access Alerts

Provides instructions for completing the Add and Edit User Access Alerts workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Configure alerts in Secure Access to monitor the number of end users that are blocked from reaching internet or private destinations. Updates by administrators to the access rules in the Access policy or posture profiles, or changes to endpoint settings can cause end users to lose access to certain destinations.

Secure Access triggers a user-access alert when a maximum number (threshold) of end users are blocked from reaching destinations. To count toward the threshold, an end user must have accessed the destinations during the last 24 hours before the block occurred. Once the number of end users that are blocked from reaching the destinations exceeds the configured threshold, Secure Access raises the alert.

Secure Access resets the threshold for the end users that are blocked from accessing a destination when:

- An administrator dismisses the alert that was caused by endpoint settings that do not comply with the Endpoint posture profiles.
- An administrator modifies the Access policy or posture profiles and triggers a new instance of the alert.

In Secure Access, you can monitor these user-access conditions:

- **Users blocked due to policy update**

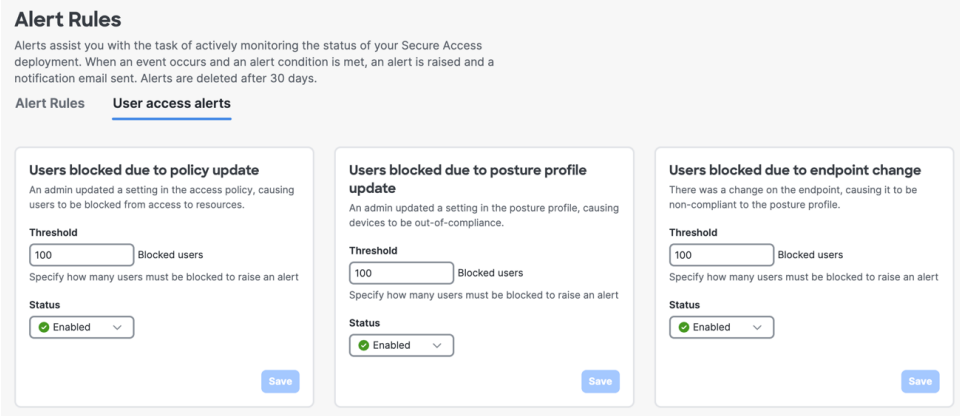
- **Users blocked due to posture profile update**
- **Users blocked due to endpoint change**

Before you begin

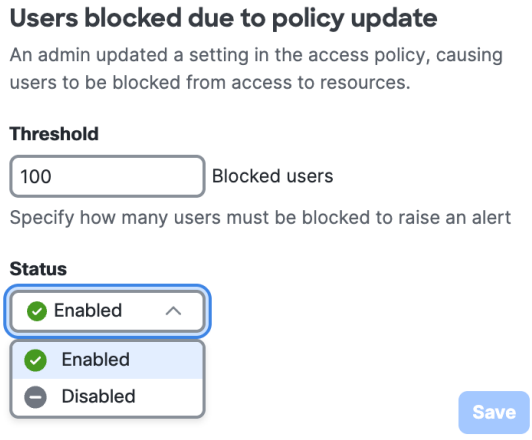
- Full Admin role in Secure Access. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Alert Rules**.



2. Click the **User access alerts** tab.
3. Navigate to **Users blocked due to policy update**.



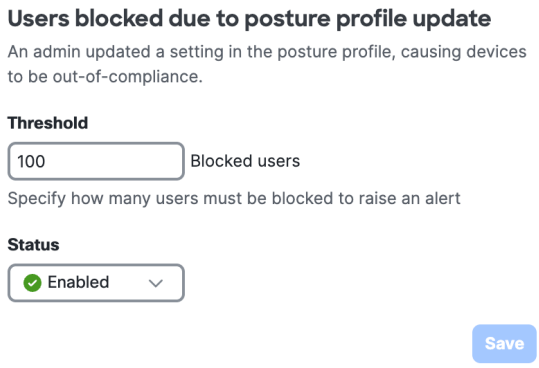
   a) For **Threshold**, set the maximum number of end users that are blocked from reaching a destination when an administrator changes the access rules in the Access policy.

      Secure Access monitors the number of end users blocked from reaching destinations. If an end user accessed a destination in the 24 hour period before the block occurred, the end user is included in the count of the threshold for the alert.

      Once the number of end users that are blocked reaches the threshold for the alert, Secure Access raises the alert.

   b) For **Status**, choose **Enabled** to activate the alert or choose **Disabled** to deactivate the alert.
   c) Click **Save**.

4. Navigate to **Users blocked due to posture profile update**.



a) For **Threshold**, set the maximum number of end users that are blocked from reaching a destination when an administrator changes the posture profiles in the organization.

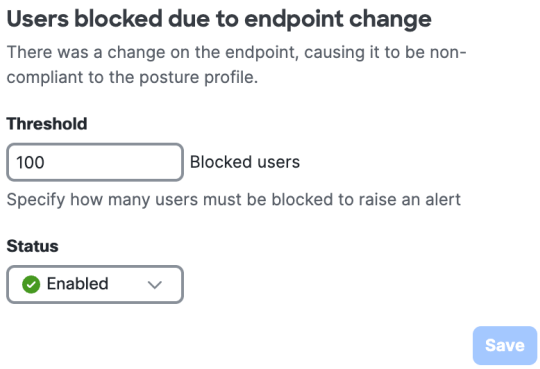
   Secure Access monitors the number of end users blocked from reaching destinations. If an end user accessed a destination in the 24 hour period before the block occurred, the end user is included in the count of the threshold for the alert.

   Once the number of end users that are blocked reaches the threshold for the alert, Secure Access raises the alert.

b) For **Status**, choose **Enabled** to activate the alert or choose **Disabled** to deactivate the alert.

c) Click **Save**.

5. Navigate to **Users blocked due to endpoint change**.



a) For **Threshold**, set the maximum number of end users that are blocked from reaching a destination when their endpoint settings conflict with the organization's Endpoint posture profiles.

   Secure Access monitors the number of end users blocked from reaching destinations. If an end user accessed a destination in the 24 hour period before the block occurred, the end user is included in the count of the threshold for the alert.

   Once the number of end users that are blocked reaches the threshold for the alert, Secure Access raises the alert.

b) For **Status**, choose **Enabled** to activate the alert or choose **Disabled** to deactivate the alert.

c) Click **Save**.

Add and Edit Alert Rules for Resource Connectors

Configure and manage proactive alert rules to monitor connectivity, certificate lifecycle, and software support status for Cisco Secure Access resource connectors and connector groups.

Secure Access checks the status of resource connectors and resource connector groups at regular intervals. When a resource connector is disconnected or an issue meets alert conditions, Secure Access delays raising the alert for 10

minutes. If alert conditions are still met after 10 minutes, Secure Access raises the alert. This delay avoids unnecessary alerts caused by transient network disruptions and connector flapping.

> **Note**
>
> When you edit an alert rule, Secure Access dismisses any active alerts for that rule.

After you add an alert rule, Secure Access begins to monitor the conditions defined for the alert. You can view the alerts generated by Secure Access for the Behavior analytics alert rules in the organization.

In Secure Access, navigate to the toolbar at the top of your browser window.



Click the bell icon to open the Alerts drop-down menu. Secure Access displays the alerts generated for the configured alert rules. For information about viewing alerts in Secure Access, see Monitor Alerts From Secure Access.

Before you begin

Before creating or editing alert rules for Resource Connectors, ensure you meet the following requirements:

- You must have Full Administrator role in Cisco Secure Access. For more information, see Manage Accounts.
- At least one resource connector group and active resource connector must be deployed in your organization.
- Valid email addresses or distribution lists must be identified for alert notifications.

Procedure

1. In the Cisco Secure Access navigation menu, navigate to **Monitor** > **Alert Rules**.
2. Choose one of the following actions to open the alert rule wizard:
   - To create a new alert rule, click **Add Rule**.
   - To update an existing alert rule, locate the rule in the table, click **More Options** (**...**), and select **Edit**.
3. In the **General Settings** tab, specify the rule identity and severity:
   a) In the **Alert rule name** field, enter a unique, descriptive name for the alert rule.
   b) From the **Category** drop-down list, select **Resource Connector**.
4. From the **Alert type** drop-down list, select the condition you want to monitor.

Table 34: Resource Connector Alert Types

Alert Type	Trigger Condition
Resource connector software updates	
Resource connector update started	Alert on an over-the-air (OTA) software update beginning on a resource connector during its scheduled maintenance window.
Resource connector update succeeded	Alert on a software update completing successfully and the resource connector restarting with the updated software image.
Resource connector update failed	Alert on a resource connector software update failure, requiring verification of outbound firewall access to Cisco update repositories.
Resource connector certificate & security	

Alert Type	Trigger Condition
Resource connector certificate renewal failed	Alert on the failure of automatic TLS client certificate renewal between the resource connector and Cisco cloud services.
Resource connector certificate expiring soon	Alert on a resource connector TLS client certificate approaching expiration within 10 days.
Resource connector certificate expired	Alert on a resource connector TLS client certificate expiring, resulting in tunnel authentication termination.
Resource connector software vulnerability detected	Alert on a security vulnerability detected in the running resource connector software package.
Resource connector host OS vulnerability detected	Alert on a security vulnerability detected in the underlying host operating system of the resource connector.
Resource connector connectivity & sync	
Resource connector tunnel disconnected	Alert on a resource connector tunnel remaining disconnected for 10 or more consecutive minutes.
Resource connector tunnel reconnected	Alert on a previously disconnected resource connector tunnel successfully restoring connection to Cisco Secure Access.
Resource connector configuration out of sync	Alert on the local configuration metadata on a resource connector failing to match cloud tenant records.
Resource connector end-of-support	
Resource connector software image end of support	Alert on a running resource connector software image reaching End-of-Support (EoS).
Resource connector host OS end of support	Alert on the underlying host operating system of a resource connector reaching End-of-Support (EoS).
Resource connector group connectivity	
Resource connector group disconnected	Alert on all resource connectors within a connector group disconnecting simultaneously, interrupting ZTNA access to associated private resources.
Resource connector group partially reconnected	Alert on at least one resource connector reconnecting in a previously offline group, indicating degraded operational capacity.
Resource connector group performance	
Resource connector group overloaded	Alert on active connection load or bandwidth throughput exceeding capacity thresholds for a resource connector group.

5. Configure rule severity and description:
   a) From the **Severity level** drop-down list, select the severity level: **High**, **Medium**, **Low**, or **Info**.
   b) (Optional) In the **Description** field, enter or edit the remediation description (maximum 150 characters).
   c) Click **Next**.
6. In the **Alert Conditions** tab, specify the trigger scope for the alert rule:
   a) Choose one of the following trigger options:
      - **Trigger notifications for all regions and connector groups:** To trigger alerts for every region and connector group.
      - **Trigger only for selected regions and connector groups:** To limit the alert rule to targeted regions and/or connector groups.

- Select the **Regions affected** check box, and then from the **Select regions** drop-down list, choose one or more cloud regions.
- Select the **Connector groups affected** check box, and then from the **Select connector groups** drop-down list, choose one or more resource connector groups.

b) Click **Next**.

7. In the **Notifications** tab, enable the notifications for the alert rule. You can enable **Webhook notifications** and **Email notifications**

   Secure Access always enables in-product notifications. For more information about in-product notifications, see Monitor Alerts from Secure Access.

   a) Choose **Web notifications** to configure push notifications to a third-party product or service.

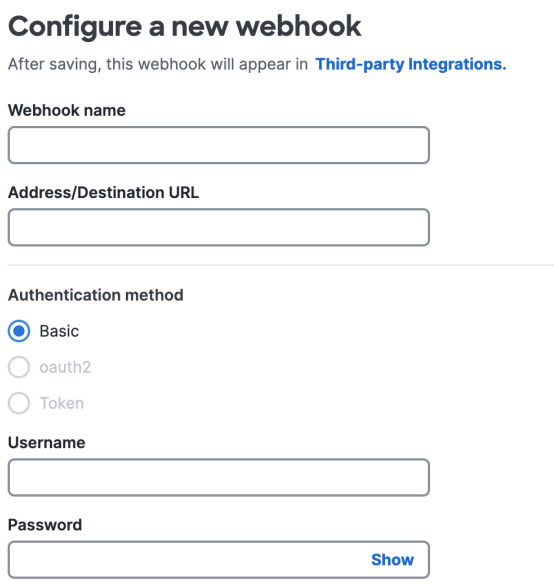
      You can choose from a list of configured webhooks or add a new webhook.

   b) Click on the **Select a webhook** drop-down menu and then choose a webhook from the list of configured webhooks.

   c) Click **+ Configure a new webhook**. After you complete the configuration of the new webhook, click **Save**.

      Complete the configuration of the webhook and add the webhook in the organization. You can add at most 10 webhooks.

      For information about webhooks, see Manage Webhooks for Third-Party Integrations.

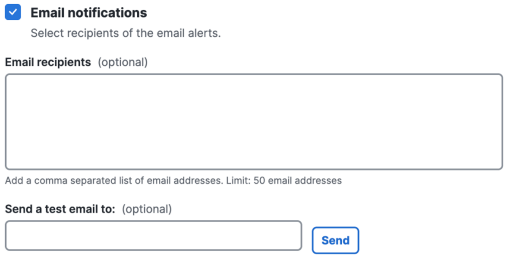


   d) Click **Email notifications** to configure notifications to a list of email recipients.

      You can configure and send a test notification to the list of email recipients.

   e) Add a comma-separated list of email addresses.

> **Note**
>
> You are limited to 50 email addresses.



f) (Optional) Enter an email address, and then click **Send**.

Secure Access sends a test alert to evaluate that the email address receives the alert.

8. In the **Summary** tab, review the configured general settings, alert conditions, and notifications, then click **Save**.

The alert rule is saved and listed in the **Alert Rules** table. Cisco Secure Access continuously evaluates connector status against the configured conditions and delivers notifications when matching events occur.

What to do next

After configuring alert rules, you can:

- Filter active and dismissed alerts in the notification drawer. For more information, see Monitor Alerts From Secure Access.
- Click **Dismiss** on an alert card to clear acknowledged notifications. For more information, see Monitor Alerts From Secure Access.
- Toggle the rule status to **Disable** in the Alert Rules table to suspend notifications without deleting the rule configuration. For more information, see Manage Alert Rules.

Manage Alert Rules for Destination Lists

This topic describes how to create, edit, and manage alert rules to monitor destination list sizes and prevent indicator write failures.

Secure Access monitors the number of destinations across destination lists for your organization. When the number approaches a configured limit, Secure Access alerts you. This helps you address over-utilization of Destination Lists which can lead to write failures, and impact enforcement for threat intelligence feeds and other integrations, if the list size limit is reached.

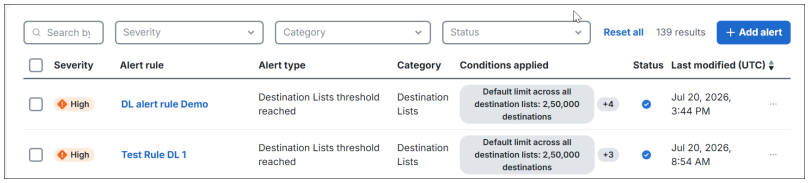
> **Note**
>
> When you edit an alert rule, Secure Access dismisses any active alerts for that rule.

Before you begin

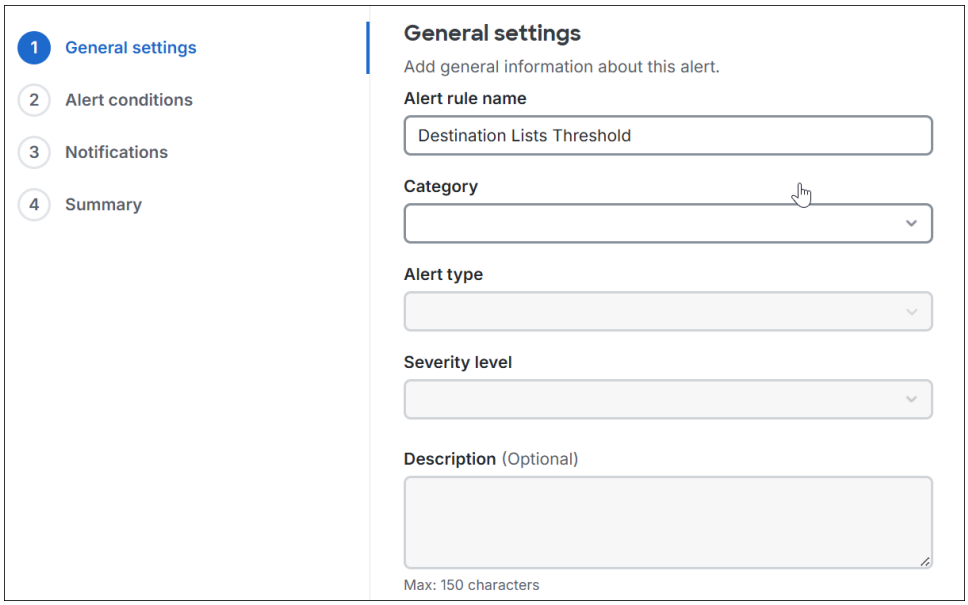
- Full administration role in Secure Access. See Manage Accounts.

Procedure

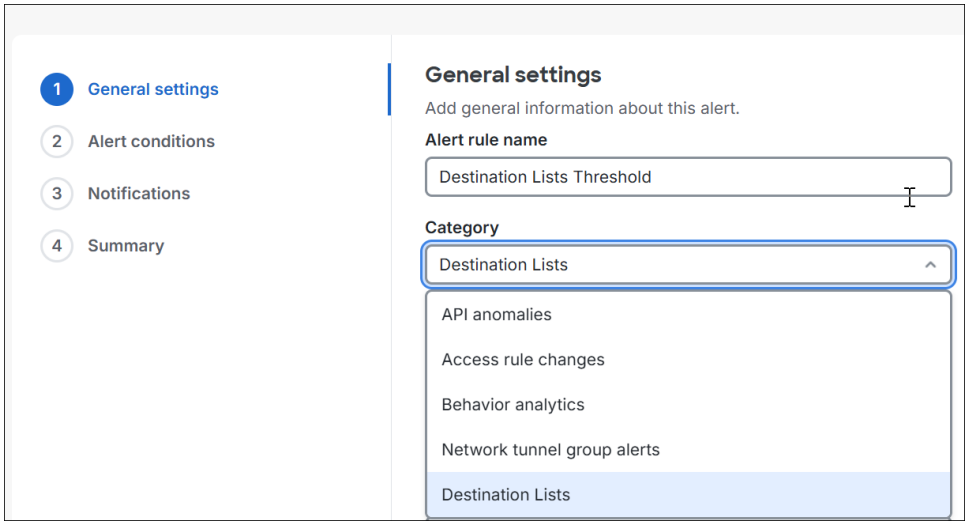
1. Navigate to **Monitor** > **Alert Rules**.
2. The **Alert Rules** page, click **Add alert** or select an existing alert rule to edit.



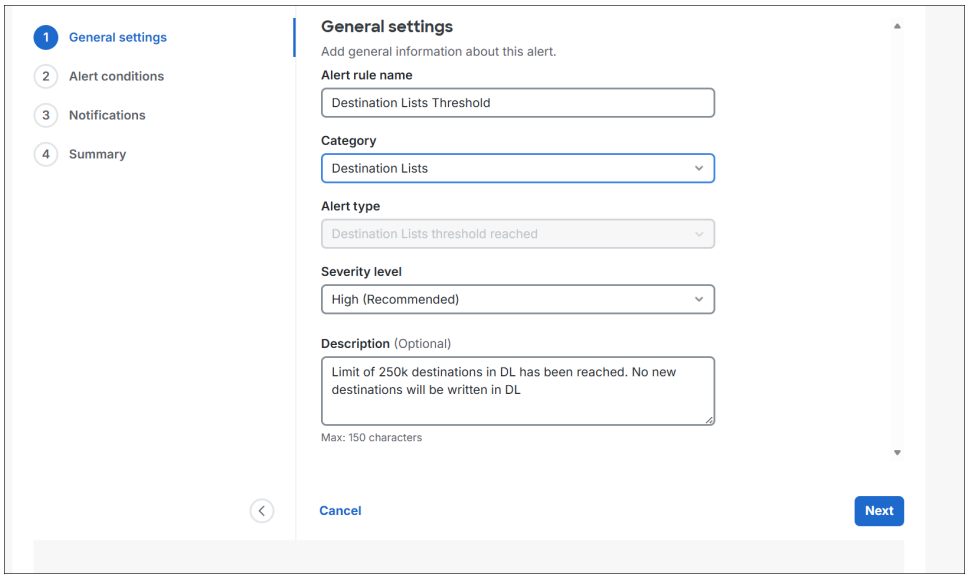
3. In the **Alert rule name** field, enter a name that begins with an alphanumeric character and contains 3 to 254 alphanumeric characters, parentheses, or hyphens.



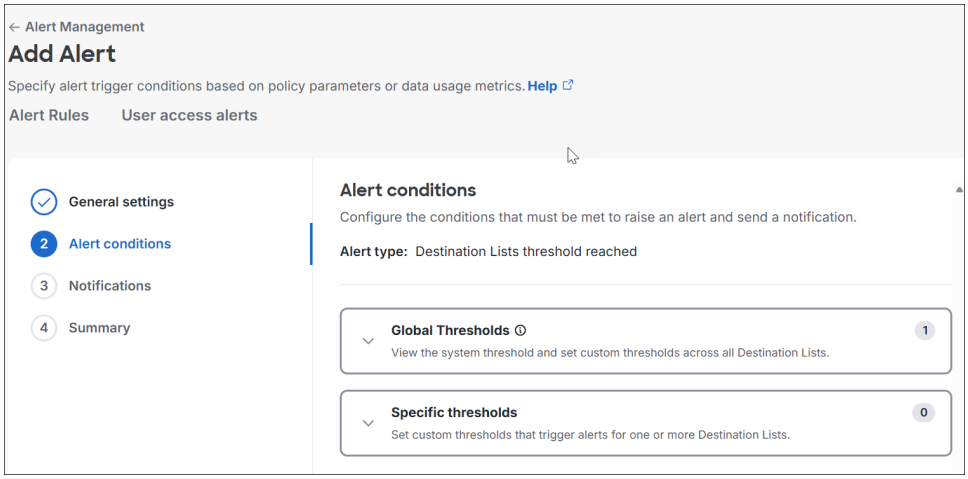
4. From the **Category** drop down list, select **Destination lists**.



5. Review the automatically populated **Alert type** (Destination Lists threshold reached) and **Severity level** (High) fields.
6. (Optional) Enter a **Description** for the alert rule.

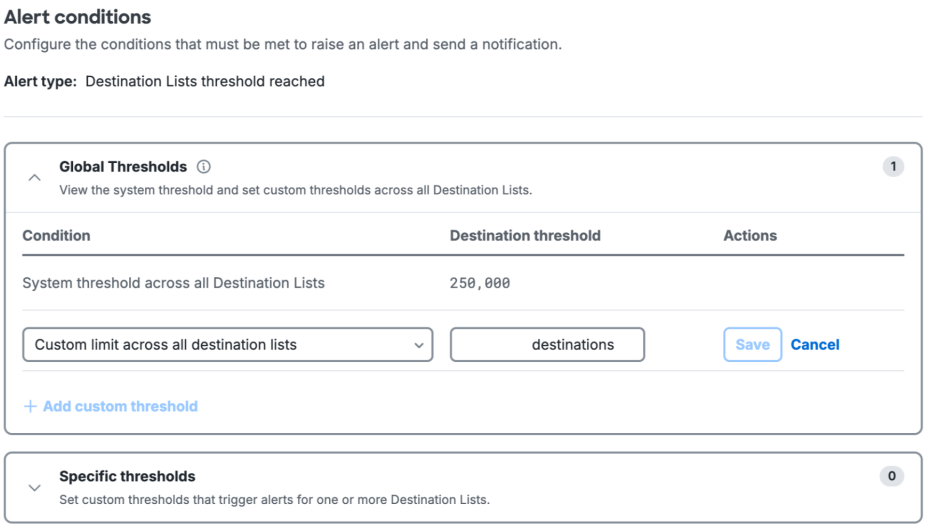


7. Click **Next**.
8. On the **Alert Conditions** page, configure the conditions that trigger an alert:

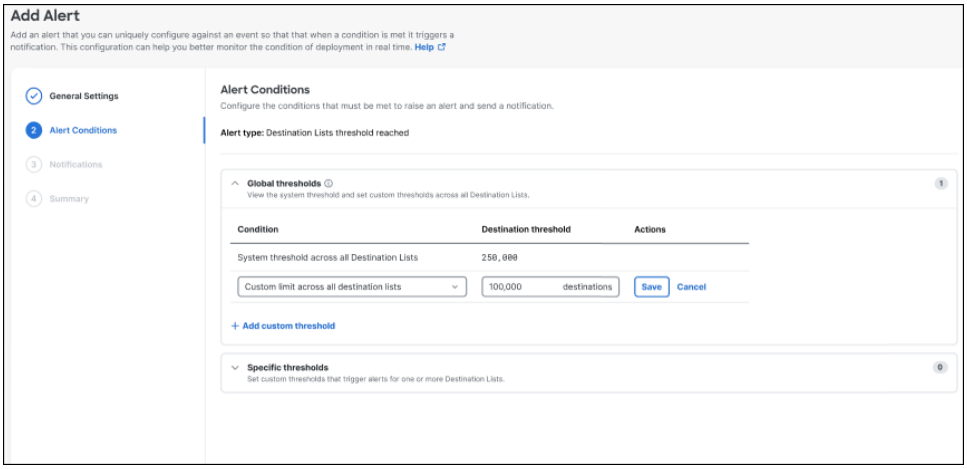


a) **Global thresholds:** Click the section to expand it. You can click **Add custom threshold** to set additional limits.

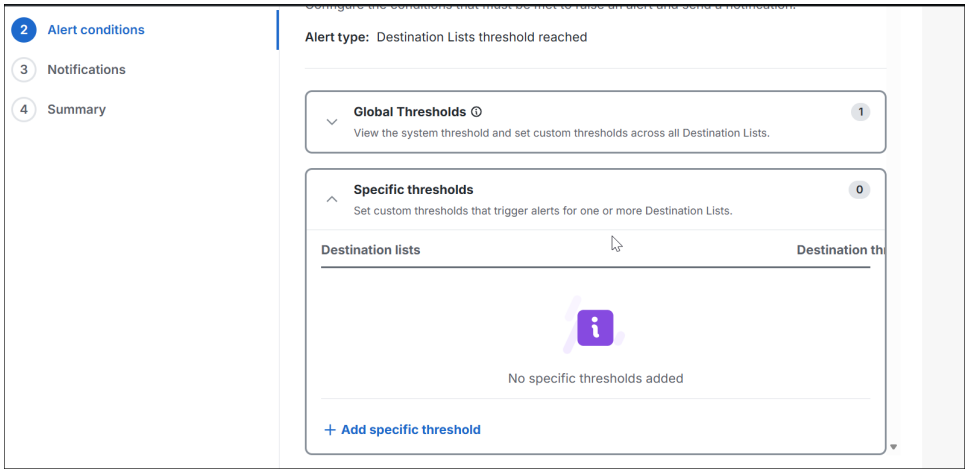
> **Note**
>
> Cisco Secure Access has an overall limit of 250,000 destinations across all Destination Lists to ensure optimal performance. As such, by default, when configuring an alert for Destination Lists, Secure Access automatically applies a global alert threshold of 250,000 destinations. You can click Add custom threshold to set additional limits.



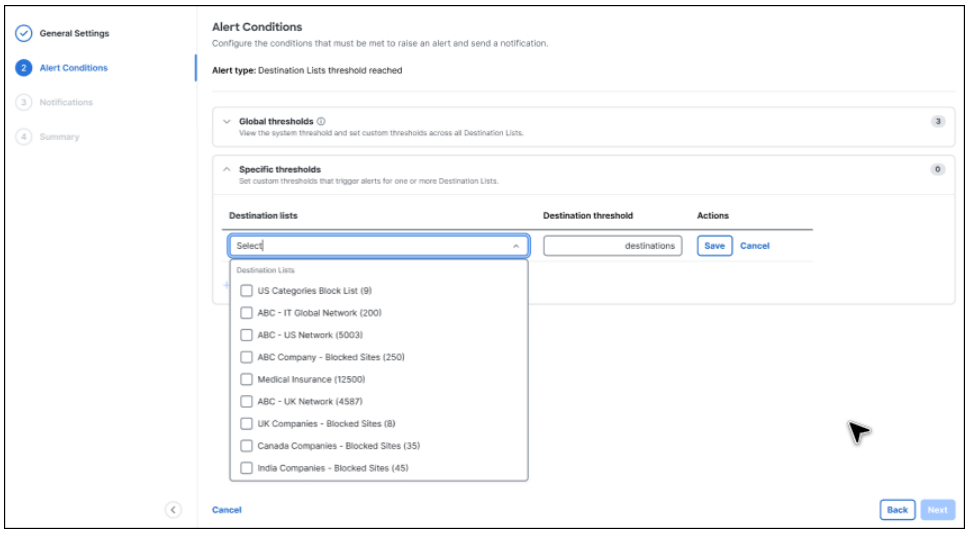
- From the **Condition** drop down list, select **Custom limit across all destination lists**.
- To set a limit across all destination lists, enter a value less than 250,000.
- Click **Save**.



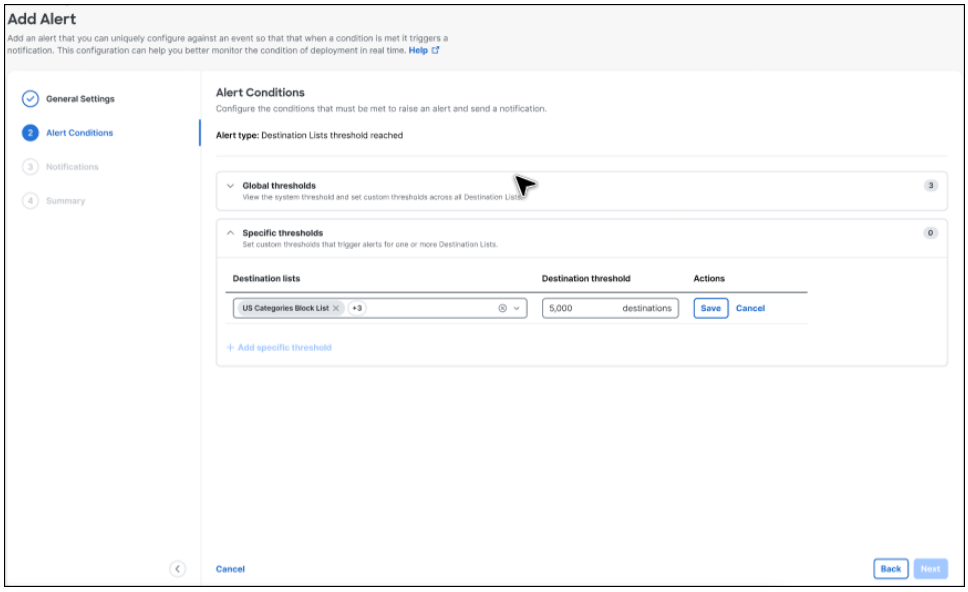
b) **Specific thresholds:** Click the section to expand it. Click **Add specific threshold**.



- From the **Destination lists** drop down list, select one or more destination lists.
- Enter the threshold value that trigger the alert in the Destination threshold field.
- Click **Save**.

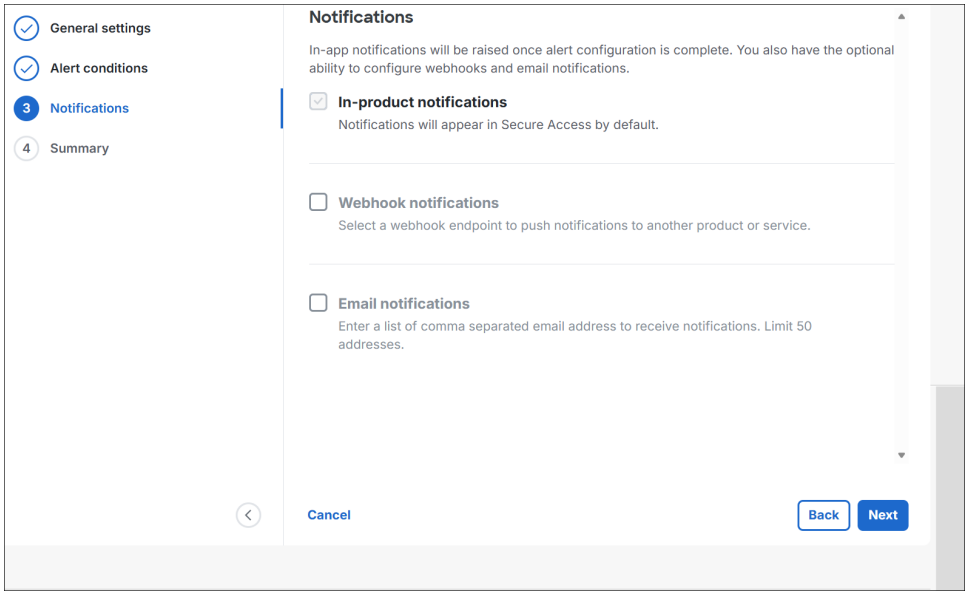


> **Note**
>
> You can create up to 10 conditions in one alert rule. Global thresholds and specific thresholds share this condition limit. To add a new condition after reaching the limit, first remove an existing condition. Secure Access validates each threshold before you save it.

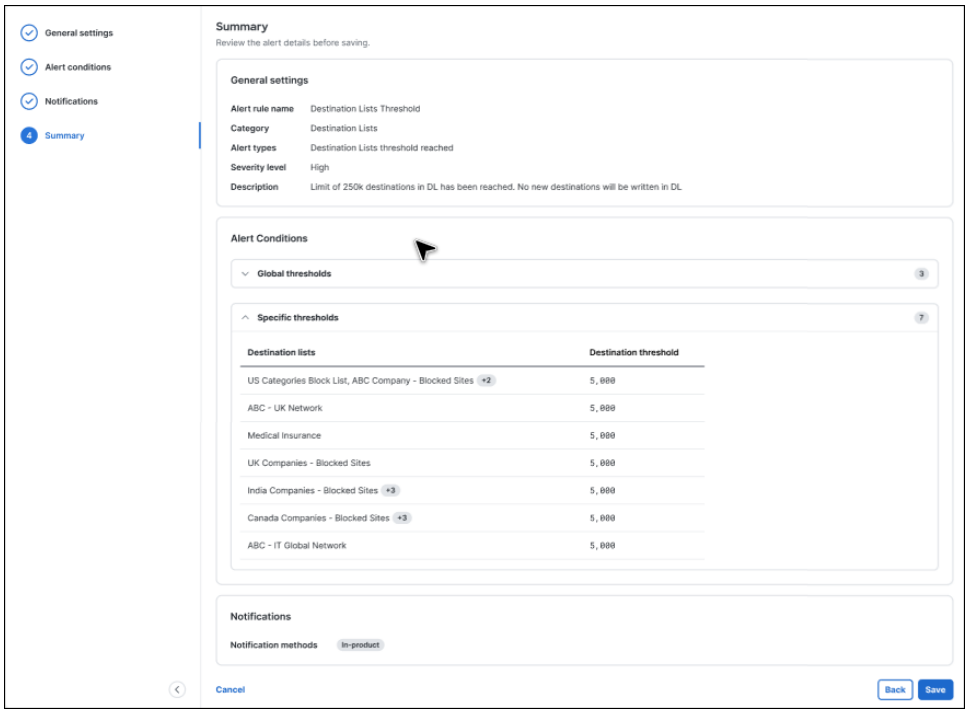


9. On **Notifications**, select the delivery methods for receiving notification alerts. Secure Access always enables inproduct notifications.

> **Note**
>
> For more information, see Monitor Alerts from Secure Access. You can also configure **Webhook notifications** and **Email notifications**.



10. Click **Next**.
11. On the **Summary** page, review the alert rule details and click **Save**.



What to do next

When Secure Access raises an alert, review your destination lists and remove any destinations. This will allows you to add new indicators.

Monitor Alerts from Secure Access

Provides instructions for completing the Monitor Alerts from Secure Access workflow in Cisco Secure Access. Monitor and manage alerts directly from Secure Access.

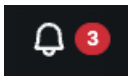
Monitor and manage alerts directly from Secure Access.

Procedure

1. In Secure Access, navigate to the toolbar at the top of your browser window.

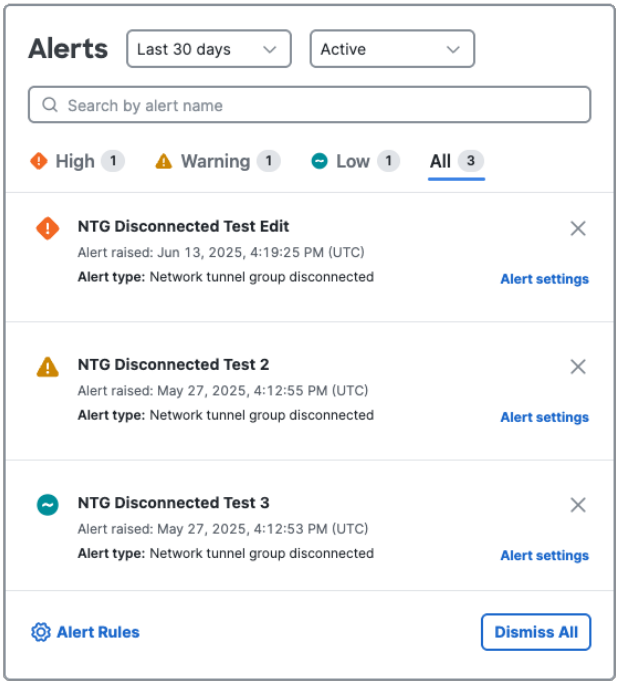


2. Click the bell icon to open the Alerts dropdown. The bell indicates the number of active alerts.



3. Click the **Alerts** drop-down menu.

   Secure Access lists the alerts in chronological order with the most recent alert shown first.



   The **Alerts** dropdown includes these controls:

   - Filter by alerts raised in the last 30 days, last 7 days, or last 24 hours.
   - Filter by Active or Dismissed.
   - Search by alert name.
   - View lists of alerts by **Severity**: High, Warning, Low, or All.
   - Click the X at the top right of an alert to dismiss it.

- Click **Dismiss All** to dismiss all active alerts.
- Click **Alert settings** to edit the alert rule.

4. Click **Alert Rules** to navigate to the Alert Rules page.

   For more information, see Manage Alert Rules.

Splunk Integration: Configure Alert Rules for Access Policy Changes

Describes Splunk Integration: Configure Alert Rules for Access Policy Changes in Cisco Secure Access. You can set up your instance of the Splunk to receive alerts from Secure Access.

You can set up your instance of the Splunk to receive alerts from Secure Access. Configure an Alert Rule that publishes events when Secure Access detects changes to the rules in your organization's Access policy. Before you add the Alert Rule for Splunk, configure a Secure Access Webhook.

Set up a Secure Access Webhook with the URL for the Splunk listener and select the Webhook when you configure the Alert Rule. For more information, see Manage Webhooks for Third-Party Integrations.

Set Up an Alert Rule in Secure Access for Splunk

1. Add a Webhook in Secure Access. Configure the Webhook with the URL for the Splunk HTTP listener and the Basic authentication credentials for your Splunk account. For more information, see Add a Webhook for a Third-Party Integrations.
2. Add an Alert Rule in Secure Access and select the Webhook that you configured for Splunk. Set up the Alert Rule to emit notifications when Secure Access detects the creation or deletion of rules in the Access policy, changes to the settings in the rules, or the reordering of the rules. For more information, see Add and Edit Alert Rules for Changes on Access Rules.
3. Validate that your instance of Splunk receives the configured alerts from Secure Access.

ServiceNow Integration: Configure Alert Rules for Access Policy Changes

Describes ServiceNow Integration: Configure Alert Rules for Access Policy Changes in Cisco Secure Access. You can set up your instance of the ServiceNow app to receive alerts from Secure Access.

You can set up your instance of the ServiceNow app to receive alerts from Secure Access. Configure an Alert Rule that publishes events when Secure Access detects changes to the rules in your organization's Access policy. Before you add the Alert Rule for the ServiceNow app, configure a Secure Access Webhook.

Set up a Secure Access Webhook with the URL for the ServiceNow HTTP listener and select the Webhook when you configure the Alert Rule. For more information, see Manage Webhooks for Third-Party Integrations.

Step 1: Set Up ServiceNow to Receive Secure Access Alerts

Before you begin, obtain a ServiceNow account with administrative privileges.

1. In your instance of the ServiceNow app, create a Group for your Cisco Secure Access organization.
2. Configure authentication for the ServiceNow HTTP listener. Allow end users to manage the Basic authentication credentials for the Cisco Secure Access Group.
3. Submit the configuration of the Group for Cisco Secure Access.
4. ServiceNow exposes a single Scripted REST API endpoint URL for all groups.

Step 2: Set Up an Alert Rule in Secure Access for ServiceNow

1. Add a Webhook in Secure Access. Configure the Webhook with the URL for the ServiceNow HTTP listener and the Basic authentication credentials for your ServiceNow account. For more information, see Add a Webhook for a Third-Party Integrations.
2. Add an Alert Rule in Secure Access and select the Webhook that you configured for ServiceNow. Set up the Alert Rule to emit notifications when Secure Access detects the creation or deletion of rules in the Access policy, changes to the settings in the rules, or the reordering of the rules. For more information, see Add and Edit Alert Rules for Changes on Access Rules.
3. Validate that your instance of the ServiceNow app receives the configured alerts from Secure Access.

70 Monitor with Reports

Topics:

- Monitor Secure Access with Reports
- Report Scheduling
- Report Search Window and Retention
- Assess and Monitor Configurations in Secure Access

Provides an overview of Monitor with Reports in Cisco Secure Access, including Monitor Secure Access with Reports, Report Scheduling, and Report Search Window and Retention. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Monitor Secure Access with Reports

Describes Monitor Secure Access with Reports. Use Cisco Secure Access reports to monitor your Secure Access deployment and to better understand your Secure Access usage.

Use Cisco Secure Access reports to monitor your Secure Access deployment and to better understand your Secure Access usage. Gain insights into request and block activity, determining which of your sources are generating blocked requests. Reports help build actionable intelligence in addressing threats including changes in usage trends over time.

Available Reports

Describes Available Reports in Cisco Secure Access. Remote Access Logs–Lists users that have remotely connected to Secure Access and requested access to destinations.

- Remote Access Logs–Lists users that have remotely connected to Secure Access and requested access to destinations.
- Activity Search–Search for activity from the sources in your environment over a selected time period.
- Connectivity Logs–View the events for each tunnel within your Network Tunnel Groups. Address risks as they arise by troubleshooting connectivity issues and confirm traffic is securely transmitted between devices and Secure Access.
- Security Activity –Lists security-related activity in your environment over a selected time period.
- Total Requests Report –Provides a visualization of traffic trends over a specified time period in your environment, based on selected categories, traffic types, and responses.
- Activity Volume Report –Provides a summary of traffic by security categories and policies influenced by content categories and Destination Lists, highlighting allowed and blocked traffic, and identifying potential risk activities within the organization.
- App Discovery–Provides information about the cloud apps in use in your environment.
- Top Destinations–Lists the top traffic-generating sources over the selected time period. Filterable by source and destination.
- Top Categories–Lists the most popular security and content categories for your organization over the selected time period.
- Third-Party Apps–Lists third-party cloud applications that have been authorized to access sanctioned tenant applications.
- Data Loss Prevention–Lists security events related to content classified as personally identifiable or sensitive information.
- Data Security Posture Management–Lists posture, recommendations, scan coverage, risky asset owners, high-risk assets, and analytics.
- Cloud Malware–Lists malicious files detected within your organization and provides details of the potential risk and exposure these files present.
- Admin Audit Log–Lists a record of any configuration changes made to your settings by any of your Secure Access administrators.

Export Report Data to CSV

Provides instructions for completing the Export Report Data to CSV workflow in Cisco Secure Access. Some reports let you export the results of a query to the CSV format.

Some reports let you export the results of a query to the CSV format. This lets you create other reports and graphs by feeding this data to other tools.

> **Note**
>
> The timezone of exported data is always the timezone selected for your account. You can change this for your account at **Admin** > **Account.**

Exportable reports:

- Network Tunnel Group Usage
- Remote Access Log
- Activity Search
- Connectivity Logs
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- Events

Troubleshooting

Depending on the time range and filters applied to the exported report, some report exports may take a very long period of time to generate and, in some cases, will time out. However, the timeout is not reflected in the dashboard. Instead, status is set to **Generating...** and persists. Typically, this happens somewhere between 12 to 24 hours after the report export is first begun. If this situation occurs, rerun the report export with a shorter date range, fewer rows, or more detailed filters.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

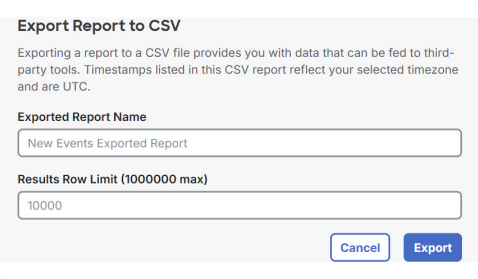
1. Navigate to **Monitor** > **Reports** > **<report>** and click **Export CSV** .

   For Remote Access Logs, the selected time range and applied filters are used for the export, including filters selected from the filter menu or added from a table value.

   Click **Download** in the case of the Third-Party Apps, Cloud Malware, and Data Loss Prevention reports.

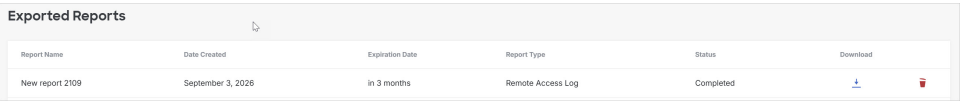
2. Give your report a good **Report Title**, add the number of rows of data to be returned, and click **Export**.



Note

When exporting to CSV, data is limited to a maximum of 100,000 rows. Due to the queue-based processing system, reports may experience significant latency. To minimize wait times, consider running reports for shorter time periods, reducing the number of rows to be exported, or applying more detailed filters. For efficient management of large datasets, check the last row of the initial report and then run the report again from that point for the next segment of data.

3. When you click **Export**, you are taken to the Exported Reports page to download your CSV file.



4. Find this page at any time by navigating to **Monitor** > **Management** > **Exported Reports**.

Bookmark and Share Reports

Provides instructions for completing the Bookmark and Share Reports workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Secure Access stores the report state in the URL, making it easy to share a report with colleagues or bookmark a report for future use.

Before you begin

A minimum user role of Read-only. For more information, refer to Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **<report>**.
2. Filter the report to display the data you need.
3. Use your browser's bookmark function. When you retrieve the bookmark the report will have the same filters applied. You can also share the URL of the page with any colleague in your organization with access to your dashboard.

   If the report has a relative date filter–last 24 hours, last 7 days, and so on–the relative date is applied. If the report has an absolute date filter (for example, Jan 7, 2019), the absolute filter is applied.

Report Scheduling

Describes Report Scheduling in Cisco Secure Access. Various reports in Secure Access can be configured so that Secure Access regularly emails you a summary of that report.

Various reports in Secure Access can be configured so that Secure Access regularly emails you a summary of that report. You can configure filters for these reports so that they only contain the information you want. Each emailed report includes an HTML version of the report, a .ZIP file containing a CSV file with the entire data set, and a link to Secure Access and the report. See Schedule a Report.

Important

It is recommended to open the CSV file format of scheduled reports received through email using **Numbers** (for Mac users) or **Excel** (for Windows users). This ensures optimal formatting and ease of data analysis.

Reports can be scheduled so that you receive an email daily, weekly, or monthly.

Note

- You can unsubscribe from a report email through the **Unsubscribe** link at the bottom of every report email.
- There is a limit of 100 scheduled reports per organization.

You can schedule the following reports:

- **Remote Access Log** –Lists users that have remotely connected to Secure Access and requested access to destinations. The report provides key session details and relevant fields to aid in debugging, troubleshooting, and monitoring remote access activity within your environment.
- **Activity Search**–Activity from the identities in your environment over a selected time period. Filterable by identity name, destination, source IP, response, content category, and security category.
- **Network Connectivity Monitoring** –Lists events for network tunnel groups and resource connectors to help you monitor connectivity, track state changes, and troubleshoot issues to ensure that traffic is securely transmitted between your environment and Secure Access.
- **Total Requests**–Total requests for destinations from your organization over the selected time period. Filterable by identity.
- **Activity Volume**–Total queries within your organization broken down by security categories and results over the selected time period.
- **Top Destinations**–A list of the top traffic-generating identities over the selected time period. Filterable by identity and destination.
- **Top Categories**–A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- **Data Loss Prevention** –Lists data violations detected through the DLP Real Time and SaaS API rules.
- **Cloud Malware Report**–Provides an overview of malicious files within your environment and details the potential risk and exposure these files present.

- **Events Report**–Provides unified, correlated visibility into all security and network events by linking every stage of a traffic flow with a unique Event Correlation ID. This enables end-to-end tracking, streamlined troubleshooting, and comprehensive compliance monitoring across your security environment.

Important

Cisco Secure Access uses SparkPost as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (like an ISP) may block communications from SparkPost as marketing-related spam. If after scheduling your reports you do not receive them, check the spam filter at your mail server gateway. Whether your mail server gateway is hosted locally or in the cloud, it's likely the email was quarantined at that level.

Secure Access sends its reports from scheduled-reports-feedback@opendns.com.

Check Your Spam Folder

Secure Access uses SparkPost as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (for example, an ISP) may block communications from SparkPost as marketing-related spam. If you do not receive your scheduled reports, check the spam filter at your mail server gateway. Whether your mail server gateway is hosted locally or in the cloud, it's likely the email was quarantined at that level.

Unsubscribe From a Report

You can unsubscribe from a scheduled report at any time by clicking the **Unsubscribe** link at the bottom of the email.

Schedule a Report

Provides instructions for completing the Schedule a Report workflow in Cisco Secure Access. When scheduling a report, it's important to select filters so that you receive only the data that you want and that your reports don't exceed 10,000 rows–the limit of an emailed report.

When scheduling a report, it's important to select filters so that you receive only the data that you want and that your reports don't exceed 10,000 rows–the limit of an emailed report. As well, you want your scheduled report to be digestible and actionable by recipients. If you choose not to add filters, the report will apply to all traffic types for that report across your entire environment and may contain too much data to be readily read and interpreted by the recipient. With scheduled reports, you select filters for the report before you run the Schedule wizard.

Note

Once scheduled, if you do not receive the report, check the spam filter at your mail server gateway–whether it is hosted locally or hosted in the cloud. It's likely that the email was quarantined at that level.

Before you begin

Full Admin user role. For more information, see Manage Accounts.

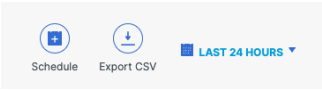
Procedure

1. Navigate to **Monitor** > **Reports** and select the report you want to schedule.

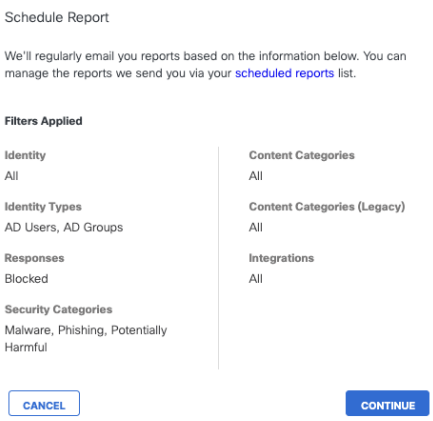
   For a list of schedulable reports, see Report Scheduling.

2. Select filters for the report and then click **Schedule**.

   Filters are applied to the report and the Scheduling wizard opens.



3. Review filters and click **Continue** .

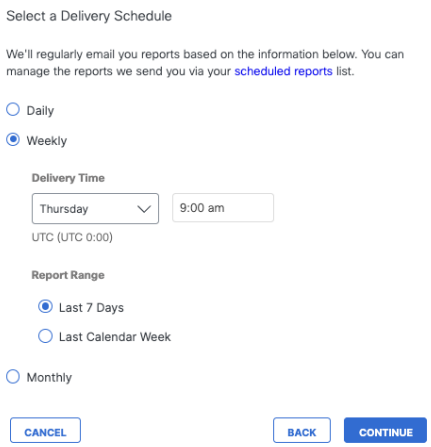


4. Select time parameters to set when and how often you want this report sent to recipients. Click **Continue**.

   For each time period, you can specify a time and range within that time period. Data is limited to 100,000 rows when exporting to CSV. If your report exceeds 100,000 rows, consider re-running the report with a shorter timeframe or with a more granular filter. It's a good idea to check the last row of your first report, then re-run the report from that time period for the next chunk of data.

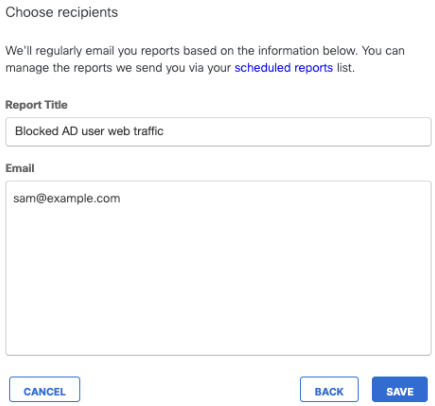
> **Note**
>
> Delivery schedule defaults to the timezone of the user scheduling the report. If additional recipients need reports delivered at a different time, set up additional scheduled reports with the appropriate delivery schedule.

> **Note**
>
> Attempting to schedule a report for a time on the current day, regardless of whether the report is scheduled in the future from the current time on that same day, results in the report being scheduled on the next day at the earliest for weekly and monthly frequencies.



5. Give your report a good descriptive name, add email addresses for recipients of this report, and click **Save**.

   Enter as many recipients as you like separating addresses with commas or semicolons.



6. Your newly scheduled report is listed at **Monitor** > **Management** > **Scheduled Reports**.

   You can update this schedule at any time. For more information, see Update a Scheduled Report.

Update a Scheduled Report

Provides instructions for completing the Update a Scheduled Report workflow in Cisco Secure Access. You can update your scheduled reports at any time.

You can update your scheduled reports at any time. When you update filters for the scheduled report, the Scheduling wizard takes you to the report in question, where you can select filters as necessary and then save the updated schedule.

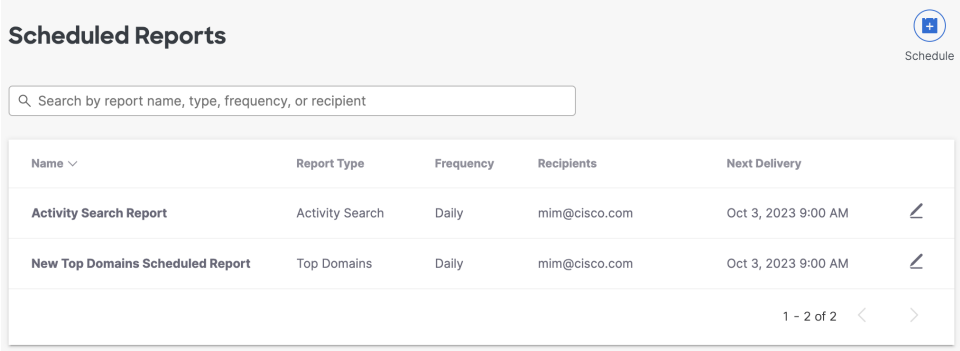
Before you begin

Full Admin user role. For more information, see Manage Accounts.

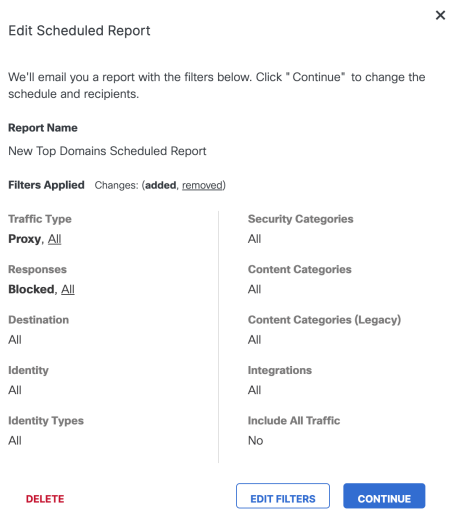
Procedure

1. Navigate to **Monitor** > > **Management** > **Scheduled Reports** and click a scheduled report.

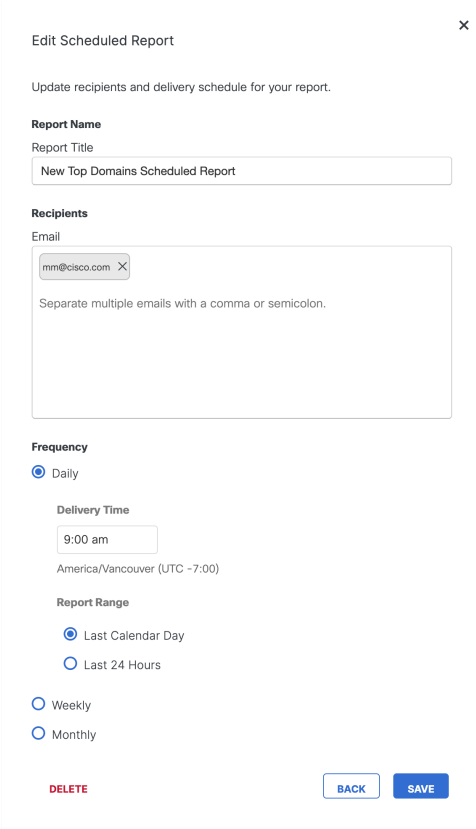
   The Edit Scheduled Report modal opens and lists filters applied to the report.



2. Review and edit filters, if needed. Click **Continue**.

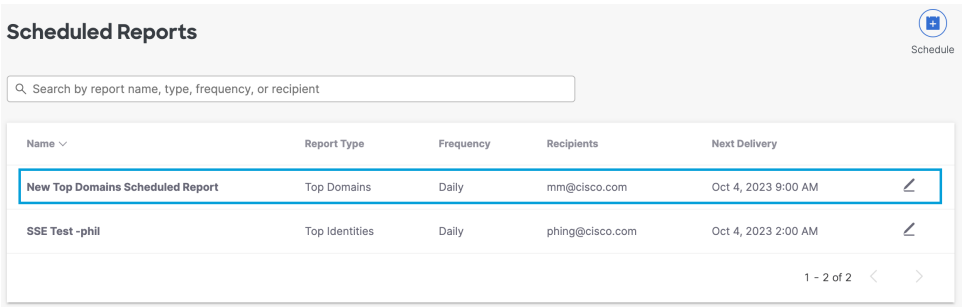


3. Update recipients (press **Enter** to add addresses), the report's delivery schedule, and click **Save**.



Your newly updated scheduled report is listed at **Monitor** > **Management** > **Scheduled Reports**.

> **Note**
>
> This updated report replaces the current report.



Report Search Window and Retention

Describes Report Search Window and Retention in Cisco Secure Access. Secure Access reports will return results as soon as you start sending traffic to Secure Access.

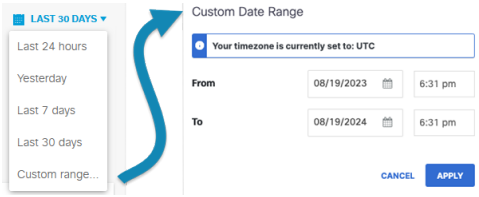
Secure Access reports will return results as soon as you start sending traffic to Secure Access.

Report Search Window

Describes Report Search Window in Cisco Secure Access. Use the date picker to filter report data by a search window date range.

Use the date picker to filter report data by a search window date range.

Most Secure Access reports allow a search window of the **Last 24 hours**, **Yesterday**, **Last 7 days**, **Last 30 days**, or a **Custom range** that you define.



The following reports are limited to a 30-day search window:

- Activity Search Report
- Security Activity Report
- Top Destinations Report

The following reports are limited to a 3-month search window:

- Admin Audit Log Report

Report Retention

Describes Report Retention in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The following reports retain DNS data and all non-DNS data for 90 days :

- Remote Access Logs Report
- Activity Search Report
- Security Activity Report
- Total Requests Report
- Activity Volume Report
- Top Destinations Report
- Top Categories Report
- AI Supply Chain
- Events Report

The following reports retain data for 30 days:

- App Discovery Report
- Private Resource Discovery Report
- Alert Rules

The following reports retain data for one year:

- Cloud Malware
- Data Loss Prevention Report

The following reports retain data indefinitely:

- Admin Audit Log Report
- Third-Party Apps Report

Assess and Monitor Configurations in Secure Access

The deployment insights report provides a cumulative score and detailed checks for your organization configurations, including a breakdown by domain and severity.

Secure Access assesses your organization's configurations to identify security risks, errors, or configuration gaps. Assessments can be run manually by an administrator. Secure Access assesses only the configuration domains and checks that apply to your organization based on your enabled services, subscriptions, and available configuration data. Checks for services that are not licensed or enabled do not affect your assessment score.

The platform assigns severity labels—Critical, High, Medium, or Low—to checks needing action, which contribute to the cumulative posture score.

Secure Access monitors the following applicable configuration domains:

- **Certificates:** Identifies expiring RAVPN, SAML SP, and custom CA certificates before they cause authentication, VPN, or private access disruptions.
- **Client Profiles:** Checks ZTNA client profile safeguards, including auto-enrollment for roaming users and trusted-network definitions that could accidentally bypass enforcement.
- **Network Connectivity:** Validates tunnel presence, tunnel health, split-tunnel steering, region or IP pool consistency, and cipher strength to reduce outage and routing-risk conditions.
- **Data Loss Prevention:** Ensures DLP rules are enabled, cover sensitive data such as PII, use blocking actions where required, and apply broadly across identities.
- **Security Controls:** Identifies overly broad access rules, missing threat-category blocks, weak default internet policy, and missing posture checks for sensitive private resources.

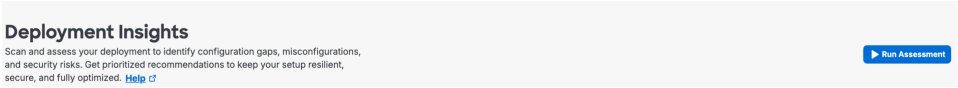
After reviewing the assessment checks, you can take direct action to modify your configuration settings and resolve identified security gaps.

Before you begin

You must have a full admin user role to access the deployment insights report. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Deployment Insights**.
2. Click **Run Assessment** to get the latest assessment score for the configurations in the organization.

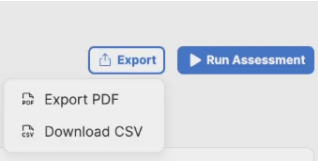


   - If your organization has add-on features such as data loss prevention enabled, select the add-ons you want to include in the assessment.
   - If data loss prevention is not enabled, the assessment runs for the four standard domains.

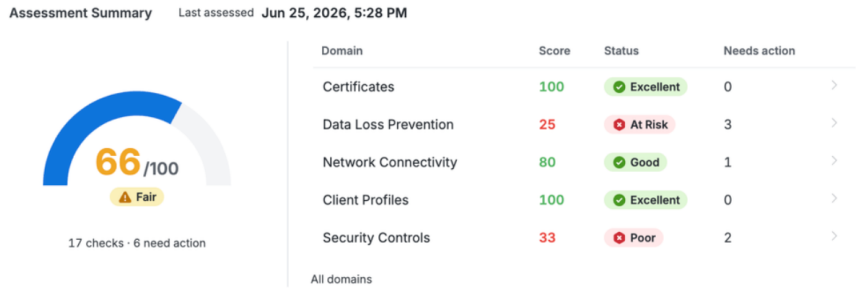
- If data loss prevention is not subscribed, the assessment runs for the four standard domains and the add-on selection modal does not appear.

> **Note**
>
> Only add-on products appear in the **Run Assessment** dialog as default products are included automatically. Add-ons not selected for a run are excluded from the cumulative score.

Secure Access reviews the configurations in the organization, assigns severity-labeled assessment checks, scores the configurations, and reports on the assessments. To export the latest report of the assessments, click **Export** and then choose **Export PDF** or **Download CSV**.



3. Review the **Assessment Summary** to view the cumulative score, status gauge, last assessed date, and a per domain breakdown of the score, status, and needs action count for each domain.



Understanding assessment results

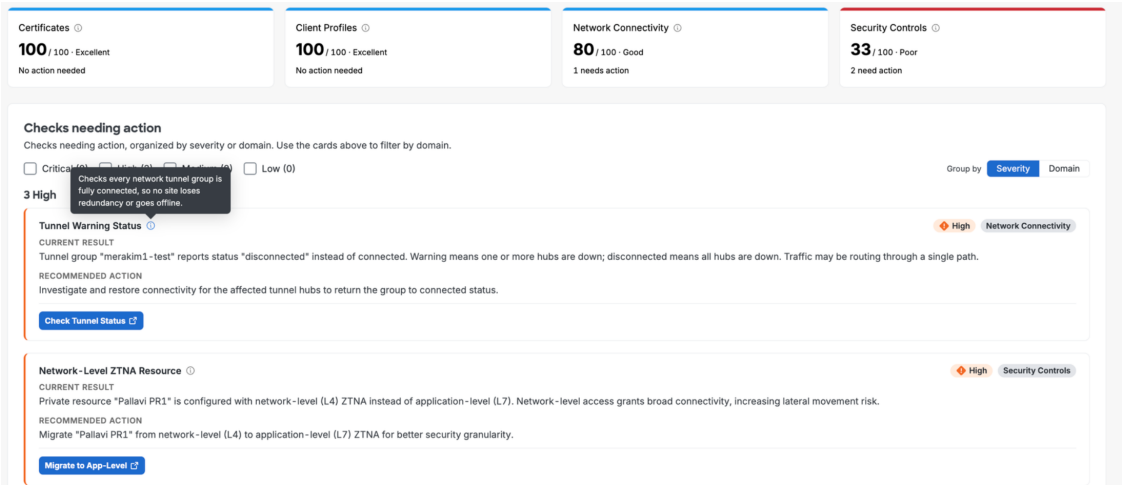
- **Cumulative score:** The summary provides an overall posture score on a scale of 0 to 100, which helps you track improvement over time and benchmark your deployment against recommended baselines.
- **Status labels:** Secure Access assigns the following labels to your organization posture:
  - **Excellent:** 85 to 100
  - **Good:** 70 to 84
  - **Fair:** 50 to 69
  - **Poor:** 30 to 49
  - **At risk:** 0 to 29
- **Domain breakdown:** Assessment checks are categorized by domain to help you identify specific areas of risk, such as certificates, network connectivity, client profiles, security controls, and data loss prevention.
- **Actionable checks:** Checks are sorted by severity to help you prioritize remediation. Each check includes a description of the impact and a direct link to the relevant dashboard page to facilitate quick resolution.

4. Click a domain card to filter the checks needing action for that specific domain.

> **Note**
>
> Click the information icon next to any domain to view a tooltip that explains the assessment criteria for that domain.

The **Checks needing action** section displays results organized by severity or domain. Each check shows the severity, category, and recommended action.

> **Note**
>
> Click the information icon next to any check to view tooltips that explain the criteria for the check status.



a) Under **Group By**, choose whether to filter the checks by **Severity** or **Domain**.
b) (Optional) Choose the severity level: **Critical**, **High**, **Medium**, or **Low**.

   Secure Access filters checks by the selected severity level.

c) Choose **Domain** to filter the checks for that specific domain.

5. Navigate to an assessment under **Checks needing action** to view the list of configuration gaps.
   - **Current result:** Displays the current configuration state that triggered the check.
   - **Recommended action:** Provides the steps required to resolve the security gap.

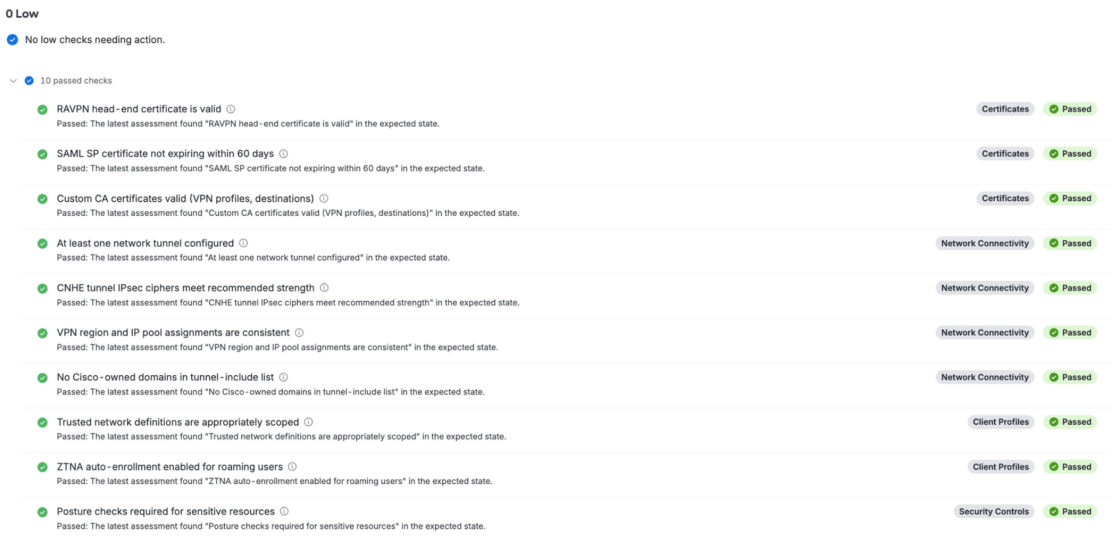
6. Click the action button to open the relevant Secure Access configuration page where you can resolve the check.



> **Note**
>
> The action button does not enable inline editing from the **Checks needing action** card but directs you to the appropriate configuration page within Secure Access to modify settings.

7. Expand **Passed checks** to review successful configurations.

> **Note**
>
> Click the information icon next to a passed check to view tooltips that explain the criteria for the successful status. This information helps you maintain a consistent security posture and provides context for future troubleshooting if a check fails.



71 Activity Reports

Topics:

- Activity Search Report
- Security Activity Report
- Activity Volume Report

Provides an overview of Activity Reports in Cisco Secure Access, including Activity Search Report, Security Activity Report, and Activity Volume Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Activity Search Report

Describes Activity Search Report in Cisco Secure Access. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time.

The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time. Use this report to find the result of every DNS, URL, and IPv4 or IPv6 request from your various sources in descending date and time.

You can also refine your search using filters to help identify security issues that require attention.

View and Customize the Activity Search Report

Describes View and Customize the Activity Search Report in Cisco Secure Access. This topic explains the functions of the Activity Search report and where to find the report in Secure Access.

This topic explains the functions of the Activity Search report and where to find the report in Secure Access.

Prerequisites:

A minimum user role of Read-only. For more information, see Manage Accounts.

The following procedures describe how to:

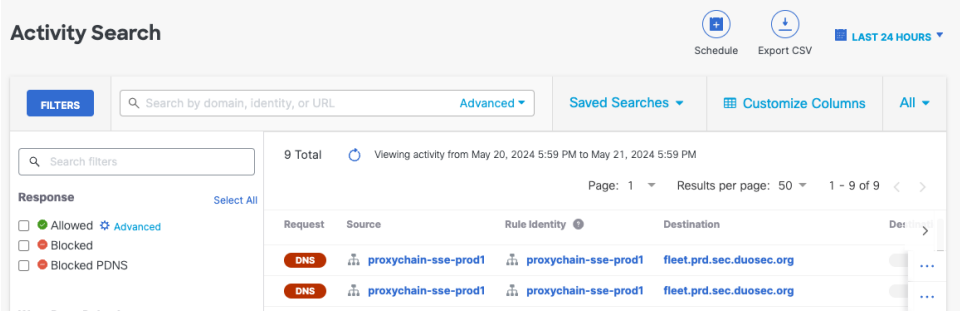
- View the Activity Search Report
- Customize the Activity Search Report
- Save Activity Search Report columns and filters for future use
- Customize and Manage Saved Searches
- View Access Policy Rule from Activity Search

View the Activity Search Report

Provides instructions for completing the View the Activity Search Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**. This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time.



The Activity Search report supports partial results if one or more event type queries (such as Proxy, Firewall, IP, Intrusion, or Decryption) fail due to an internal error. The report displays all available results from the successful queries, rather than showing an error for the entire request. Any unavailable event types will be clearly indicated in a message displayed on the screen.

> **Note**
>
> This feature update ensures continued visibility into available security data, even when certain backend services encounter issues. All retrieved data remains accessible for review and export.

2. Hover over individual column values to apply it as a search filter or to exclude it from the search.
3. To learn more about individual results, click the blue ellipsis **View Actions** icon to the right of each search result. For more information, see View Activity Search Report Actions.

Customize the Activity Search Report

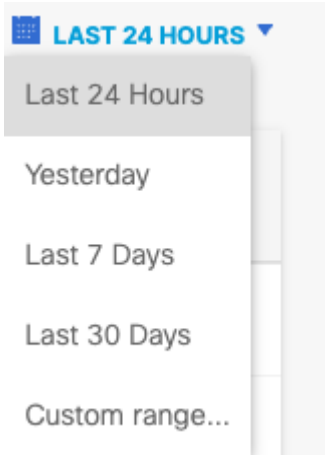
Provides instructions for completing the Customize the Activity Search Report workflow in Cisco Secure Access. Choose a time frame to view the report.

Procedure

---

1. Choose a time frame to view the report.

   The default is **Last 24 Hours**. The maximum is **Last 30 Days**.



2. **Customize Columns** to select columns to display, drag and drop to reorder column position, then click **Apply**.

Column name	Column description
Request	When **All Requests** is selected, this column displays the type of request for each event. Event request types are DNS, Web, Firewall, IPS, ZTNA Clientless, ZTNA Client-based, and Decryption.
Source	The name of the source of the request. Applicable to all request types.
Rule Identity	The identity of the source that Secure Access used to determine which rule applied to the request. Applicable to DNS, Web, Firewall, and ZTNA requests. A request can have multiple identities. Click the row to view Event Details including all identities associated with a request. For more information, refer to View Activity Search Report Actions.

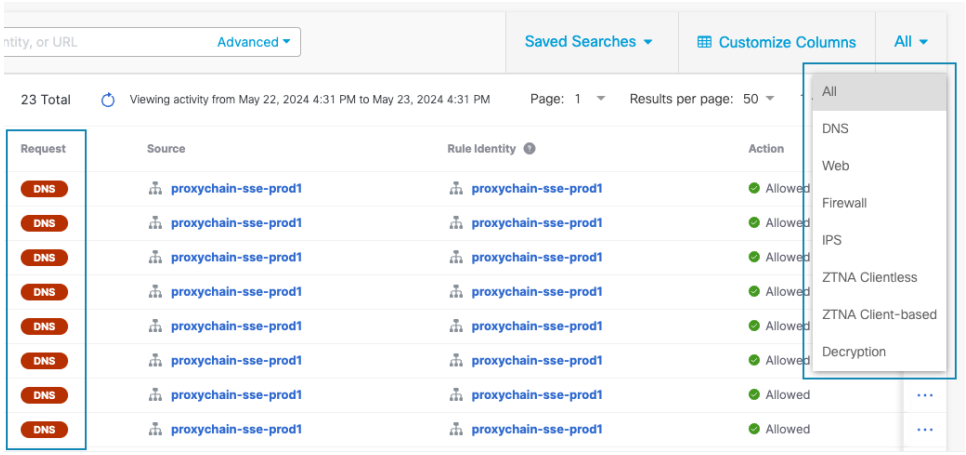
Column name	Column description
Destination	The destination of the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
Destination IP	The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and Decryption requests.
Destination Port	The UDP/TCP port of the destination request. Applicable to client-based ZTA requests. For more information, refer to Comparison of Client-Based and Browser-Based Zero Trust Access Connections.
Destination Country	The two-character country identifier. Applicable to DNS, Web, and Firewall requests.
File Name	The name of the file involved with the activity, where applicable. Applicable to Web and Firewall requests. **Note** File Name will only populate for traffic matching rules with File Type Control or File Inspection enabled (you can enable File Type Control without blocking any file types by clicking enable and saving the rule.) If none of the rules have File Type Control enabled, the file name and extension fields remain blank.
Internal IP	The internal IPv4 or IPv6 address of the request. Supports both compressed and long-form IPv6 address formats. Applicable to DNS and Web requests.
External IP	The external IPv4 or IPv6 address of the request. Supports both compressed and long-form IPv6 address formats. Applicable to DNS and Web requests.
DNS Type	The DNS record type. Applicable to DNS requests.
Action	The request is either Blocked or Allowed. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests. **Blocked – Certificate Error** indicates certificate and TLS error events when the request is processed by a ruleset with **HTTPS inspection** and **File Analysis** enabled. **Blocked – AI Supply Chain** indicates end user attempts to download AI model files that are associated with prohibited suppliers, rely on a copyleft license, or can execute arbitrary code when the request is processed by an internet access rule with a security profile for internet access with **AI Supply Chain Blocking** enabled. For more information, refer to AI Supply Chain Report.

Column name	Column description
Categories	Content and Security categories flagged with the activity. Applicable to DNS, Web, and Firewall requests. Click **Dispute Categorization** in the Event Details navigation drawer to suggest a different category for a Source. The label, Block List appears when DNS traffic is blocked by an internet access rule with a specific destination list or destinations set to Any. Block List is a reporting label only and is not a separate manageable category or destination list.
Resource/Application	The resource or application involved with the activity, when applicable. Populates for traffic matching rules with Application Controls enabled. If no rules have Application Controls enabled, then the field will remain blank. Applicable to DNS, Web, Firewall, and ZTNA requests. For more information, refer to Advanced Application Controls.
Signature List Name	The Secure Access Intrusion Prevention System (IPS) signature list applied to the request. Applicable to IPS requests. For more information, refer to Manage IPS Profiles.
IPS Signature	The signature of the known threat that was blocked or logged by Secure Access IPS. Applicable to IPS requests. For more information, refer to Manage IPS Profiles.
Protocol	Displays whether the Web request protocol is HTTP or HTTPS, and whether the Firewall, IPS, or Decryption request protocol is TCP or UDP. Decryption request protocol includes the cryptographic protocol, such as TLS.

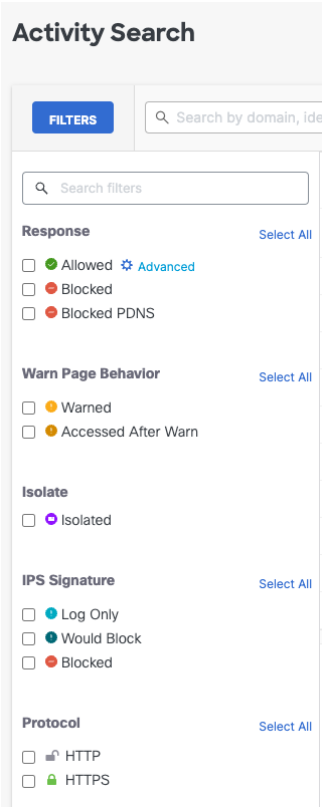
Column name	Column description
Rule Name	The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests. When a DNS event is evaluated and resolved by underlying platform security settings rather than a user-defined policy rule, Secure Access displays one of the following system-generated descriptions: • **Block due to security setting (0):** Access was blocked by a DNS security policy rather than an explicit access rule. • **Allow with domain on global allow list (9223372036854775807):** Access was allowed because the requested domain is explicitly permitted on your Global Allow List. • **No action with default rule not defined (9223372036854775806):** No action occurs because the traffic does not match any user-defined rule and a default catch-all rule does not exist. • **Error due to invalid policy (9223372036854775805):** An error occurred during evaluation due to an invalid policy configuration. **Note** System-generated policy names appear as plain text in the report and do not contain a clickable link to the Access Policy page. Click the rule name to view your Access Policy where the rule is configured. For more information, refer to Manage the Access Policy. Click the row to view Event Details including details of the rule (such as destination list or schedule applied). For more information, refer to View Activity Search Report Actions.
Application Category	If an application is involved with the activity, this column contains the categories associated with the application. Applicable to DNS, Web, and Firewall requests. For the full list of application categories, refer to Application Categories.
Application Protocol	If an application is involved with the activity, this column contains the protocol for the application (HTTP, SSL, RTP, DNS, or none). Applicable to Firewall requests.
Request Method	The HTTP method used by the request. Applicable to Web requests.

Column name	Column description
Referer	The URI from which the request originated. Applicable to Web requests.
Status Code	Standard HTTP status codes. Applicable to Web requests.
Content Type	The HTTP content type. Applicable to Web requests.
File Extension	The extension of the file involved in the activity, where applicable. Applicable to Web and Firewall requests.
OS	The operating system of the client's device. Applicable to ZTNA requests.
Browser	The client's browser. Applicable to ZTNA requests.
Location	The two-character country identifier. Applicable to ZTNA requests.
Location IP	The IPv4 or IPv6 address of the client. Supports both compressed and long-form IPv6 address formats. Applicable to ZTNA requests.
Date and Time	The date and time stamp of the request. Applicable to all request types.

3. Filter **Request** by selecting an option from the dropdown menu at the top right. Filters and columns update to those that are relevant to the selected Request type. The default Request type is **All**.



4. Search and select additional **Filters** to the left of the report results. For the complete list of filters and options, see the table below.



Choose from the following filters and options. Filter options available in this menu are determined by the **Request** selected in the previous step.

Note

Filters apply a logical **OR** relationship between options, except in the case **Event Type**. Selecting more than one **Event Type** option will not return results because the **Event Type** filter applies a logical **AND** relationship between options.

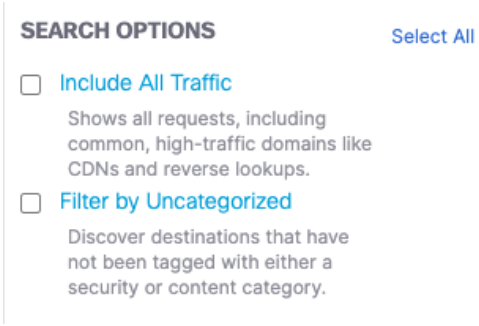
For example, if you filter for both the **Public Application** and **Destination List** event types, the Activity Search report will not return any results because an event can have only one event type.

For all other filters, selecting some or all options can return results. For example, if you filter for both the **HTTP** and **HTTPS** protocols, the Activity Search report will return all web events because they will have used either the HTTP **OR** HTTPS protocol.

Filter	Filter options
Response	**Allowed** **Blocked** **Blocked PDNS** The Response filter applies a logical **OR** relationship when you select more than one option. Optionally, you may apply one or both advanced options to the Allowed event filter: **Allow**: All events that were allowed by passing through your security policies. For Web Policies, this will include the Allow-Security enforced action. **Security Overridden**: Identities will be permitted to access destination even if we detect a security issue. This action will only appear on activity associated with Web Policies.
Warn Page Behavior	**Warned** **Accessed After Warn** The Warn Page Behavior filter applies a logical **OR** relationship when you select more than one option.
Isolate	**Isolated** events are browser-based security threats that were redirected to a Secure Access cloud-based host. For more information, refer to About Isolated Destinations.
IPS Signature	**Log Only** **Would Block** **Block** The IPS Signature filter applies a logical **OR** relationship when you select more than one option.
Protocol	**HTTP** **HTTPS** The Protocol filter applies a logical **OR** relationship when you select more than one option.

Filter	Filter options
Event Type	**Public Application** **Destination List** **Any Security Category** **Any Content Category** **Cisco AMP Disposition is Malicious** **Antivirus Disposition is Malicious** **Integration** **Tenant Controls** **Certificate and TLS Errors** **Data Loss Prevention** **Geolocations** The Event Type filter applies a logical **AND** relationship when you select more than one option and will return only one type of event.
Identity Type	The type of source in the **Rule Identity** column. Identity Type options vary by event and by organization. The Identity Type filter applies a logical **OR** relationship when you select more than one option.
Decryption Actions	**Decrypt Inbound** **Decrypt Outbound** **Do not Decrypt** **Decrypt Error** The Decryption Actions filter applies a logical **OR** relationship when you select more than one option.
Security Categories	For the full list of filter options, see Threat Category Descriptions. The Security Categories filter applies a logical **OR** relationship when you select more than one option.
Content Categories	For the full list of filter options, see Available Content Categories. The Content Categories filter applies a logical **OR** relationship when you select more than one option.

5. Select **Search Options** below the **Filters** menu in the previous step.
   - **Include All Traffic** – Includes data from all domains including noisy domains that are filtered out by default.
   - **Filter by Uncategorized** – Includes destinations that are not classified under a specific security or content category.

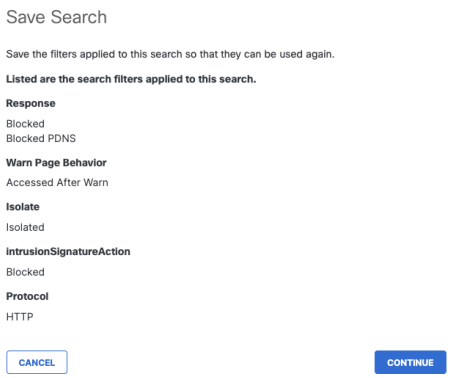


Save Activity Search Report columns and filters for future use

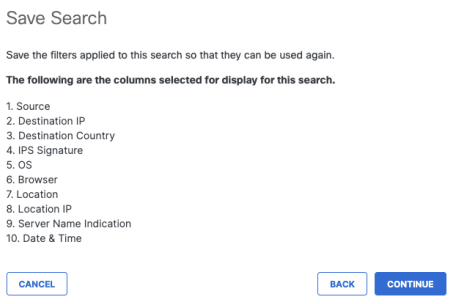
Provides instructions for completing the Save Activity Search Report columns and filters for future use workflow in Cisco Secure Access. Once you select a filter on a new search, a Save Search button will appear.

Procedure

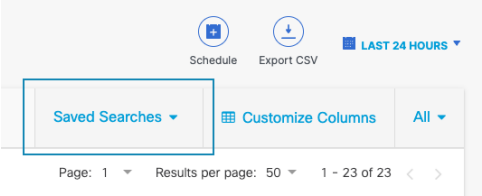
1. Once you select a filter on a new search, a **Save Search** button will appear. Configure filters and customize columns, then click **Save Search**.
2. Review search filters applied to this search, then click **Continue**.



3. Review customized columns selected for display for this search, then click **Continue**.



4. **Search name** is required and **Description** is optional. Once you **Save**, you will be able to access and update your customized report from the **Saved Searches** dropdown at the top right of the report.



Customize and Manage Saved Searches

Describes Customize and Manage Saved Searches in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Activity Search Report supports enhanced customization and search management with the following functions:

- **Auto-Save of Search State:** When you apply filters or customize columns, your current view is automatically saved. If you navigate away from the Activity Search Report and then return, your last auto saved state including filters and column selections is automatically restored.
- **Restore Options:** Restore options will appear only when a previous state or changes exist to revert to. Restore options allow you to quickly revert your report view to a previous or default state.
  - **Restore to default Layout:** Revert the report to its original default view.
  - **Restore to Previous State:** Return to your last auto-saved view.

    This option is disabled if no previous state exists (such as on your first visit or before making changes).

View an Access Policy Rule from the Activity Search Report

Use this procedure to quickly access and review the access policy rule associated with a specific activity found in the Activity Search report for faster investigation and policy tuning.

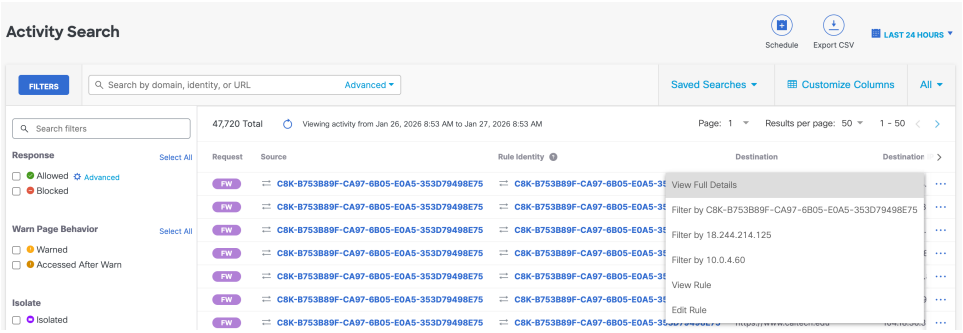
You can seamlessly move from an activity record in the Activity Search report to the associated access policy rule. This feature enables faster investigation, troubleshooting, and policy tuning by allowing you inspect, view, or edit the rule that triggered a specific activity.

Note

System-generated DNS rules (such as Block due to security setting (0)) are triggered by global security settings rather than user-defined rules. These specific activity records do not contain a link to the Access Policy page.

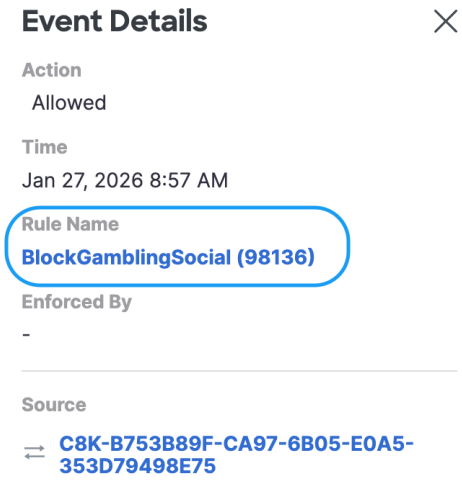
Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Use the filters and search bar to locate the activity you want to investigate in the Activity Search report. For more information, see Customize the Activity Search Report.
3. In the Activity Search results, locate the activity record you want to investigate and click the **View Actions** (three-dot) menu for that record.

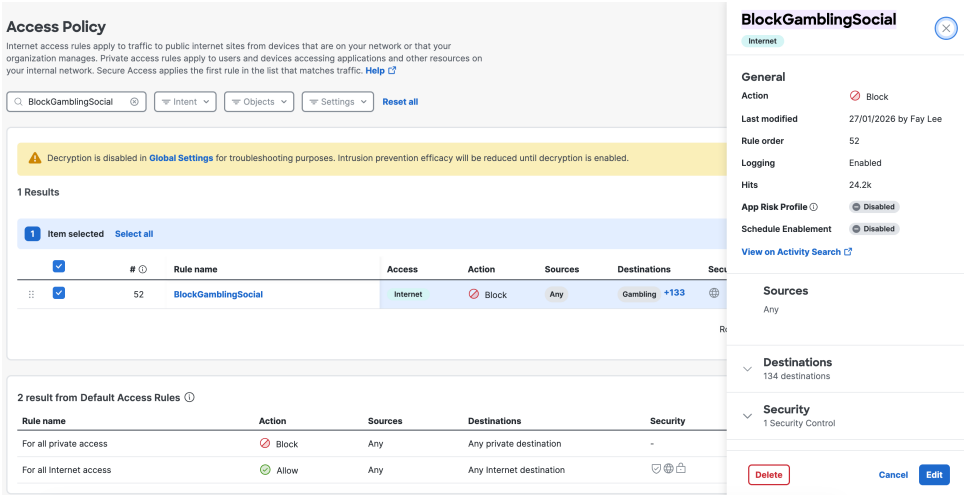


Choose one of the following options:

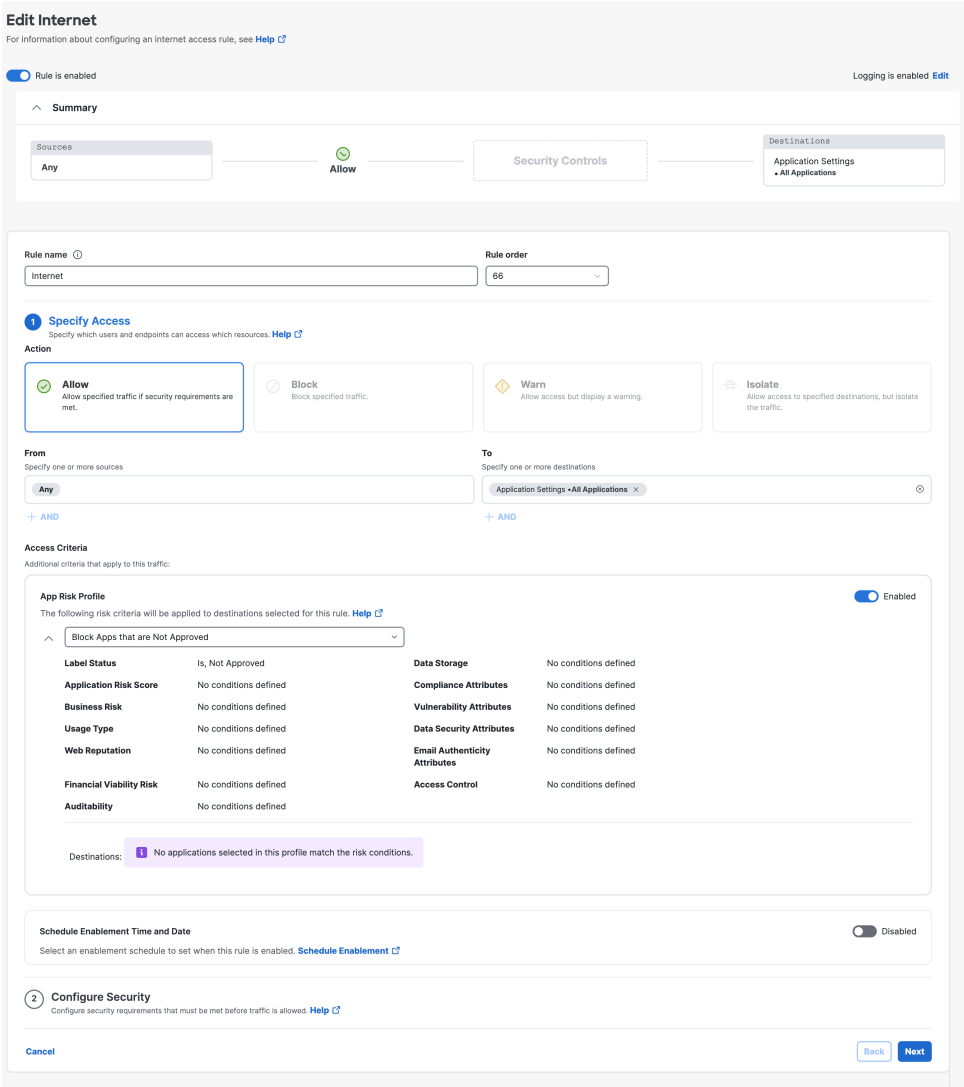
- **View full details**: Opens the **Event Details** panel. In the **Event Details** panel, click the rule name to navigate to the Access Policy page with the associated rule filtered and highlighted.



- **View Rule**: Directly opens the Access Policy page with the relevant rule filtered and highlighted.



- **Edit Rule**: Opens the associated rule in edit mode, allowing you to modify its configuration as needed.



View Firewall Events in Activity Search Report

Describes View Firewall Events in Activity Search Report in Cisco Secure Access. The Activity Search report includes full details about Firewall requests that have been allowed or blocked by an Access Policy rule.

The Activity Search report includes full details about Firewall requests that have been allowed or blocked by an Access Policy rule.

For more information about the Activity Search report, see View the Activity Search Report. For more information about your Access Policy rules, see Manage the Access Policy.

> **Note**
>
> File Name and other fields related to file inspection and file type controls will only populate for events involving file access that match private access rules with File Inspection or File Type Control enabled. If no private access rules have File Inspection or File Type Control enabled, the file name and extension fields will remain blank for events with the Firewall request type. For more information, see Get Started With Private Access Rules, Manage File Inspection and File Analysis, and Manage File Type Controls.

Filter the Report by Firewall Requests

Provides instructions for completing the Filter the Report by Firewall Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

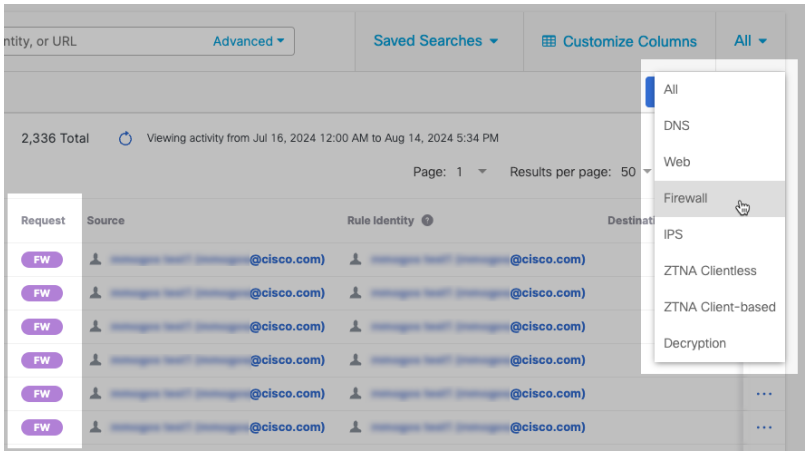
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view events from the **last 24 hours** (default), **Yesterday** , **Last 7 Days**, **Last 30 Days**, or a **Custom range**.

   The label **FW** in the **Request** column indicates a Firewall event.
3. Select the **Firewall** option from the dropdown menu at the top right to filter the report for Firewall events. Columns and Filter options update to those that are relevant to Firewall events.



4. Click the row to view Event Details.

   The Activity Search Report displays Event Details for each search result in a navigation drawer on the right. For more information, see View Activity Search Report Actions.

   Firewall event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see View and Customize the Activity Search Report.

   - **Action**
   - **Time**
   - **Rule Name**
   - **Source**

- **Destination IP**
- **Categories**
- **File Name**
- **Protocol**
- **Application Protocol**

Firewall event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Source IP	The source IPv4 or IPv6 address. Supports both compressed and long-form IPv6 address formats.
Source Port	The network port number on the source host from which the request originated.
Destination Port	The TCP or UDP port number on the destination host to which the request was sent. This field identifies the specific service or application targeted by the connection (for example, port 80 for HTTP or port 443 for HTTPS).
Resource/Application	The name of the resource or application.
Session Bytes Sent	The total number of bytes sent during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data sent from the source to the destination for the event session.
Session Bytes Received	The total number of bytes received during the Firewall session. This value is reported at session disconnect and reflects the cumulative amount of data received from the destination by the source for the event session.
File Status (Disposition)	The file's Cisco AMP disposition: • **Clean**: Indicates that the AMP cloud categorized the file as clean. • **Malware**: Indicates that the AMP cloud categorized the file as malware, or local malware analysis identified malware. • **Unknown**: Indicates that the system queried the AMP cloud, but the AMP cloud has not assigned the file a disposition.
SHA256 Hash	The checksum of the file, if available and the event matched rules with File Type Control or File Inspection enabled.
File Transfer Direction	**DOWNLOAD**, **UPLOAD**, or **UNKNOWN**, if the event matched rules with File Type Control or File Inspection enabled.
Identified Threat	The name of the detected malware.

Field Name	Description
Malware Analysis Detected	If the event matched rules with File Inspection enabled, this field shows one of the following values as a result of file analysis by Cisco Secure Malware Analytics. For more information, see Enable File Analysis by Cisco Secure Malware Analytics. • **UNKNOWN** • **NOT ANALYZED** • **ANALYSIS COMPLETE NO VIRUS** • **ANALYSIS FAILED** • **ANALYSIS COMPLETE MALWARE DETECTED**
Threat Severity Score	The threat score most recently associated with this file. This is a value from 0 to 100.
File Type Identifiers	The type of file. For example, PDF or MSEXE.
File Size (bytes)	The size of the file in bytes, if the event matched rules with File Type Control or File Inspection enabled.
Archive File Name	The name of the archive file involved with the activity, if the event matched rules with File Type Control or File Inspection enabled.
Archive Extraction Depth	The level (if any) at which the file was nested in an archive file.
Archive SHA-256 Hash	The checksum of the archive file, if the event matched rules with File Type Control or File Inspection enabled.

View Web Events in Activity Search Report

Describes View Web Events in Activity Search Report in Cisco Secure Access. The Activity Search report provides a detailed view of the web events in your organization.

The Activity Search report provides a detailed view of the web events in your organization. For more information about the Activity Search report, see View the Activity Search Report.

Filter the Report by Web Requests

Provides instructions for completing the Filter the Report by Web Requests workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

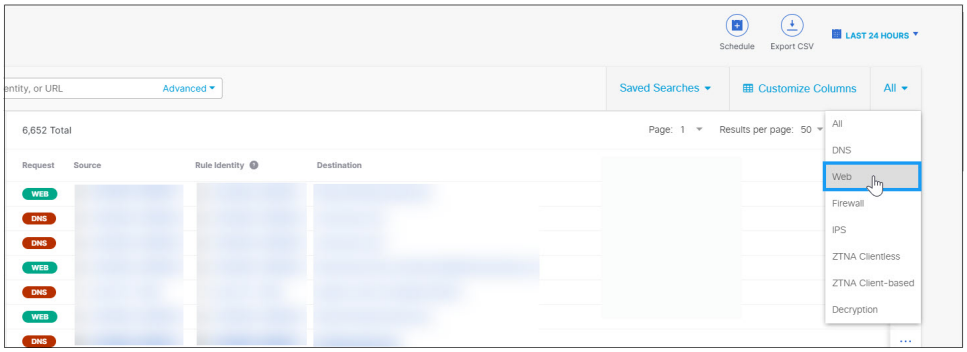
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

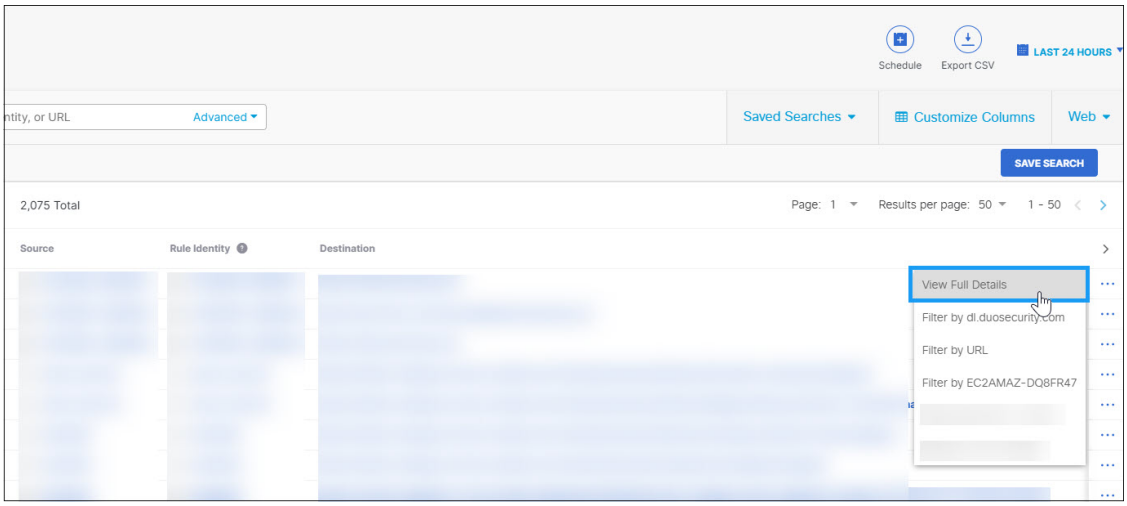
Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **last 24 hours** (default), **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**.

3. From the drop-down menu at the top-right of the table, choose the **Web** option to filter the report for web events.



4. Click the ellipsis (**...**) and choose the **View Full Details** option to view web event details in the side panel.



For more information, see View Activity Search Report Actions.

Web event details include the following fields that are also available as Activity Search report columns. For more information about these fields, see Customize the Activity Search Report.

- **Action**
- **Time**
- **Rule Name**
- **Source**
- **Rule Identity**
- **Internal IP Address**
- **External IP Address**
- **Destination**
- **Categories**
- **Resource/Application**
- **Application Category**
- **Content Type**
- **Request Method**
- **Referrer**
- **Status Code**

Web event details also include the following fields that do not appear as Activity Search report columns.

Field Name	Description
Hostname	Fully Qualified Domain Name (FQDN) of the machine or container from which the event originated.
File Action (Remote Browser Isolation)	Action taken on a file, such as Viewed, Original File Downloaded, Sanitized PDF File Downloaded.
Total Size, in Bytes	The number of bytes sent from the client for all the requests, including HTTP headers, for example, 234.
User Agent	The user agent string as captured by the proxy, for example, Mozilla 5.0 (X11; Linux x86_64; rv:12.0) Gecko 20100101 Firefox 21.0.
SHA256 Hash	This represents the SHA-256 hash of the response body.
Egress IP Address	The IP address is used by the proxy to communicate with the origin server. Dot notation is used for IPv4 and RFC 5952 is used for IPv6 , for example, 1.2.3.4, 2001:db8::1.
Egress Data Center	The data center that processed the request.
YouTube Channels	The YouTube channel name, such as @Cisco in the Cisco YouTube channel (https://www.youtube.com/@Cisco).
YouTube Categories	The set of YouTube categories, such as Education, Entertainment, Animation.

View Zero Trust Events in Activity Search Report

Describes View Zero Trust Events in Activity Search Report in Cisco Secure Access. The Activity Search report includes the full details about the Zero Trust Access traffic events in your organization.

The Activity Search report includes the full details about the Zero Trust Access traffic events in your organization. For more information about the Activity Search report, see View the Activity Search Report.

> **Note**
>
> If you assign **Block** to a rule that is destine for a private application and there is an HTTPS “Get” request for a downloadable file, the rule blocks matching traffic and actions appropriately but the event appears in Activity Search twice: one entry as the action is “blocked” and one entry as the action is “allow”. Activity Search does not currently condense events that generate multiple entries and thusly increases the hit counter as “2”.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

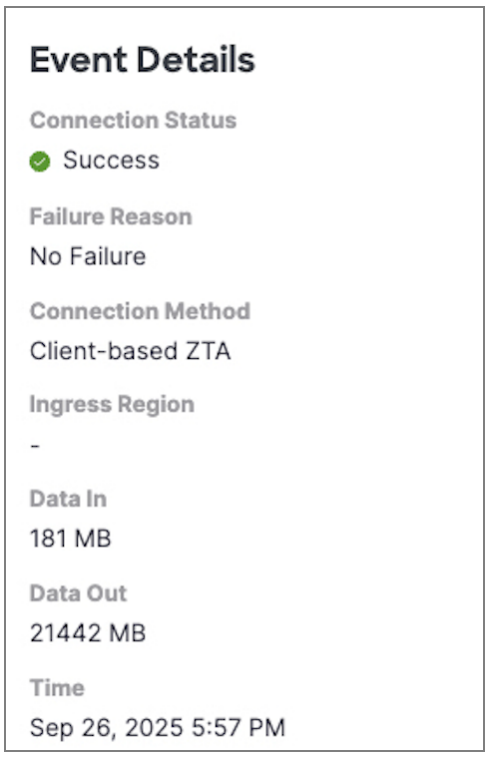
Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **last 24 hours** (default), **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**.
3. From the **Requests** menu, choose a request type or the default of **All**. Filters update to those that are relevant to the type of request chosen.
4. For an item in the report, click on the ellipsis (**...**). Click **View Full Details** to display the details of the Zero Trust Access event.

Event Details

Describes Event Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

View the Zero Trust event details in the Activity Search report.

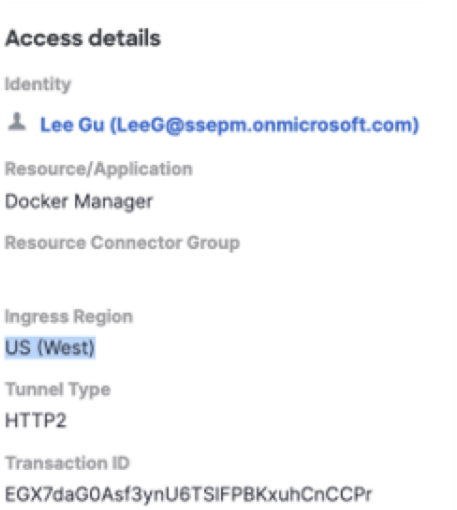


Field Name	Description
Connection Status	Indicates the result of the connection attempt, such as Success or Blocked.
Failure Reason/Block Reason	If the connection was not successful, this field explains the reason for the failure. Block Reason is displayed for authorization events. Failure Reason is displayed for flow events.
Connection Method	The type of connection method: ZTA Client-based or ZTA Browser-based.
Ingress Region	The geographic region of the data center where Secure Access received the incoming connection request.
Data In	The total amount of data received from the client during the connection session, displayed in megabytes (MB).
Data Out	The total amount of data sent to the client during the connection session, displayed in megabytes (MB).
Time	The timestamp indicating when the event occurred.

Access Details

Describes Access Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

View the Zero Trust access details in the Activity Search report.

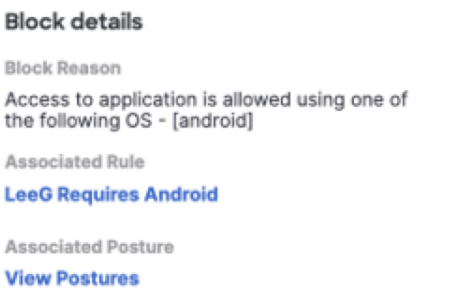


Field Name	Description
Identity	The name and email of the user identified in the Zero Trust connection event.
Ingress Region	The geographic region of the data center where Secure Access received the incoming traffic.
Resource/Application	The name of the private application.
Zero Trust Access Profile	The name of the Zero Trust Access Profile used in the event.
Trusted Network	The trusted network identified in the connection, disconnection, or evaluation of a policy-triggered event.
Egress IP	The IP address used when traffic exits a network or system to reach the destination outside of it.
Resource Connector Group	The ID of the resource connector group that provides access to the private resource.
Tunnel Type	The type of traffic supported by the network tunnel, which the endpoint established with the proxy. The transport protocol on the tunnel is either **HTTP** or **HTTP3**.
Transaction ID	The unique ID associated with the Zero Trust connection request. Use the transaction ID to correlate and troubleshoot connection issues.

Block Details

Describes Block Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

View the Zero Trust block details in the Activity Search report.

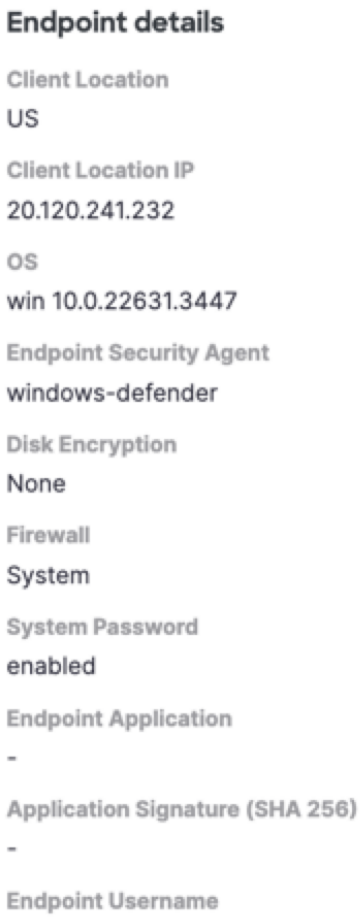


Field Name	Description
Block Reason	Secure Access provides an explanation for blocking access to the private resource.
Associated Rule	When access was blocked for not meeting access or posture requirements, Secure Access reports the closest matched policy rule that would have allowed access.
Associated Posture Profile	The posture profile that is configured for the associated rule.

Endpoint Details

Describes Endpoint Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

View the Zero Trust endpoint details in the Activity Search report.



Field Name	Description
Client Location	The two-character country identifier.
Client Location IP	The IPv4 or IPv6 address of the client. Supports both compressed and long-form IPv6 address formats.
OS	The operating system of the client's device.
Endpoint Security Agent	The name of the endpoint security agent.

Field Name	Description
Disk Encryption	Indicates if the client's device has disk encryption.
Firewall	Indicates if the client environment has a firewall enabled.
System Password	Indicates if the client has a system password enabled.
Endpoint Application	The name of the endpoint application, which initiated the connection.
Application Signature	The SHA256 signature of the endpoint application process.
Endpoint Username	The username that is associated with the endpoint application process.

View AI Semantic Inspection Events in Activity Search Report

Describes View AI Semantic Inspection Events in Activity Search Report in Cisco Secure Access. The Activity Search report provides a detailed view of the Model Context Protocol (MCP) communications on the MCP servers observed by Secure Access for the organization.

The Activity Search report provides a detailed view of the Model Context Protocol (MCP) communications on the MCP servers observed by Secure Access for the organization.

- For information about the AI Semantic Inspection Report, see AI Semantic Inspection Report.
- For information about the Activity Search report, see View the Activity Search Report.

Filter the Report by Semantic Inspection for MCP Servers

Provides instructions for completing the Filter the Report by Semantic Inspection for MCP Servers workflow in Cisco Secure Access. A minimum user role of Read-only in Secure Access.

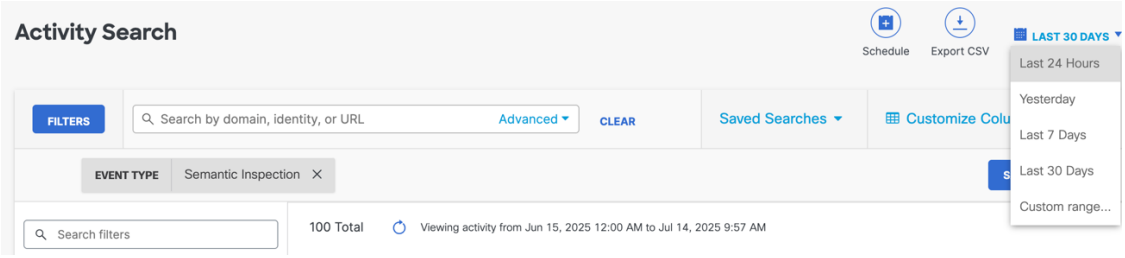
Filter the Activity Search report for Model Context Protocol (MCP) messages on the MCP servers observed by Secure Access.

Before you begin

- A minimum user role of **Read-only** in Secure Access.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**.
2. Choose a time frame to view the report. You can view the results for the **Last 24 hours**, **Yesterday**, **Last 7 Days**, **Last 30 Days**, or a **Custom range**. The default time range is **Last 24 hours**.



3. Navigate to **Event Type**, and then click **Semantic Inspection**.



Secure Access displays the events of the detected MCP messages on the MCP servers.

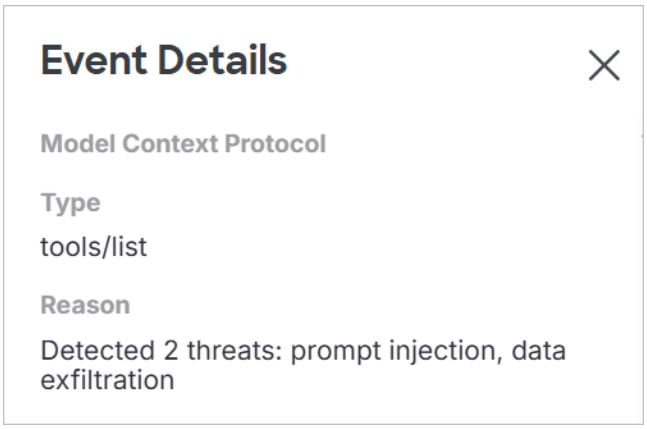
a) Navigate to an item in the table for the Activity Search report, click the ellipsis (**...**), and then choose **View Full Details**.

   In the side panel, Secure Access displays the details of the MCP event on the MCP server. For information about the web events in the Activity Search report, see Filter the Report by Web Requests

b) Navigate to **Model Context Protocol**.

   Secure Access displays the details about the MCP server and the verdict assigned to the MCP messages.

   - **Type**–The type of action performed by the MCP server, for example **tools/call**.
   - **Reason**–The reason for the verdict assigned by Secure Access for the action on the MCP server.



View Activity Search Report Actions

Describes View Activity Search Report Actions in Cisco Secure Access. To learn more about the results of your activity search, click the View Actions icon for a result and choose an item from the menu.

To learn more about the results of your activity search, click the **View Actions** icon for a result and choose an item from the menu.

See Full Details

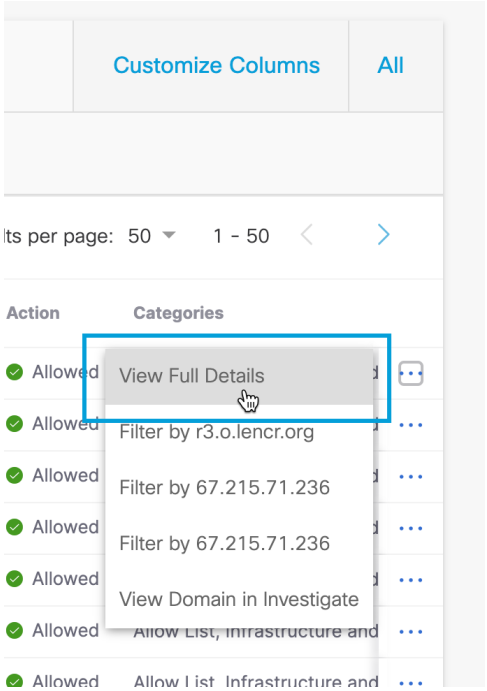
Provides instructions for completing the See Full Details workflow in Cisco Secure Access. For each entry listed, from the View Actions icon, choose View Full Details.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

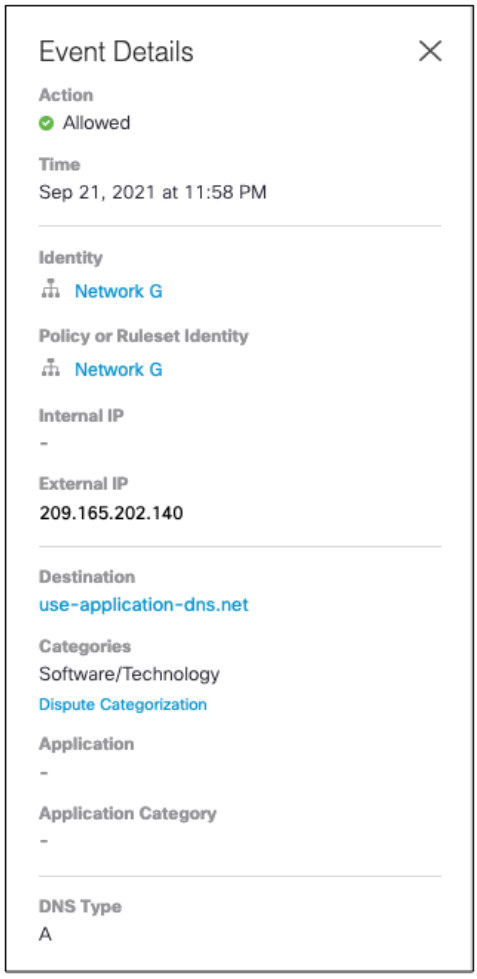
Procedure

For each entry listed, from the **View Actions** icon, choose View Full Details.

What to do next



The details of each activity result are displayed. The details listed depend on the event type.



View Isolated Event Details

Provides instructions for completing the View Isolated Event Details workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

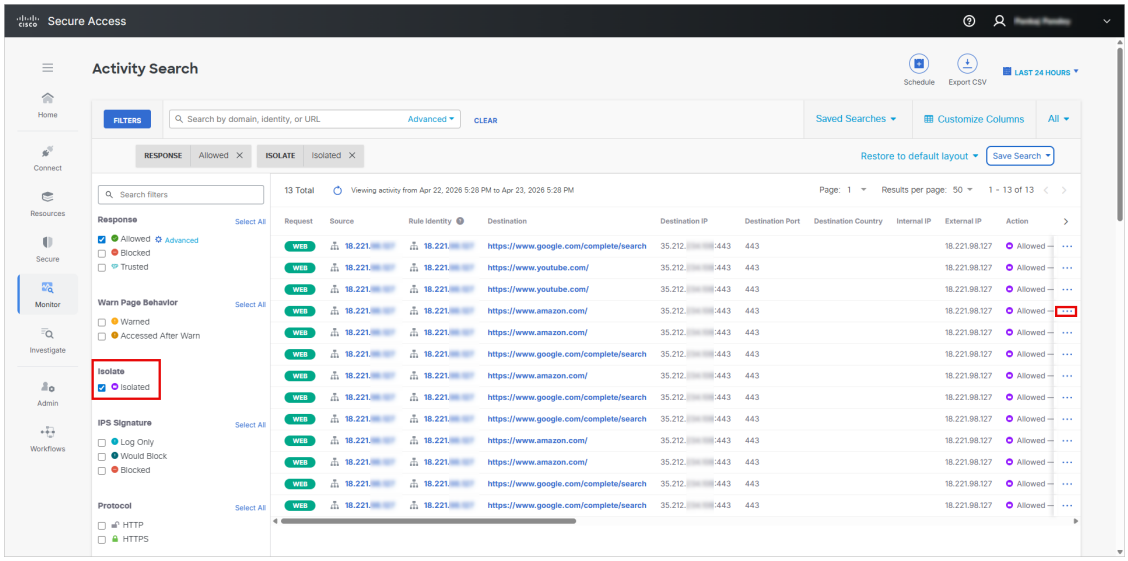
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

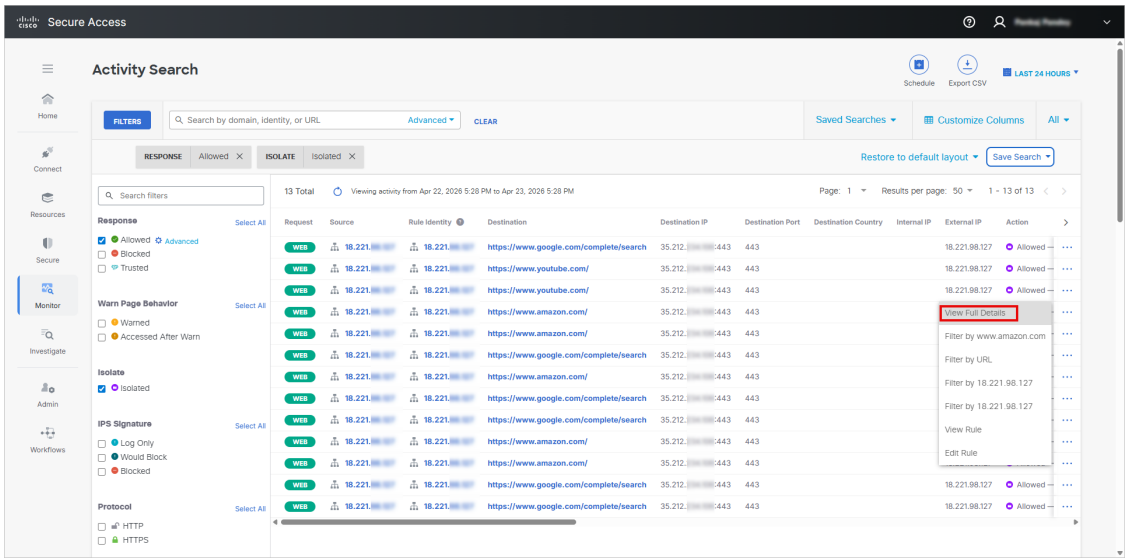
Procedure

1. Navigate to **Monitor** > **Activity Search**.
2. Select **Isolated** in the filter pane.

   The Isolated events appear.



3. Click the **View Actions** icon (three dots) for any event to view a menu of options and then click **View Full Details**.



4. The Event Details window displays information depending on the Event Type:

- **Action** – Indicates the action taken on the event. In this case, the traffic was allowed but routed through an isolated (Remote Browser Isolation) environment.
- **Time** – The timestamp when the event occurred.
- **Rule Name** – The name of the rule that was triggered for this event.
- **Tenant List** – Lists the tenants associated with the event.
- **Tenant ID** – The ID of tenants associated with the event
- **Source** – The IP address from which the request originated.
- **RBI Profile Name** – The name of the Remote Browser Isolation (RBI) profile applied to this session.
- **Rule Identity** – The identity (IP) of the triggered rule.
- **Internal IP Address** – The internal (private) IP address of the source.
- **External IP Address** – The external (public) IP address of the source.

- **Destination** – The full URL the user attempted to access.
- **Hostname** – The hostname/domain of the destination website.
- **Categories** – The content categories assigned to the destination.
- **Dispute Categorization** – An option to dispute or challenge the assigned category.
- **Resource/Application** – The specific application or resource being accessed.
- **Application Category** – The broader category under which the application falls.
- **YouTube Channels** – Specific YouTube channel information (if applicable).
- **YouTube Categories** – YouTube content category (if applicable).
- **Content Type** – Specifies the format and character encoding of the content returned by the destination.
- **File Action (Remote Browser Isolation)** – Indicates any file-level action taken during the RBI session.
- **Total Size in Bytes** – The total size of the data transferred during this event.
- **Request Method** – The HTTP method used for the request.
- **Referer** – The referring URL that led to this request.
- **Status Code** – The HTTP response status code (200 indicates a successful request).
- **User Agent** – Information about the browser and operating system used to make the request.
- **Egress IP Address** – The IP address used to exit the network toward the destination.
- **Egress Data Center** – The data center from which the request exited.

Filter Views

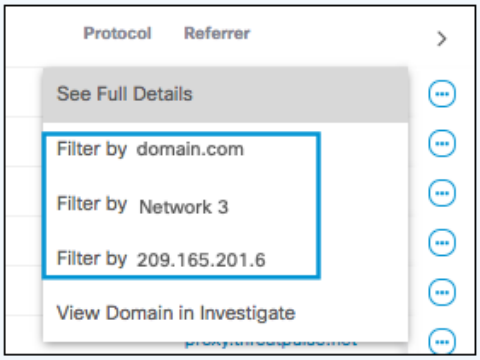
Describes Filter Views in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Where applicable, certain results can be filtered by the following:

- Application
- Destination
- URL
- Source
- External IP

Note

- The URL filter applies only to proxy or web requests, whereas the domain filter applies to both DNS and proxy or web requests.
- The Destination column displays either a URL (for example, https://example.com/profile/log/info) or a domain (for example, www.google.com)
- To filter URLs in the Destination column, use the URL filter. To filter domains in the Destination column, use the domain filter.

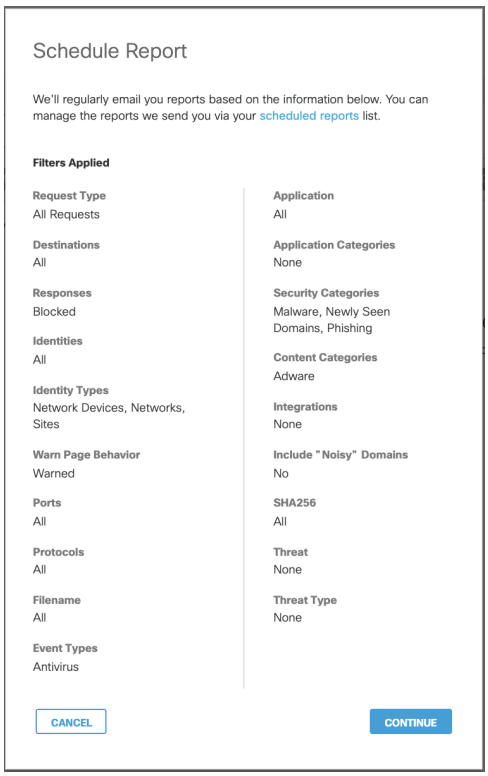


Schedule an Activity Search Report

Describes Schedule an Activity Search Report in Cisco Secure Access. You can schedule a report to be emailed to you at regular intervals.

You can schedule a report to be emailed to you at regular intervals. Your emailed report is a table showing an HTML version of the report and an attached CSV file containing the entire data set. Also included in your email is a link to a live version of the same report. For more about scheduled reports, see Schedule a Report.

When scheduling a new report for Activity Search, any current filters selected apply.



Use Search and Advanced Search

Describes Use Search and Advanced Search in Cisco Secure Access. In addition to using the filters to narrow the activity results in the Activity Search report, the Search and Advanced Search features provide further filtering of event details.

In addition to using the filters to narrow the activity results in the Activity Search report, the Search and Advanced Search features provide further filtering of event details. For example, you can search for events with specific domains but exclude sub-domains you are not interested in.

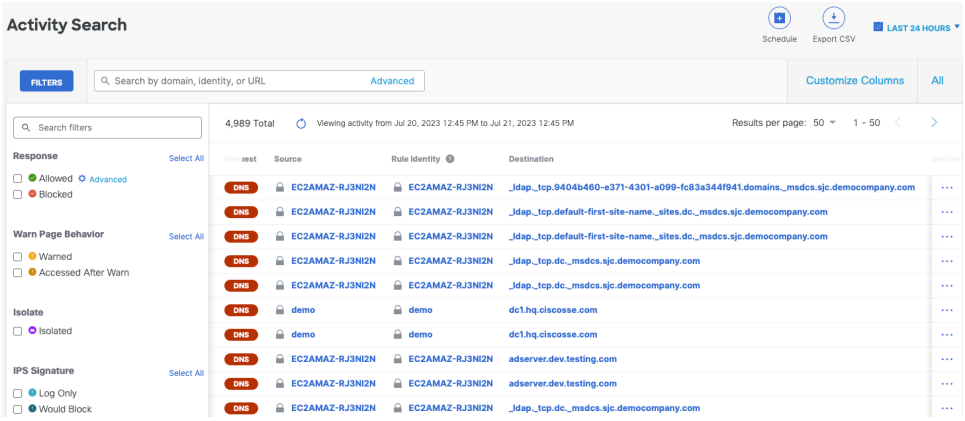
Prerequisites

A minimum user role of Read-only. For more information, see Manage Accounts.

Search

Describes Search in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

Search the report for domains, identities, or URLs. To search and filter the report by more options, such as threat type or file name, use Advanced Search.



Wildcards

Describes Wildcards in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

Wildcards, such as `'*'`, are special symbols that allow you to perform flexible searches when you are unsure of the exact spelling or full string of a specific term. By using these characters, you can broaden your search results to include multiple variations of a term simultaneously.

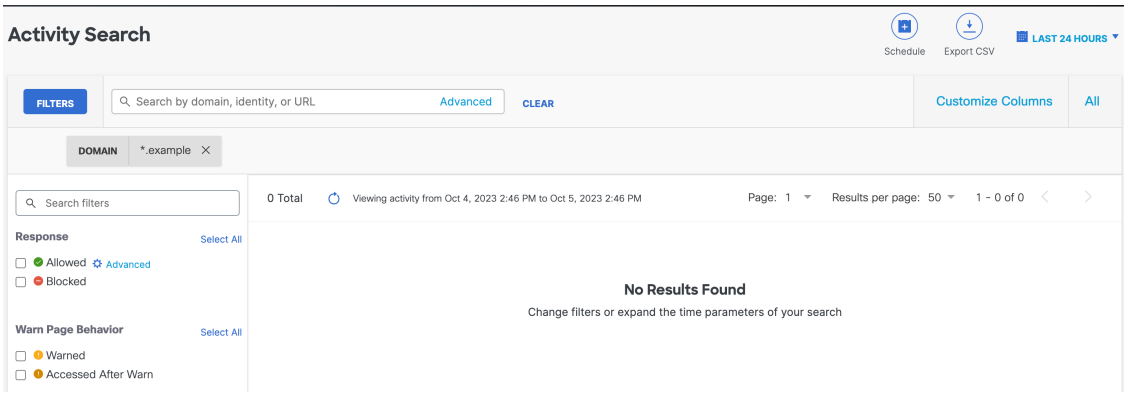
Wildcards available for some fields (Domains, URLs, and File names) allow you to search for all variations within that field. For example, using `*.gif` in File Name will search for all files that are `.gifs`.

Domains

Describes Domains in Cisco Secure Access. Domains can be searched in the search bar or advanced search with the wildcard * to include or exclude subdomains.

Domains can be searched in the search bar or advanced search with the wildcard * to include or exclude subdomains. For example, `example.com` will search the top-level parent domain of Example, `*.example.com` will search for only the subdomains of Example, and `*example.com` will search for both the parent and subdomains of Example.

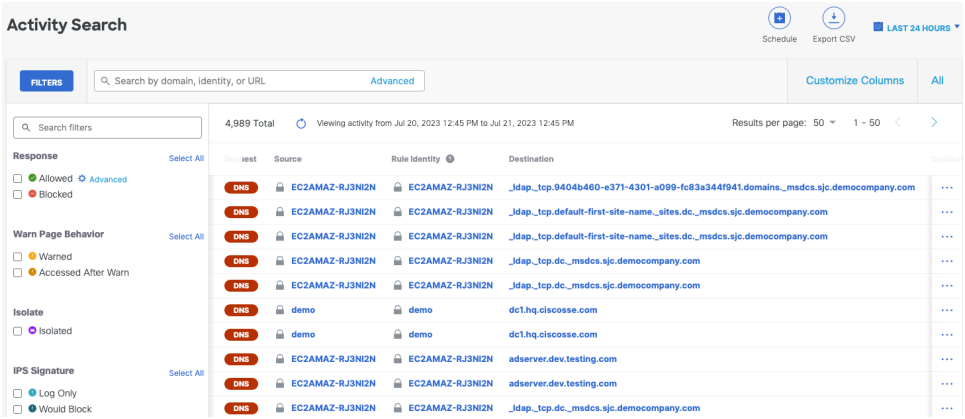
You can use wildcards to search by top-level domain. For example, `*.example` will search for all top-level domains that end in .example.



URLs

Describes URLs in Cisco Secure Access. The wildcard * can be used in any part of the URL path to search for URLs containing certain terms.

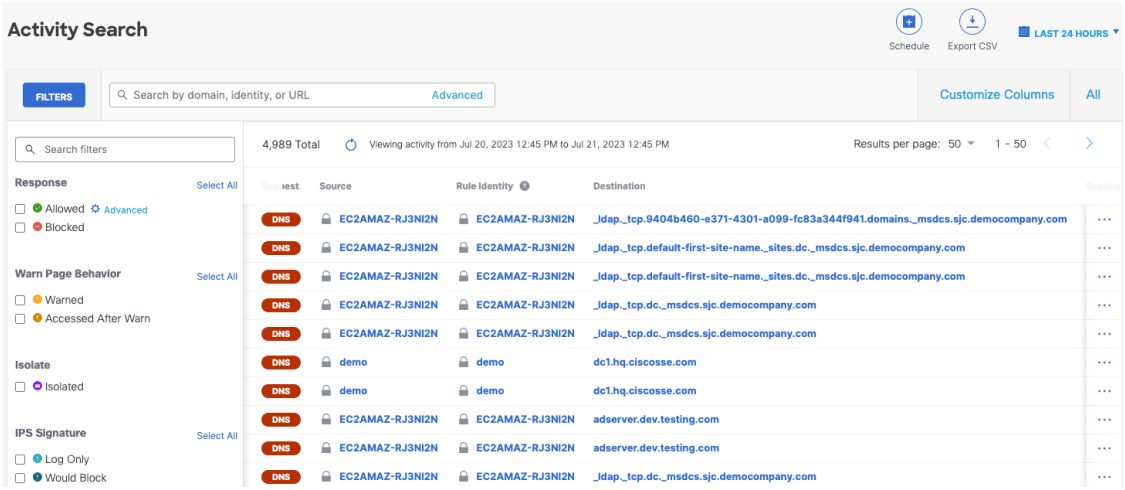
The wildcard * can be used in any part of the URL path to search for URLs containing certain terms. For example, `example*` will search for URLs containing "example".



File Names

Describes File Names in Cisco Secure Access. File names can use the wildcard * to search for file types, in Advanced Search only.

File names can use the wildcard * to search for file types, in Advanced Search only. For example, `*.gif` will search for all files that are .gifs.



Advanced Search

Provides instructions for completing the Advanced Search workflow in Cisco Secure Access. In the search bar, click Advanced to open the Advanced Search window.

Procedure

1. In the search bar, click **Advanced** to open the Advanced Search window.
2. Add search parameters and click **Apply**.

Search Parameter	Description
Identity	Include or exclude identity sources in search results. Secure Access opens a menu listing sources as soon as you begin typing.
Domain	Include or exclude one or more domains in search results. Wildcards are supported. When you add a domain, a new field appears so that you can add or exclude another domain.
SHA256	Search by the hash function.

Search Parameter	Description
URL	Include or exclude specific URLs in search results. Wildcards are supported.
IP Address	Include or exclude events associated with specific IPv4 or IPv6 addresses on your network (either internal or public egress IP address). Supports both compressed and long-form IPv6 address formats. This does not provide the capability to search for destination IP addresses.
IP Address Port	Search by a firewall port number, port range (e.g. 81-222), or port group (e.g. 81,8080,222).
Subnet	Search for events based on IPv4 or IPv6 subnets using CIDR notation. Supports including or excluding multiple subnets.
Threat	Search by threats.
Threat Type	Search by threat type. For more information, see Threat Category Descriptions .
AI Supply Chain Category	Search by the categories Prohibited Suppliers, Code Execution, or Copyleft License. For more information, see Customize the Activity Search Report.
AI Model Name	Search by AI model name. Wildcards are supported.
Block Reason	Include or exclude reasons for a blocked request. Wildcards are supported.
Transaction ID	Include or exclude transaction IDs. Wildcards are supported.
Public Application	Search by any public application.
Application Group	Search by any application group available in the drop-down.
File Name	Search by the name of a file. Wildcards are supported.
IPS Signature List Names	Search by default and custom IPS Signature List Names. For more information, see Manage IPS .
IPS Signatures	Search by up to twenty IPS signatures. For more information, see Manage IPS Profiles .
OS Type	Search by operating system from which the request originated.
Location	Search by the location from which the request originated.
Egress IP Type	Search by the egress IPv4 or IPv6 addresses: shared or reserved. Supports both compressed and long-form IPv6 address formats.
Egress Data Center	Search by the egress data center location from which activity originated.

Inline Column Filtering

Describes Inline Column Filtering in Cisco Secure Access. You can now quickly filter results directly from columns in the Activity Search dashboard.

You can now quickly filter results directly from columns in the Activity Search dashboard. You can use inline filtering on the following columns by hovering over the column header to access the **Search** or **Exclude** option:

- Rule Name
- Application
- Protocol

- Port
- Destination Country
- Browser OS
- Location
- Zero Trust Profile

To use this feature, hover over the header of one of the supported column. You will see pop-up options to **Search** or **Exclude** results based on the value in that column. This enhancement makes it easier to focus on relevant data directly from the report table, without opening Advanced Search.

Security Activity Report

Describes Security Activity Report in Cisco Secure Access. The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged—but not necessarily blocked—by Secure Access security researchers as a threat.

The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged—but not necessarily blocked—by Secure Access security researchers as a threat. Activities captured by this report include attempts to access sites hosting malware or phishing sites, botnet activity on infected machines on your local network, and attempts to download malicious files.

View Activity and Details by Filters

Describes View Activity and Details by Filters in Cisco Secure Access. The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns.

The Security Activity report gives you the ability to monitor and discover threats to your organization by displaying traffic patterns. You can filter these results by event type, category, time period, and type of request.

The Security Activity report shows security activity over time and matching events in a table. Use Search Security Activity, Event type, Response, and Filters above the chart to refine the results.

> **Note**
>
> Secure Access reports are time-dependent. Secure Access time is UTC by default but can be changed to a different timezone on a per-user basis. Navigate to **Admin** > **Accounts** and update your account's time setting.

Procedure

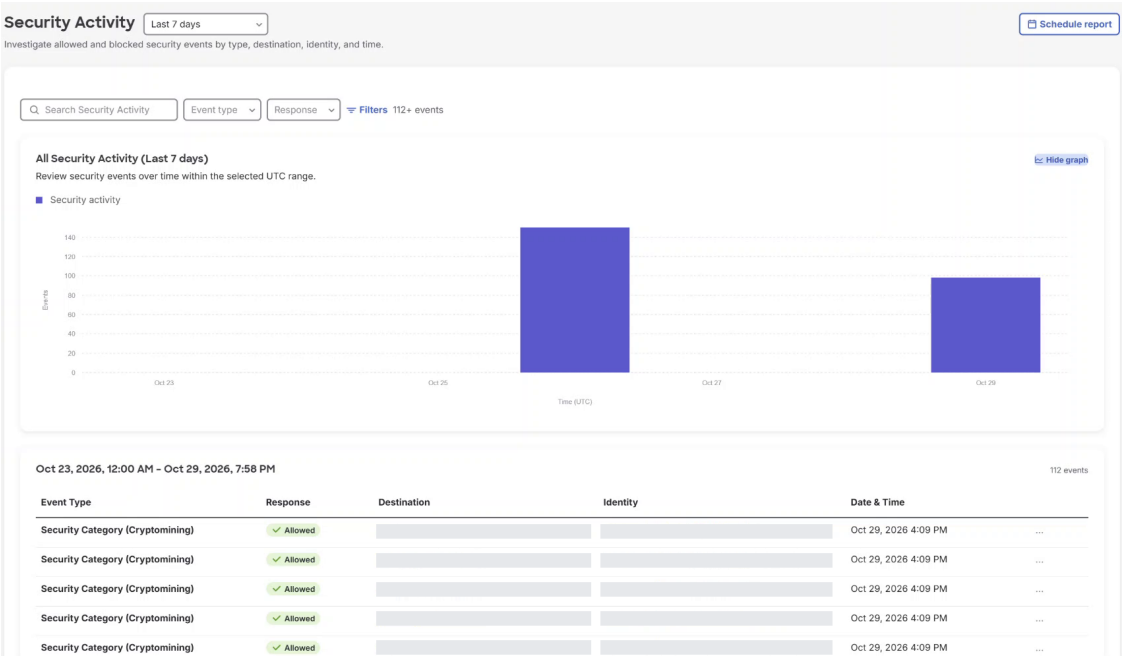
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

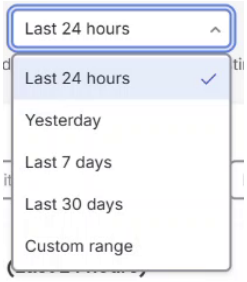
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Security Activity** .

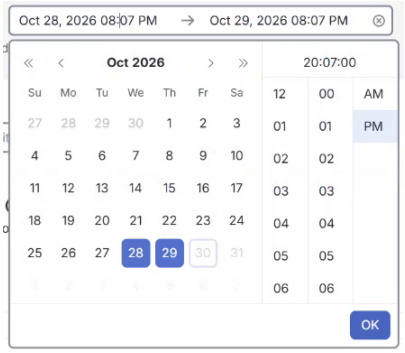


2. Use the time-range drop-down beside Security Activity to choose a time period of events to view. You can generate a report to document activities for a specific time period. You can select from the predefined ranges for the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last 30 days.



To choose a custom time period:

a) Click **Custom range**.



b) Use the date-time fields beside the report title to set the start and end dates and times.

The system allows you to choose a maximum of 31 days time period from the last 90 days.

c) Click **OK** in the date-time picker to confirm your selection.

3. Choose which security event types or categories you want to view in the report. By default, all events and categories are selected to display activity for all event types.

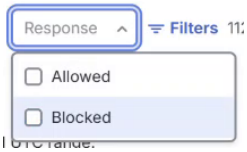
- **Antivirus Disposition is Malicious**–Lists events that have been filtered through a virus scan.

- **Cisco AMP Disposition is Malicious**–Lists events that have been filtered through Cisco Advanced Malware Protection (AMP).
- **Security Category**–Lists events allowed or blocked against selected security categories: Command and Control, Cryptomining, Malware, Phishing, and Other Categories (Contains Dynamic DNS, Newly Seen Domains, and Potentially Harmful).



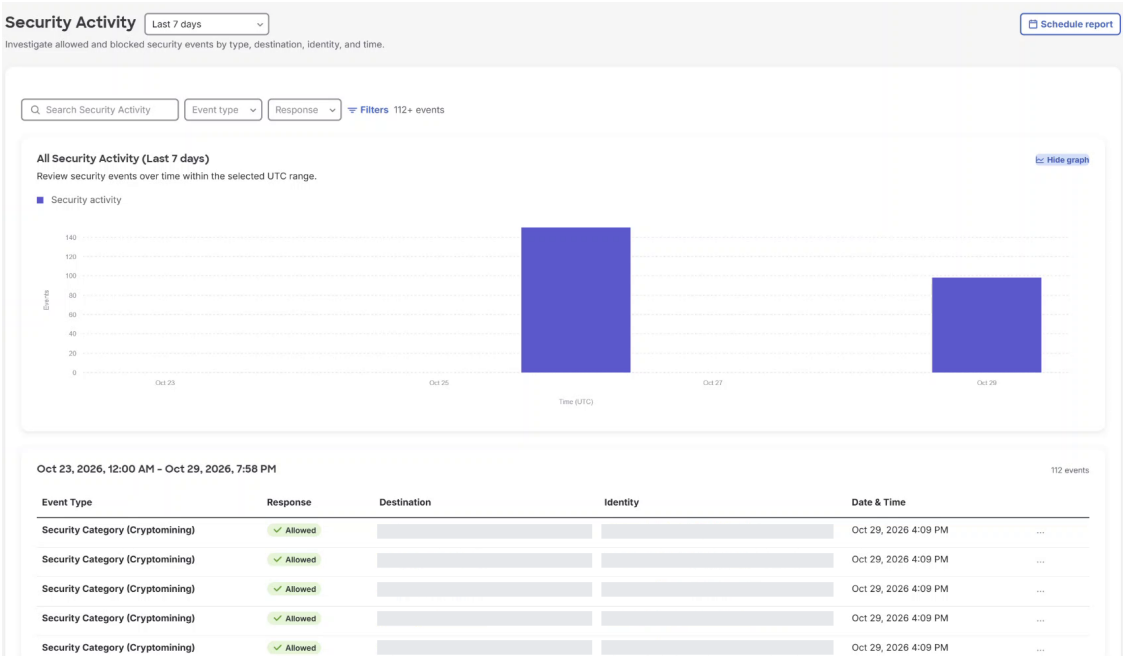
4. For **Response,** select **Allowed**, **Blocked**, or both.

> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.



What to do next

The chart and event table update to reflect the selected time range and filters. The table below the chart lists Event Type, Response, Destination, Identity, and Date & Time for the matching events.



Hover over a bar to view the security activity count for that hour or day. Click the bar to open the **Events** page for the selected time period and applicable report filters.

View Activity and Details by Event Type or Security Category

Describes View Activity and Details by Event Type or Security Category in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To compare activity for individual event types or security categories, click **Filters**. Under Display, use **Group by event type** and **Group security categories**, then click **Apply**.

Procedure

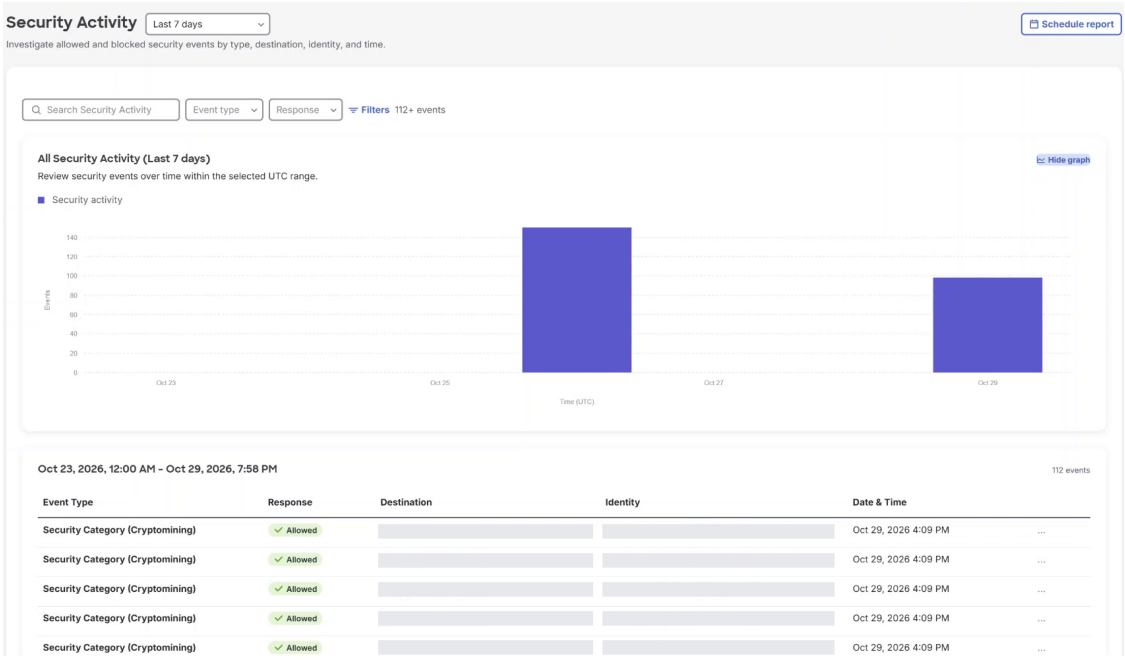
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

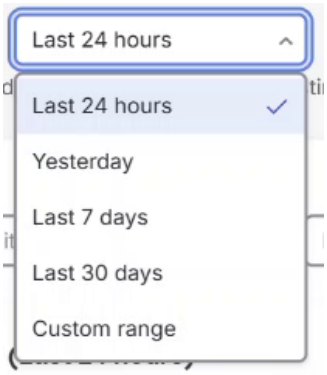
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Security Activity**.

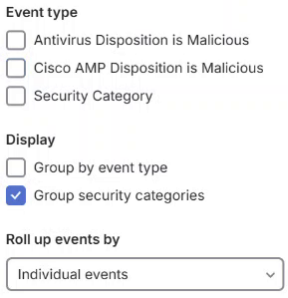


2. Choose the time range beside Security Activity: Last 24 hours, Yesterday, Last 7 days, Last 30 days, or Custom range.



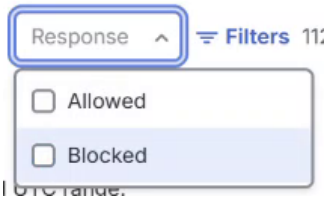
3. For Event type, select **Filters >** > **Display** > **Group by event type** and **Group security categories** as needed, then click **Apply**.

   In



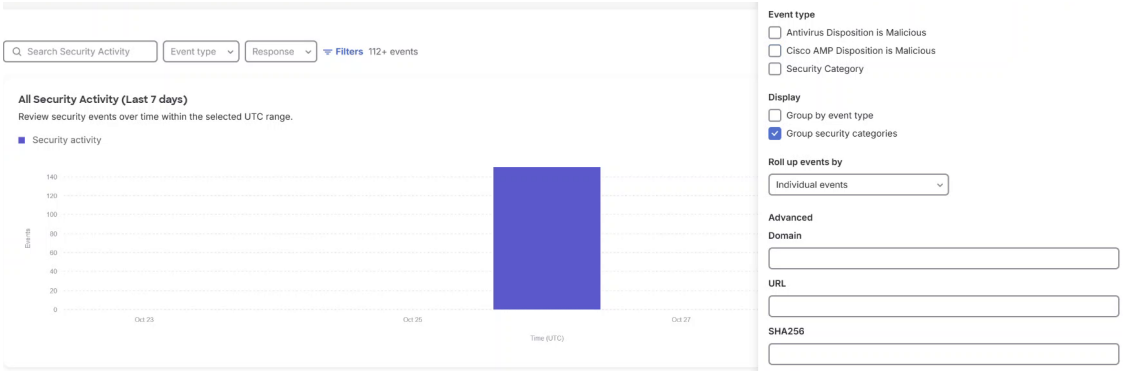
4. For **Response,** select **Allowed**, **Blocked**, or both.

> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.

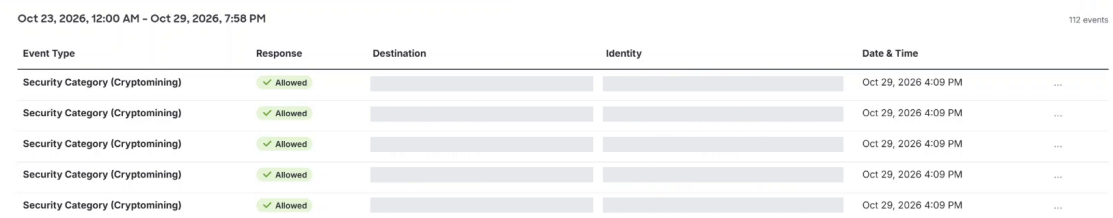


What to do next

The activity graph updates to show each selected event type so you can compare activities for each type of security risk. You can click the event type on the graph or in the filter to view or hide the events in the graph.



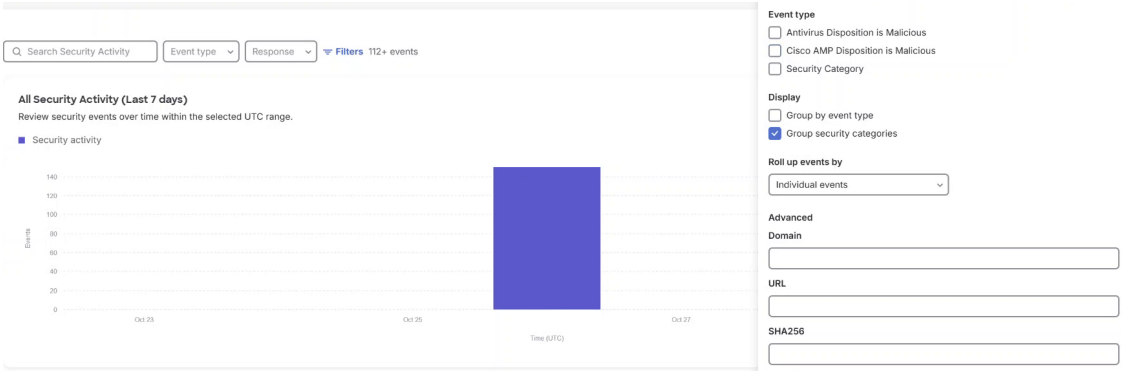
Use **Group by event type** to compare the selected event types. Use the legend to show or hide a plotted type. To change the report selection, use **Event type** in **Filters** and click **Apply**.



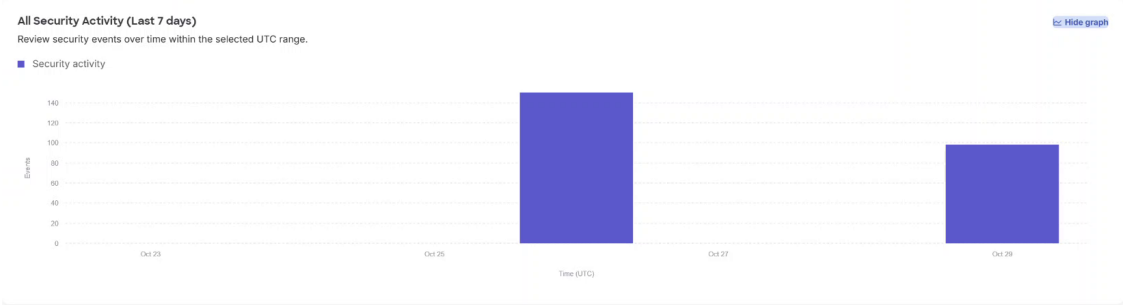
Group Security Categories

Describes Group Security Categories in Cisco Secure Access. When Group Security Categories is unchecked, the selected security categories are shown individually on the Activity graph.

Click **Filters** and uncheck **Group security categories** under **Display** to display the selected security categories individually in the activity chart, so that you can compare activity and spikes by category. Click **Apply** to update the report. Use the chart legend to show or hide a plotted category.



Hover over the chart to inspect the security activity for the selected time and categories. Click a bar to open the **Events** page for that time period and applicable report filters.



View an Event's Details

Describes View an Event's Details in Cisco Secure Access. In the Security Activity report, you can view the details of a security event, including date and time, destination, identity, and the event's result (Blocked or Allowed).

In the Security Activity report, you can view the details of a security event, including date and time, destination, identity, and the event's result (Blocked or Allowed).

Procedure

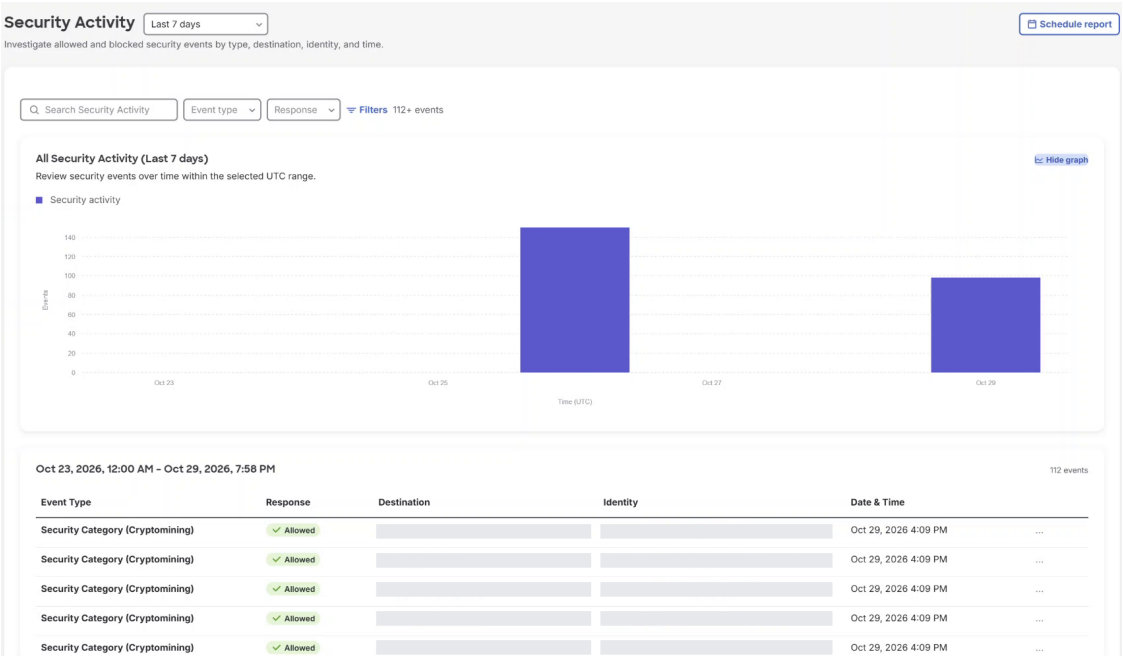
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

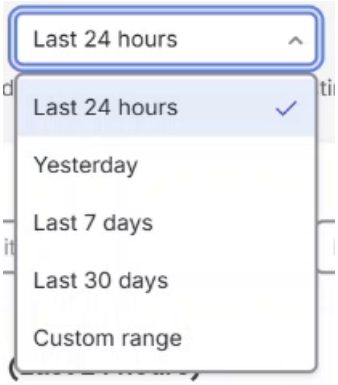
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Security Activity**.

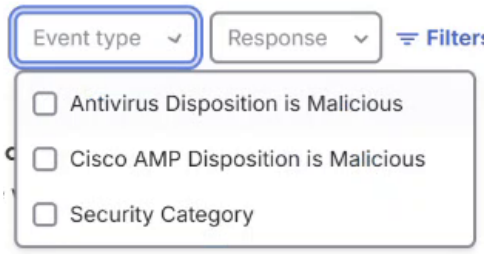


2. Choose the time range beside Security Activity: Last 24 hours, Yesterday, Last 7 days, Last 30 days, or Custom range.



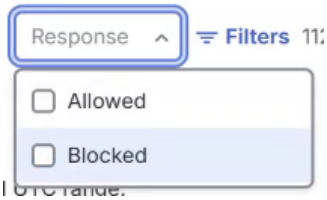
3. Use **Event type** above the chart to select the event types to include.

   For security categories or additional options, click **Filters**, make your selections, and click **Apply**.

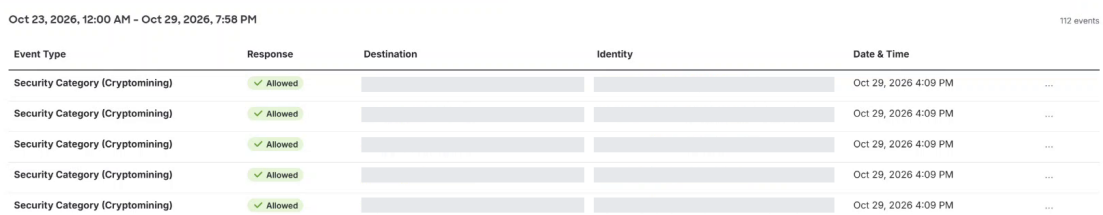


4. For **Response** select **Allowed**, **Blocked**, or both.

> **Note**
>
> If you select **Antivirus Disposition is Malicious** or **Cisco AMP Disposition is Malicious** as the Event Type, you cannot select **Response** > **Allowed**. Secure Access cannot allow viruses to pass through the system. These will always be blocked.



The events are displayed in a table below the activity chart.



5. Click an event to view its details.

   Review Event Type, Response, Destination, Identity, and Date & Time in each row. Use the destination or identity links to open the corresponding Destination Details or Identity Details.

> **Note**
>
> The available event details vary by event type.

Search for Security Activity

Describes Search for Security Activity in Cisco Secure Access. To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

To view security activities for a specific source, use the search feature to filter the Activity chart and event details by source.

Prerequisites

Describes Prerequisites in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

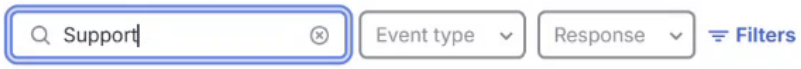
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Security Activity**.
2. Enter the source name in **Search Security Activity** and press **Enter**.

   You can filter by one source at a time.



Advanced Search

Provides instructions for completing the Advanced Search workflow in Cisco Secure Access. To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

To search security activities by more specific fields other than the source, such as domain, URL, or threat type, use the Advanced Search feature.

Procedure

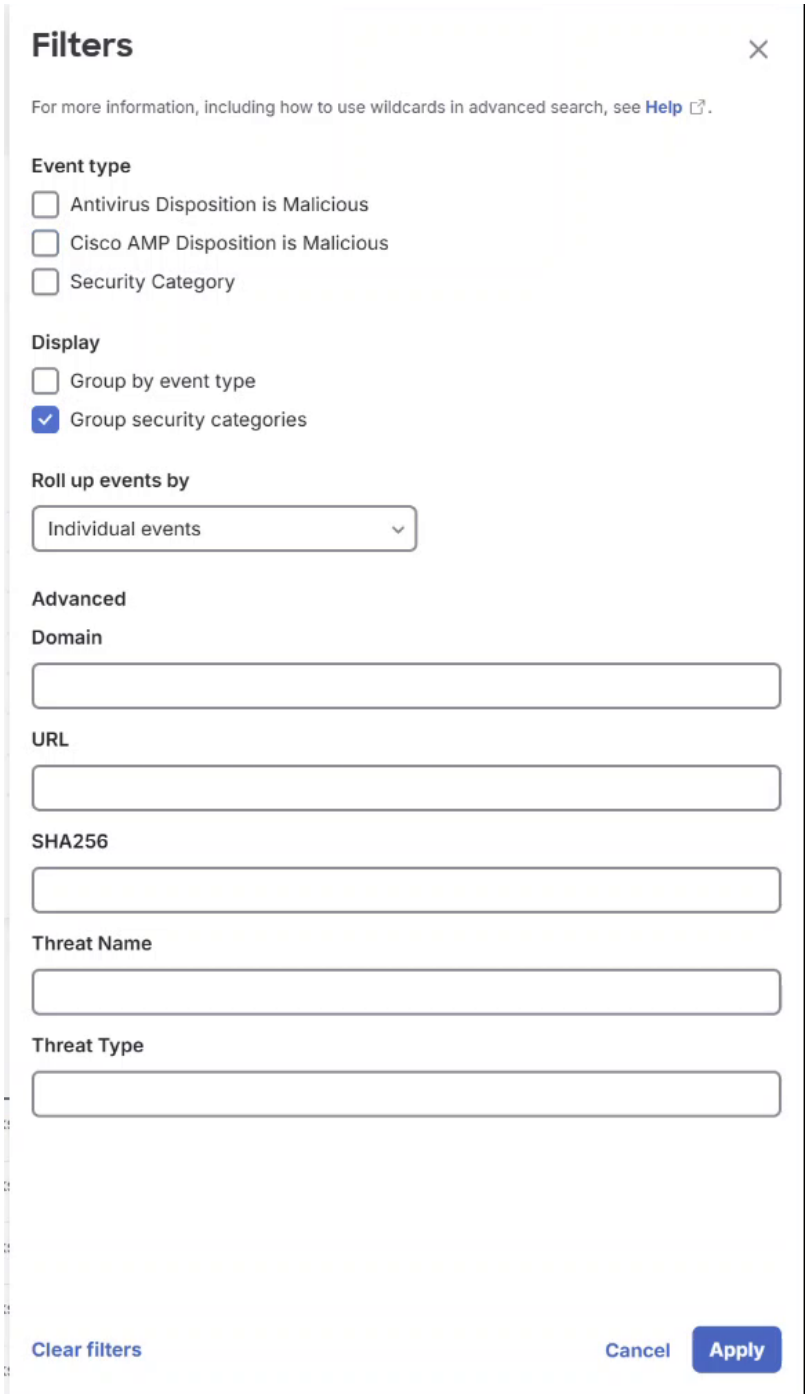
1. Click **Filters** above the chart.



   In the right-side panel, find the Advanced fields.

2. Enter the relevant Domain, URL, SHA256, Threat Name, or Threat Type criteria, and click **Apply**.

   Use **Search Security Activity** above the chart for the source or identity search. To reset the panel, click **Clear filters**; to close it without applying changes, click **Cancel**.



Activity Volume Report

Describes Activity Volume Report in Cisco Secure Access. The Activity Volume Report provides an overall summary of traffic by security categories and policies affected by content categories and Destination Lists.

The Activity Volume Report provides an overall summary of traffic by security categories and policies affected by content categories and Destination Lists. You can view traffic allowed and blocked across these fields as well as the percentage of this traffic for each field and determine which activities may be a potential risk in the organization.

View Requests by Volume of Activity

Provides instructions for completing the View Requests by Volume of Activity workflow in Cisco Secure Access. Navigate to Monitor Reports Activity Volume .You are presented with a chart that depicts categorized requests over time.

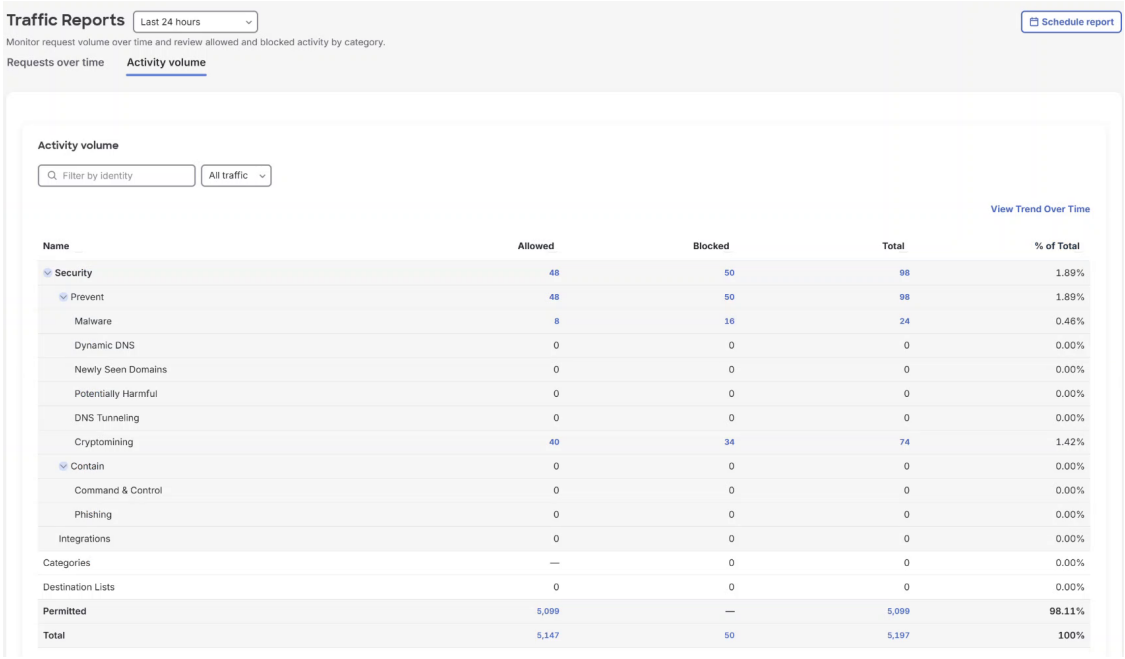
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

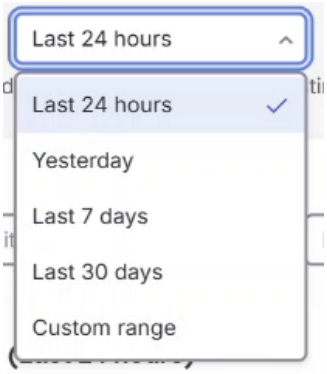
Procedure

1. Navigate to **Monitor** > **Reports** > **Traffic Reports**, then select **Activity volume**.

   The table displays categorized requests for the selected time range.

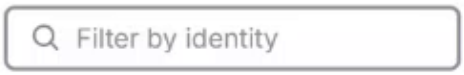


2. Choose a time range from the drop-down beside Traffic Reports. You can select Last 24 hours, Yesterday, Last 7 days, Last 30 days, or a custom range within the last 90 days.



3. Use Filter by identity to find an identity.

   Choose All traffic, DNS, or Web beside the search field.



The Activity Volume Report consists of three main fields of activity (Security, Categories, and Destination Lists), the total Permitted requests, and the Total requests of all traffic. Each field displays the number of requests Allowed, Blocked, the Total number of requests, and the Percentage of all requests that that field represents.

> **Note**
>
> Allowed Categories do not display any results.

Name	Allowed	Blocked	Total	% of Total
Security	48	50	98	1.89%
Prevent	48	50	98	1.89%
Malware	8	16	24	0.46%
Dynamic DNS	0	0	0	0.00%
Newly Seen Domains	0	0	0	0.00%
Potentially Harmful	0	0	0	0.00%
DNS Tunneling	0	0	0	0.00%
Cryptomining	40	34	74	1.42%
Contain	0	0	0	0.00%
Command & Control	0	0	0	0.00%
Phishing	0	0	0	0.00%
Integrations	0	0	0	0.00%
Categories	—	0	0	0.00%
Destination Lists	0	0	0	0.00%
Permitted	5,099	—	5,099	**98.11%**
Total	5,147	50	5,197	**100%**

View Activity Volume by Threat Categories

Describes View Activity Volume by Threat Categories in Cisco Secure Access. The Security field contains two sub-fields of traffic data relating to potential security risks: Prevent and Contain.

The Security field contains two sub-fields of traffic data relating to potential security risks: Prevent and Contain. For more information about threat categories, see Threat Category Descriptions. Integrations are not applicable to Secure Access.

Name	Allowed	Blocked	Total	% of Total
Security	48	50	98	1.89%
Prevent	48	50	98	1.89%

Prevent

Describes Prevent in Cisco Secure Access. The Prevent security section lists the threat categories utilized to prevent threats and risks in your environment.

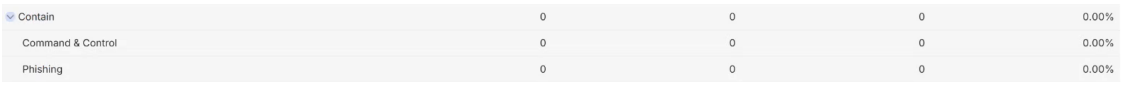
Expand **Security** and **Prevent** to review the threat categories used to prevent risks in your environment. The table lists Allowed, Blocked, Total, and % of Total for each category. Use these values to identify high-volume categories and determine whether policies need to be updated.

Prevent	48	50	98	1.89%
Malware	8	16	24	0.46%
Dynamic DNS	0	0	0	0.00%
Newly Seen Domains	0	0	0	0.00%
Potentially Harmful	0	0	0	0.00%
DNS Tunneling	0	0	0	0.00%
Cryptomining	40	34	74	1.42%

Contain

Describes Contain in Cisco Secure Access. The Contain section lists two threat categories in which threats are contained and prevented from spreading in your environment.

Expand **Contain** under **Security** to review **Command & Control** and **Phishing**. These categories help identify threats that are contained to prevent them from spreading. The table lists Allowed, Blocked, Total, and % of Total for each category.



Contain	0	0	0	0.00%
Command & Control	0	0	0	0.00%
Phishing	0	0	0	0.00%

View Activity Volume by Policy Traffic

Describes View Activity Volume by Policy Traffic in Cisco Secure Access. The Categories and Destination Lists fields provide an insight into traffic where requests were allowed or blocked due to policies configured with content categories and destination lists.

The **Categories** and **Destination Lists** rows show traffic allowed or blocked by policies configured with content categories and destination lists. The table lists Allowed, Blocked, Total, and % of Total for each row. Use these values to identify the policies receiving the most traffic.



Categories	—	0	0	0.00%
Destination Lists	0	0	0	0.00%

View Trends

Describes View Trends in Cisco Secure Access. Click the View Trend Over Time button to be redirected to the Total Requests Report for an enhanced visualization of traffic trends over a given period of time.

Click **View Trend Over Time** to switch to the **Requests over time** tab in Traffic Reports and view traffic trends for the selected period.



72 Admin Audit Log Report

Topics:

- Admin Audit Log Report

Provides an overview of Admin Audit Log Report in Cisco Secure Access, including Admin Audit Log Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Admin Audit Log Report

Describes Admin Audit Log Report in Cisco Secure Access. The Admin Audit log records changes that your administrative team has made to your organization's Secure Access settings.

The Admin Audit log records changes that your administrative team has made to your organization's Secure Access settings. Logs appear when change events occur, such as adding a user or modifying a rule. For more information about the details of the logs, see Log Formats and Versioning.

Generate Admin Audit Log Report

Provides instructions for completing the Generate Admin Audit Log Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

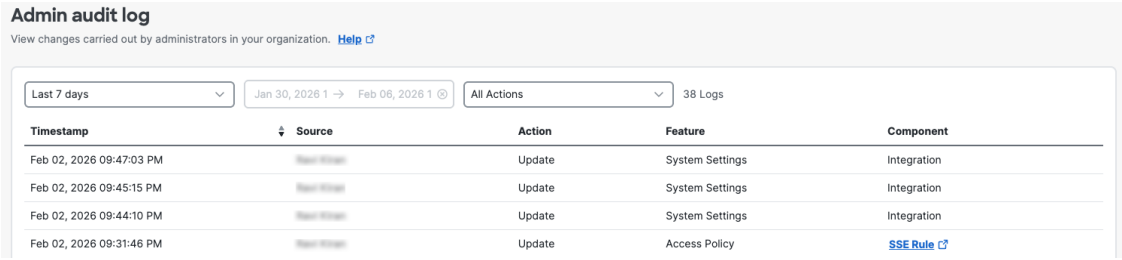
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

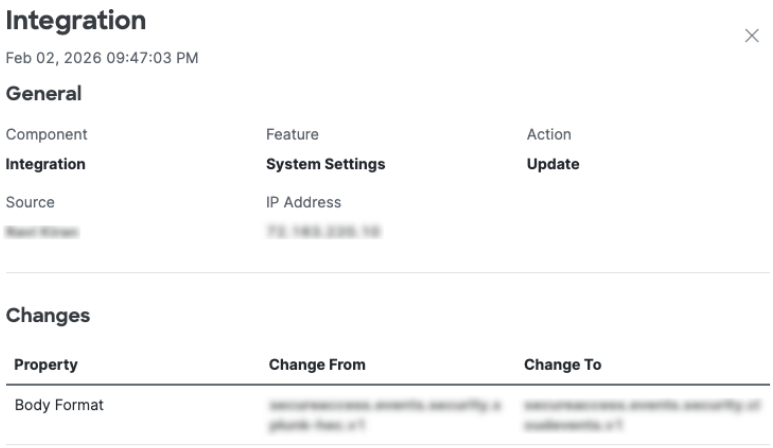
Procedure

1. Navigate to **Monitor** > **Management** > **Admin Audit Log**.

> **Note**
>
> If you see **PCAP_CiscoCX Team** entries in your audit logs, these indicate that a packet capture was performed by Cisco Support as part of a support case. This is not a customer-initiated action, and you will be informed when such activities occur. These entries are present in audit logs for transparency. If you have questions about these entries, please contact Cisco Support.



2. Click an **Action** to view further details of an event.



Export Admin Audit Log Report to an S3 Bucket

Describes Export Admin Audit Log Report to an S3 Bucket in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Admin Audit log includes:

- Policies, Identities, or Block Pages that were Created
- Policies, Identities, Block Pages, or User and Entity Behavior Analytics (UEBA) Configurations that were Updated
- Policies, Identities, or Block Pages that were Deleted

Procedure

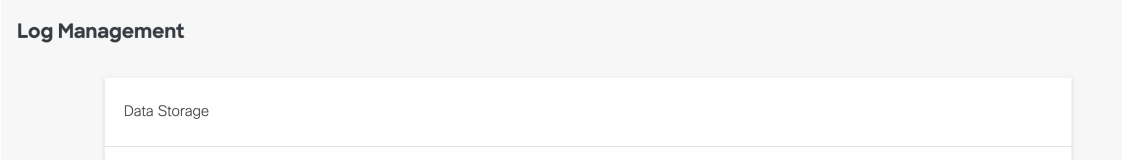
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

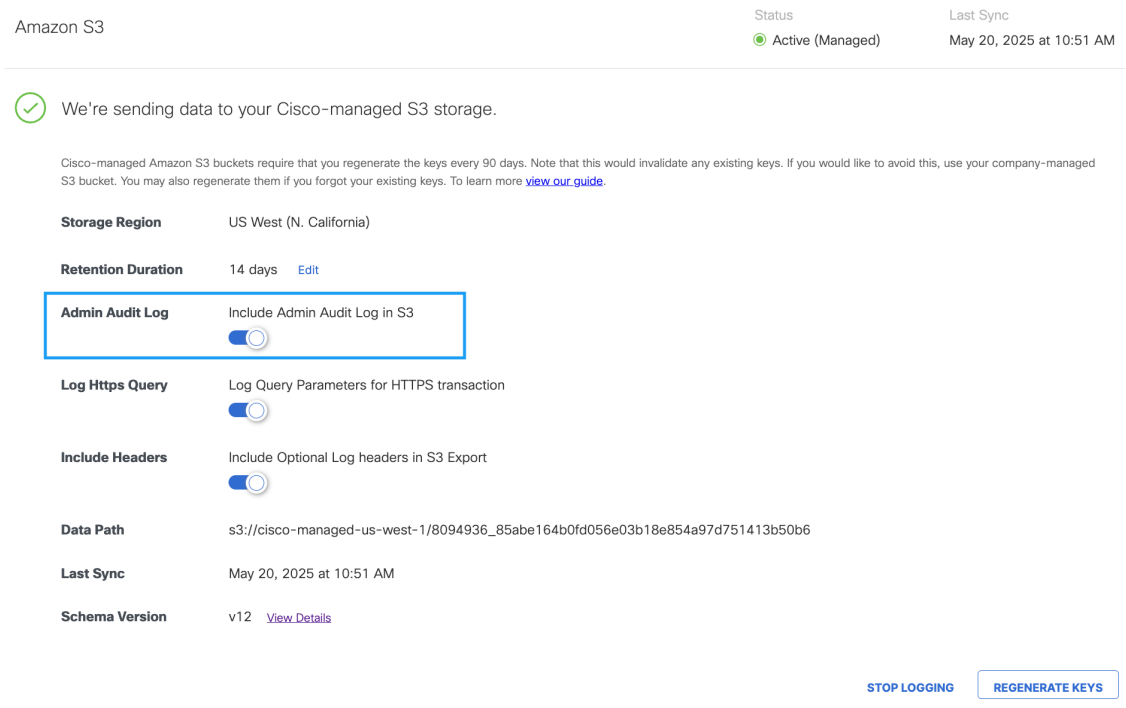
- Logging is enabled. See Manage Logging.
- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Log Management**.



2. For your activated S3 bucket, navigate to **Admin Audit Log** . Enable the exportation of Admin Audit Log reports to your S3 bucket.



Secure Access saves your Admin Audit logs to the auditlogs folder.

73 AI Related Reports

Topics:

- AI Supply Chain Report
- AI Semantic Inspection Report

Provides an overview of AI Related Reports in Cisco Secure Access, including AI Supply Chain Report and AI Semantic Inspection Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

AI Supply Chain Report

Provides instructions for completing the AI Supply Chain Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the AI Supply Chain report to monitor and control end user access to AI model files that can pose AI supply chain security and compliance risks.

Secure Access can identify and block end user attempts to download AI model files developed or authored by prohibited suppliers, released under a copyleft license, or capable of executing arbitrary code.

For more information, see Foundation AI: Robust Intelligence for Cybersecurity and Cisco AI Supply Chain Risk Management.

Before you begin

To ensure information is captured in the AI supply chain report, you must configure the following:

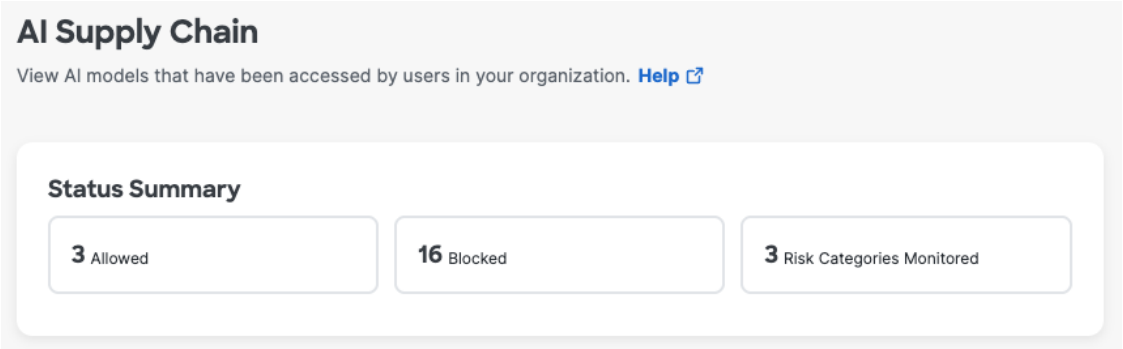
- A security profile for internet access with both **Decryption** and **AI Supply Chain Blocking** enabled. For more information, see Security Profiles for Internet Access.
- At least one internet access rule with a security profile for internet access with **AI Supply Chain Blocking** enabled. For more information, see Security Profile.

Procedure

1. Navigate to **Monitor** > **AI Supply Chain**.

   The AI Supply Chain dashboard shows information about AI model risk monitoring and model file download attempts by your end users.

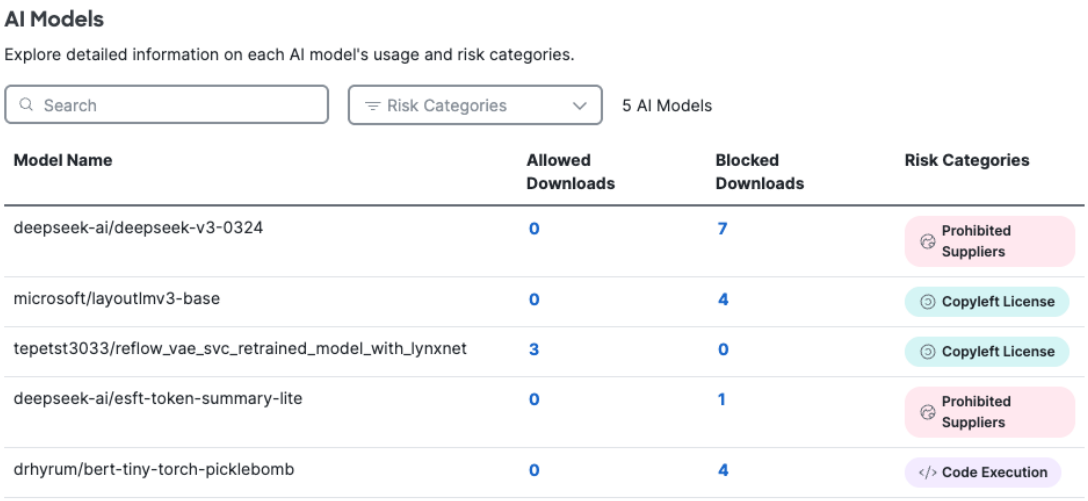
   Status Summary shows the total number of AI model downloads allowed and blocked in your organization and the number of risk categories that you are monitoring.



2. Search the AI Models table by model name or filter by risk category.

   The AI Models table shows:

   - **Model Name**–The unique identifier of an AI model.
   - **Number of Allowed and Blocked Downloads**–Click the numbers in the table to view details in the Activity Search report about allowed or blocked attempts to download files identified as related to this AI model. For more information, see Activity Search Report.
   - **Risk Categories**–Each model name will be associated with one or more of the three risk categories provided by Foundation AI: Prohibited Suppliers, Copyleft License, and Code Execution.



More about Risk Categories Provided by Cisco Foundation AI

- **Prohibited Suppliers**–AI models developed or authored by prohibited suppliers may present risks related to national security, data privacy, and influence operations. Depending on the development and deployment context, models in this category may be subject to regulatory oversight, data access laws, or government influence that raises concerns about embedded backdoors, surveillance capabilities or biased outputs shaped by geopolitical agendas.
- **Copyleft License**–AI models released under copyleft licenses can introduce legal and operational risks due to restrictive licensing terms. Copyleft licenses may require that derivative work, deployment dependent on the model, or indirect use must be released under the same license. This may present risks related to compliance with disclosure requirements of the license, legal exposure due to violation of license terms, and constraints on how the model can be integrated, scaled, or monetized.
- **Code Execution**–AI models capable of executing arbitrary code create security and reliability risks. If a model can generate and execute code dynamically, it may inadvertently or maliciously run harmful operations, access sensitive data, or interact with systems in unintended ways. A model's ability to execute arbitrary code bridges the gap between text generation and real-world impact, making it possible for a model to cause damage ranging from data breaches to system compromise.

AI Semantic Inspection Report

Describes AI Semantic Inspection Report in Cisco Secure Access. As enterprises rapidly adopt AI agents to automate and optimize business operations, many are using the Model Context Protocol (MCP) to enable AI agents to access data and perform reasoning tasks in a standardized way.

As enterprises rapidly adopt AI agents to automate and optimize business operations, many are using the Model Context Protocol (MCP) to enable AI agents to access data and perform reasoning tasks in a standardized way. Because these tools often handle mission-critical enterprise data, ensuring visibility, security assurance, threat protection, and prevention of data breaches is essential. Securing interactions between AI agents (acting as MCP clients) and enterprise systems is a key challenge in deploying agentic AI safely.

Overview

Cisco Secure Access introduces the MCP Semantics Inspection Proxy, designed to analyze MCP protocol messages between AI agents/applications and MCP servers. This proxy identifies and blocks suspicious or policy-violating requests

and responses, mitigating threats such as prompt injection, tool poisoning, reconnaissance, and data exfiltration that exploit MCP server-side vulnerabilities.

The Secure Access AI Semantics Inspection Dashboard provides visibility into detected threats by showing the number of blocked MCP messages and allowing users to drill down into detailed event reports. Threat detection and blocking are enabled by default for all MCP traffic, requiring no additional configuration or installation on client endpoints or MCP servers.

Key Features

- **Semantic Inspection Proxy:** Analyzes MCP traffic flowing through Secure Access, detecting MCP messages for risky actions such as prompt injection, tool poisoning, and data exfiltration, performed by the AI agents.
- **Verdict Assignment:** The semantic inspection proxy works in conjunction with Cisco Foundation AI model to assign each MCP message a verdict of **Block** or **Allow**.
- **Logging and Insights:** MCP messages are logged on each observed MCP server, with actionable insights displayed to users.
- **AI Semantic Inspection dashboard:** The AI Semantic Inspection dashboard on Secure Access provides visibility into detected threats, MCP server endpoint URLs and allows users to drill down into details about the security events.
- **Automatic Protection:** Threat detection and blocking operate automatically on all MCP traffic visible to Secure Access, without client-side dependencies.

Current Scope and Constraints

- This version inspects MCP requests only for agents accessing MCP servers publicly hosted on the internet, such as GitHub, Slack, Atlassian, Langchain, or Playwright.
- Inspection applies to MCP traffic entering Secure Access via Remote Access VPN, SD-WAN, or IPSec/CNHE tunnels.
- There is no dependency on client-side software; any MCP traffic visible to Secure Web Gateway (SWG) is analyzed.

Requirements for AI Semantic Inspection

To enable AI Semantic Inspection for your organization, follow these steps:

- Configure a Security Profile for internet access with **Decryption** and **AI Semantic Inspection** enabled. For detailed guidance, refer to the documentation on Security Profiles for Internet Access.
- Create at least one internet access rule that allows traffic and applies the Security Profile with Decryption enabled. See Security Profile for instructions.
- Ensure MCP traffic inspection is enabled on Remote Access VPN connections and Branch office connections to Secure Access via SD-WAN or IPsec tunnels.

Detection of Specific Threats and Security Risks

Cisco Secure Access intercepts and evaluates MCP messages between MCP clients and servers to identify security risks and threats. These are consolidated into four key categories:

- **Data Exfiltration**: Attempts to extract, export, or transfer sensitive data such as credentials, personally identifiable information (PII), training data, customer data, or internal datasets. This includes risks like data exposure via agent tooling, training data leaks, and intellectual property compromise.
- **Prompt Injection**: Attempts to override instructions, jailbreak the AI model, or manipulate system or developer directives. This category covers direct prompt injection and jailbreak attempts aimed at altering AI behavior.

- **Tool Poisoning**: Attempts to compromise tools, plugins, configurations, or the supply chain by embedding hidden instructions, backdoors, or persistence mechanisms. This includes tool exploitation, supply chain compromise, configuration persistence, and protocol manipulation.
- **Tool Shadowing**: Attempts to register a tool with the same name as a legitimate tool so the agent resolves to the attacker's version, enabling call interception, data theft, or false result injection without detection.

View AI Semantic Inspection Events in Reports

- For more information, see View the AI Semantic Inspection Report.
- For more information, see View AI Semantic Inspection Events in Activity Search Report.

View AI Semantic Inspection Report

Provides instructions for completing the View AI Semantic Inspection Report workflow in Cisco Secure Access. Ensure you have at least a Read-only user role in Secure Access.

The Cisco AI Semantic Inspection Report provides detailed statistics on MCP messages observed by Secure Access within your organization. It detects, evaluates, and logs MCP communications to protect against threats and security risks related to these interactions.

Secure Access continuously monitors MCP traffic to safeguard your organization from potential vulnerabilities and malicious activities.

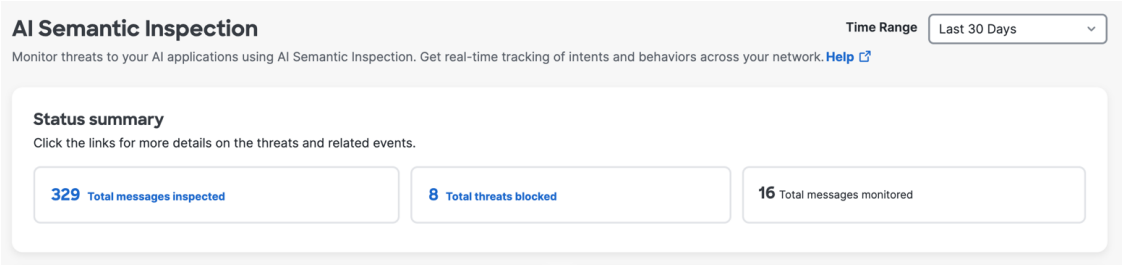
Before you begin

- Ensure you have at least a **Read-only** user role in Secure Access.
- Configure a **Security profile** for internet access with **Decryption** and **AI Semantic Inspection** enabled. For more information, see Security Profiles for Internet Access.
- Create at least one internet access rule with the **Allow** action selected and associate it with a Security profile that has **Decryption** enabled. For more information, see Security Profiles.

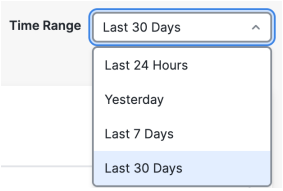
  These prerequisites ensure that Secure Access can properly inspect and report on MCP traffic for your organization.

Procedure

1. Navigate to **Monitor** > **AI Semantic Inspection**.



2. For **Time Range**, choose a time frame to review the MCP messages on the MCP servers. The default time range is the last 24 hours.



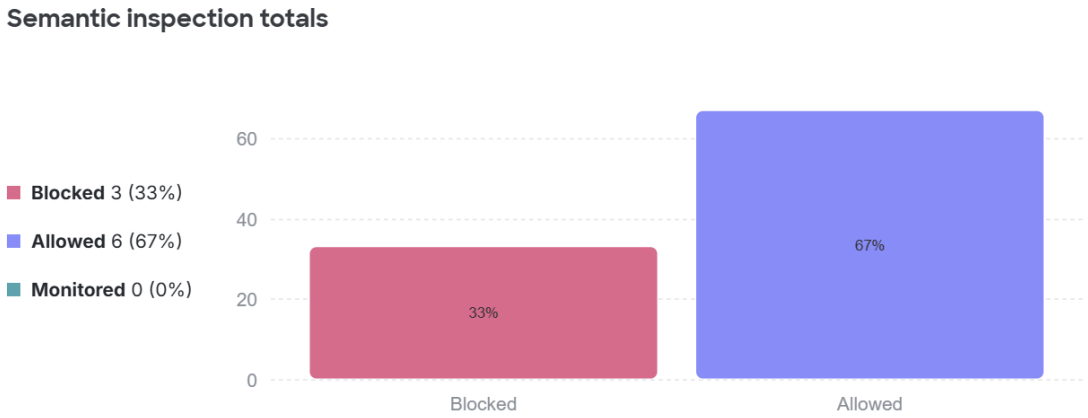
3. Navigate to **Status summary**.

   View the statistics about the MCP messages on the MCP servers observed by Secure Access.

   - **Total messages inspected**–The total number of MCP messages analyzed by Secure Access on the MCP servers.
   - **Total threats blocked**–The total number of MCP messages blocked by Secure Access on the MCP servers.

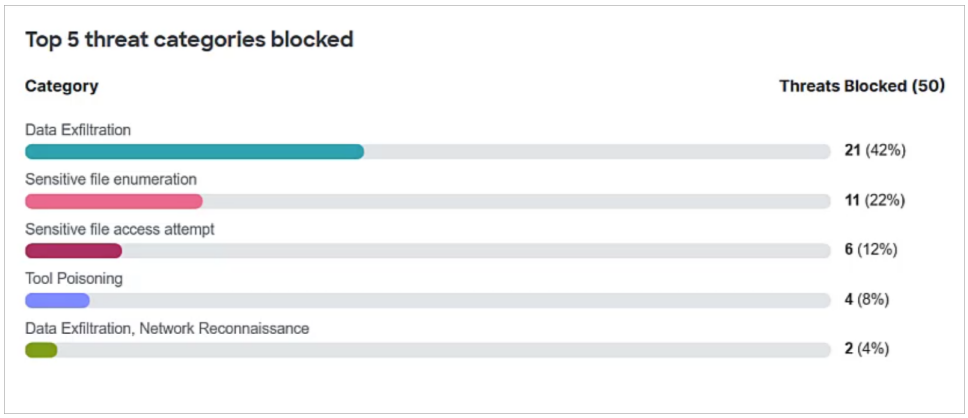
4. Navigate to **Semantic inspection totals**.

   Secure Access displays the number and percentage of **Blocked**, **Allowed**, and **Monitored** MCP messages on the MCP servers for the organization.



5. Navigate to **Top 5 threat categories blocked**.

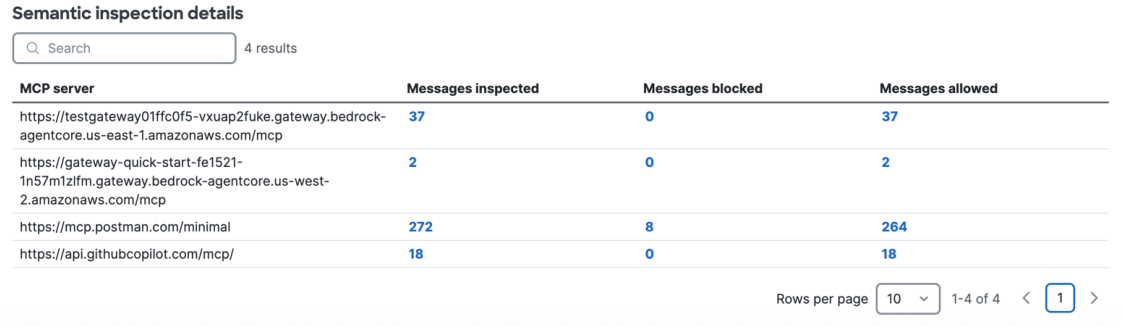
   Secure Access displays the top five threat categories associated with the MCP messages on the MCP servers, the number of threats blocked for each category, and the percentage of threats blocked on the threat category.



6. Navigate to **Semantic inspection details**.

   View the URL of the MCP servers observed by Secure Access. For each MCP server, Secure Access shows the number of MCP messages inspected, blocked, or allowed.

   - **MCP server**–The URL of the MCP server.
   - **Messages inspected**–The total number of MCP messages inspected by Secure Access on the MCP server.
   - **Messages blocked**–The total number of MCP messages blocked by Secure Access on the MCP server.
   - **Messages allowed**–The total number of MCP messages allowed by Secure Access on the MCP server.



7. For an **MCP server**, navigate to a column of MCP messages, and then click the number in the column.

   Secure Access shows the events for the MCP messages in the Activity Search report. For more information, see View AI Semantic Inspection Events in Activity Search Report.

74 App Related Reports

Topics:

- App Discovery Report
- Third-Party Apps Report

Provides an overview of App Related Reports in Cisco Secure Access, including App Discovery Report and Third-Party Apps Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

App Discovery Report

Describes App Discovery Report in Cisco Secure Access. Monitor the cloud apps in use by your organization with the App Discovery report.

Monitor the cloud apps in use by your organization with the App Discovery report. To effectively reduce the risk introduced by apps, monitor app use and look for a reduction over time in the number of DNS requests made by apps with high and very high-risk assessments. You can monitor this with the App Discovery report.

Apps can be blocked through rules when risk levels are unacceptable or when an app category is inappropriate for your organization. For more information, see Control Apps.

App Discovery data is aggregated and processed once a day. It may take up to 24 hours for new data to populate an App Discovery report. Logging of traffic is required for App Discovery to function.

View the App Discovery Report

Describes View the App Discovery Report in Cisco Secure Access. Monitor the cloud apps in use by your organization with the App Discovery report.

Monitor the cloud apps in use by your organization with the App Discovery report. To effectively reduce the risk introduced by apps, monitor app use and look for a reduction over time in the number of DNS requests made by apps with high and very high-risk assessments.

View the App Discovery Report

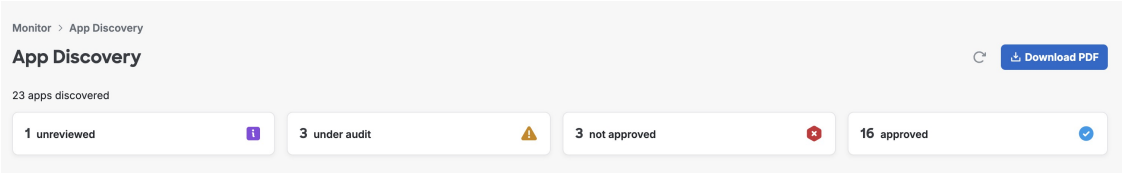
Provides instructions for completing the View the App Discovery Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

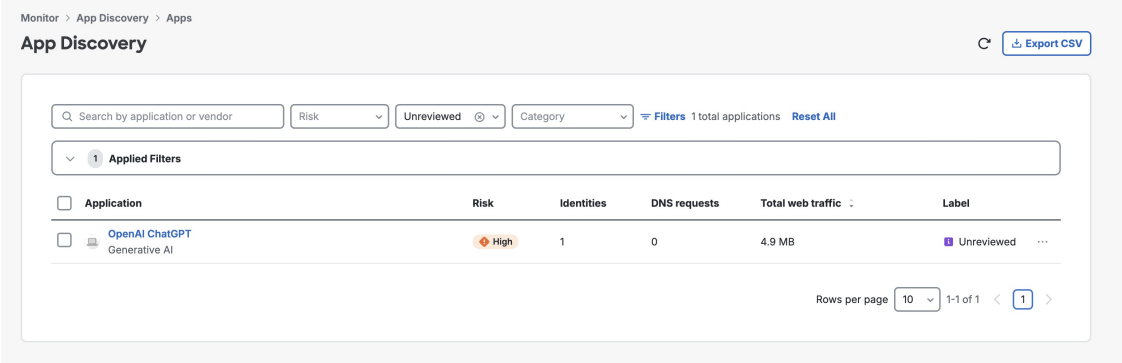
A minimum user role of Read-Only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery**.



2. View the discovered apps in your environment.
   - **Unreviewed**–The app has not yet been assigned any label.
   - **Under Audit**–The app is currently being reviewed.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Approved**–The app may be used in your environment.



Note

Once you relabel an Unreviewed app, you cannot change the app label back to Unreviewed. Use the Under Audit label for apps that still need review.

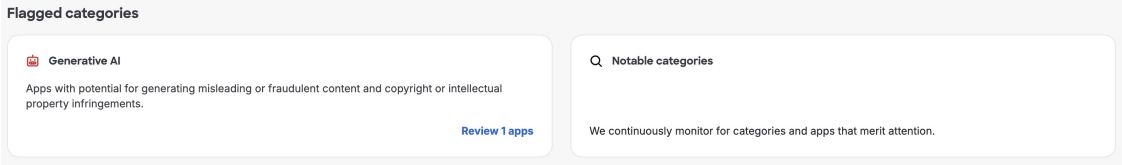
Note

Labels do *not* automatically block apps from use. You must configure a rule to block specific apps or apps with specific labels. For more information, see Control Apps.

3. View the flagged categories.

   Cisco's Cloud Security researchers categorize apps according to function, source, and other factors. The categories of most interest (and most risk) are:

   - **Anonymizers**–Services that provide an anonymous proxy tool that attempts to make activity on the Internet untraceable. Apps in this category can introduce data exfiltration risks.
   - **Cloud Storage**–Applications that offer massively scalable storage capacity that can be used for applications and file storage. Apps in this category can also be used for data exfiltration.
   - **Collaboration**–Applications that may store sensitive data in unreliable services or unsecured environments.
   - **Games**–Online and mobile games. While games are not notable for data exfiltration risks, some can be used as attractive ways to introduce malware.
   - **Generative AI**–Applications that have the potential to generate misleading or fraudulent content and copyright or intellectual property infringements.
   - **Media**–Applications that can contribute to productivity loss and are frequently managed as unwanted bandwidth consumers.
   - **P2P**–Peer to Peer torrents like apps and protocols. These apps can be used for data exfiltration.
   - **Social Networking**–Can be used to transmit sensitive data as well as contribute to productivity loss.

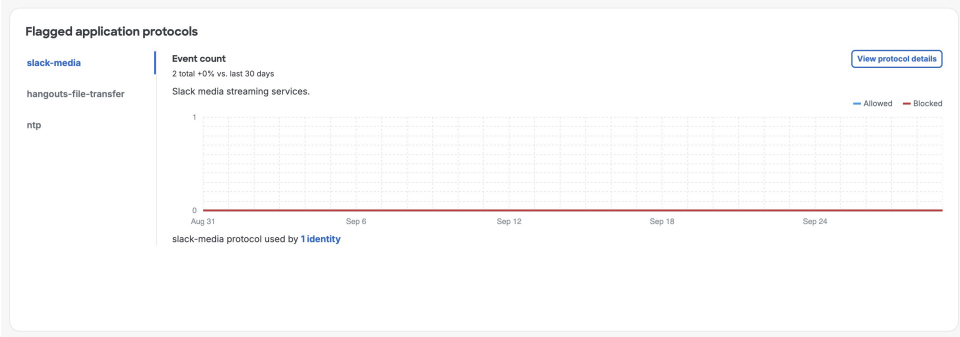


For a complete list of application categories, see Application Categories.

4. View the flagged application protocols.

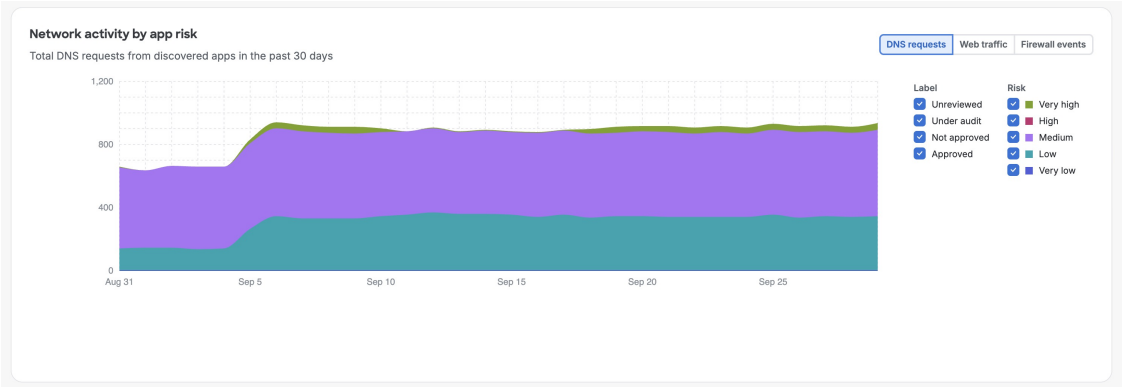
   These protocols are flagged based on the protocol used by the application.

> **Note**
>
> Dismissing a flagged app card hides it from the overview. It does not label or block the app.

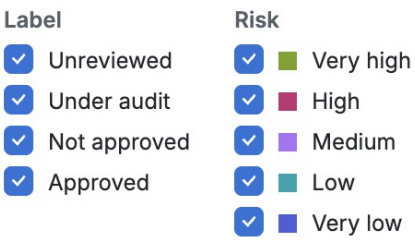


5. View Network activity by app risk.

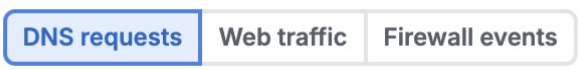
   The graph shows the total number of DNS requests for apps discovered in the past 30 days. Secure Access assigns a risk score to apps based on several factors. The DNS requests made by a high-risk app can be considered more problematic than the same number of requests made by an app with a lower risk score.



   a. Filter the graph by label and risk.



   b. Toggle between DNS requests, Web traffic and Firewall events (bytes in and out) by App Risk for the last 30 days.

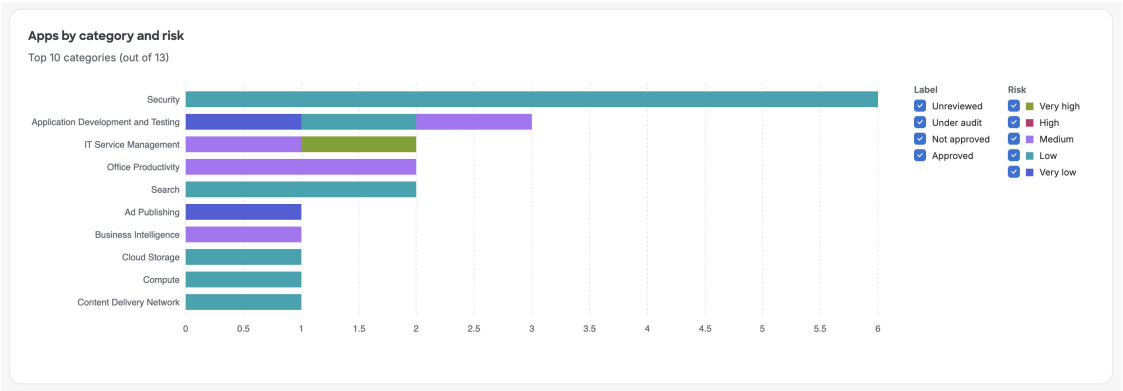


   c. View All Traffic, Outbound Traffic or Inbound Traffic.

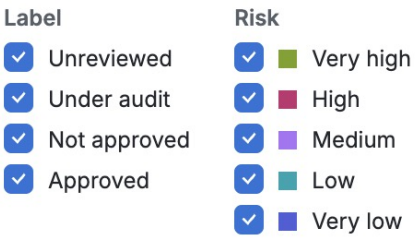


6. View apps by category and risk.

   Click a bar on the chart to view apps in that category in the App Grid.



   a. Filter by label and risk.



View the Highest Risk Apps

Describes View the Highest Risk Apps in Cisco Secure Access. You can view the highest-risk apps in the App Discovery Report by filtering for apps with the highest number of DNS requests.

You can view the highest-risk apps in the App Discovery Report by filtering for apps with the highest number of DNS requests.

The App Discovery report is used to help review apps in your environment. To block risky apps, you must configure application settings within a policy rule to control apps.

Procedure

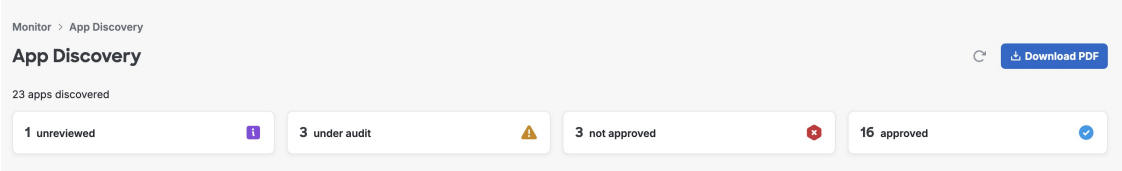
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

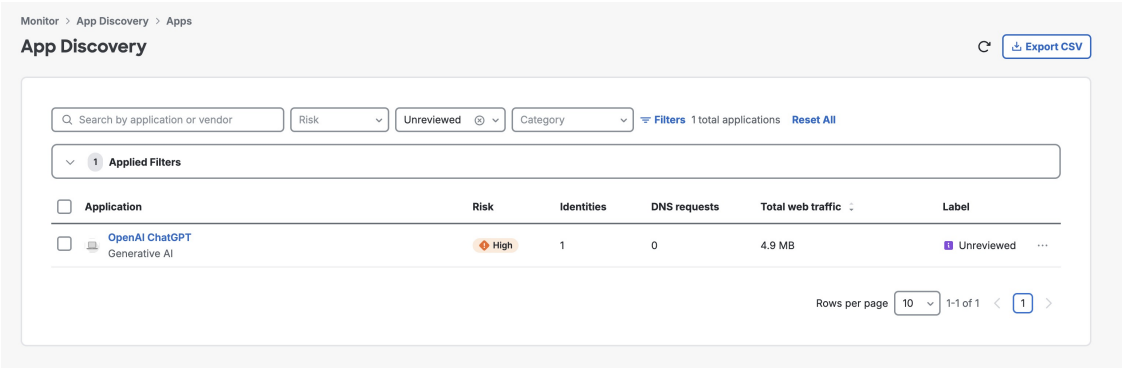
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

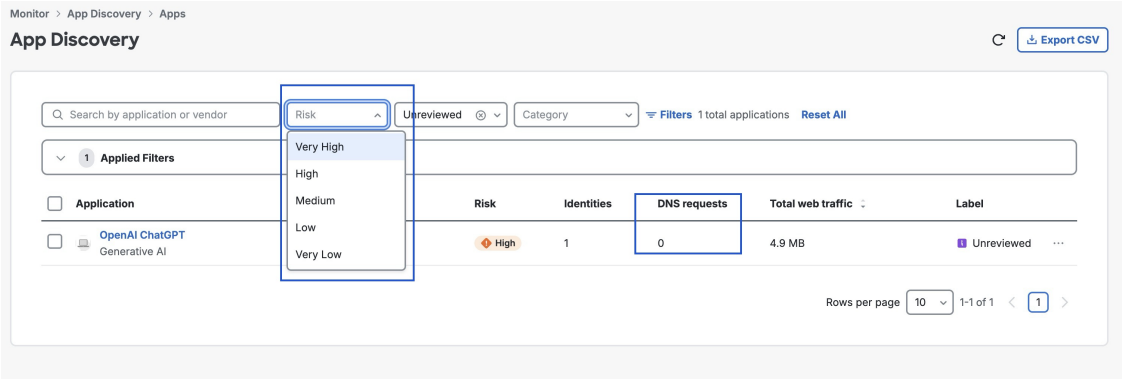
1. Navigate to **Monitor** > **Reports** > **App Discovery**.



2. From the overview, click **Unreviewed Apps**. The App Grid appears depicting data for the last 90 days.



3. Filter the list by selecting **Very High** or **High** from the Risk menu. Only the riskiest apps will be listed.
4. Filter the list by **DNS Requests** to display the apps with the highest number of requests at the top.



The apps at the top of the list should now represent the highest number of DNS requests made by the riskiest apps.

Review Apps in the Apps Grid

Describes Review Apps in the Apps Grid in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Apps Grid provides an overall view of application activity in your environment and the potential risk indicated by this traffic.

> **Note**
>
> **Packages and Feature Availability**

Not all of the features described here are available to all Secure Access packages. Information about your current package is listed on the Admin > Licensing page. For more information, see Determine Your Current Package.

If you encounter a feature here that you do not have access to, contact your sales representative for more information.

Procedure

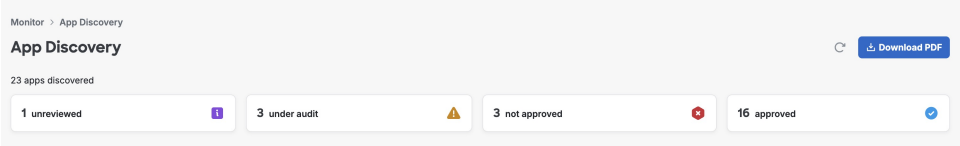
Provides instructions for completing the Procedure workflow in Cisco Secure Access. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



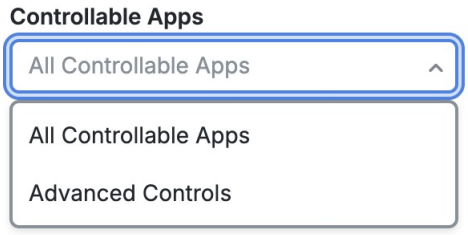
2. View by label.
   - **Unreviewed**–The app has not yet been assigned any label.
   - **Approved**–The app may be used in your environment.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Under Audit**–The app is currently under review.

> **Note**
>
> Once you relabel an Unreviewed app, you cannot change the app label back to Unreviewed. Use the Under Audit label for apps that still need review.

> **Note**
>
> Labels do *not* automatically block apps from use. You must configure a rule to block specific apps or apps with specific labels. For more information, see Control Apps.

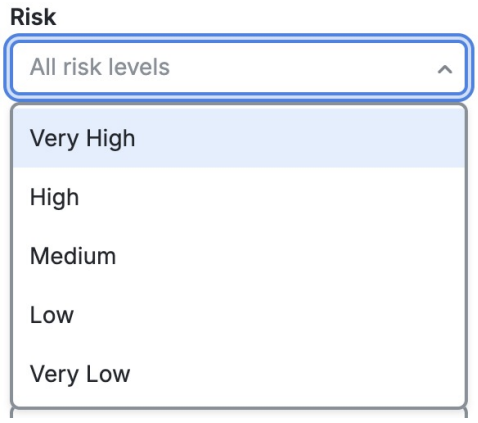
3. Filter by Controllable Apps.

You can filter the apps listed by apps that are controllable and apps that have advanced app controls.



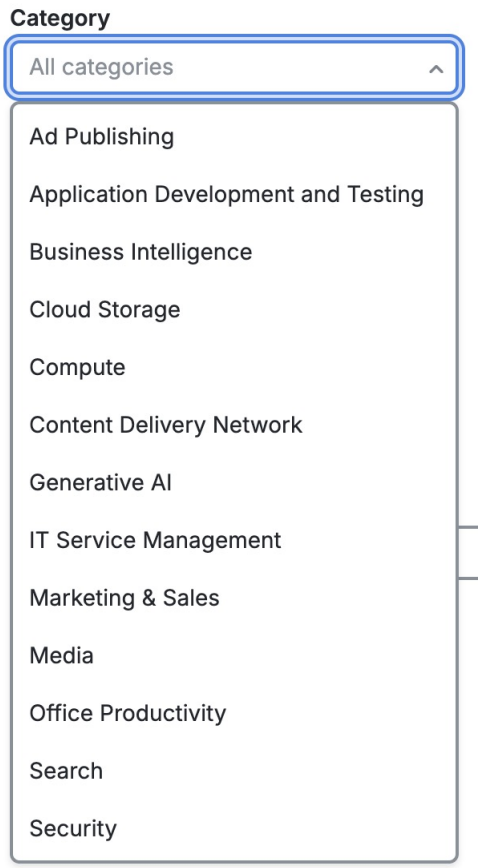
4. Filter by Risk.

   For more information on how risk is calculated, see Risk Details.

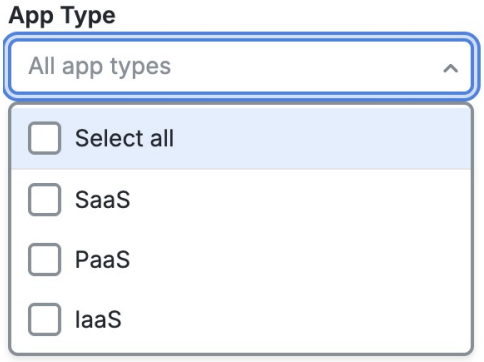


5. Filter by category.

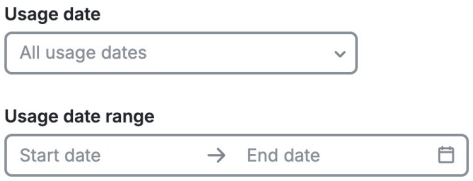
   For more information on app categories, see Application Categories.



6. Filter by app type.
   - **SaaS**–Software as a service
   - **PaaS**–Platform as a service
   - **IaaS**–Infrastructure as a service
   - **Select all**–Selects all app types



7. Filter by usage date. The app grid will display data for 24 hours based on the date selected. The default is the current date.



Configure Columns to Display

Provides instructions for completing the Configure Columns to Display workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

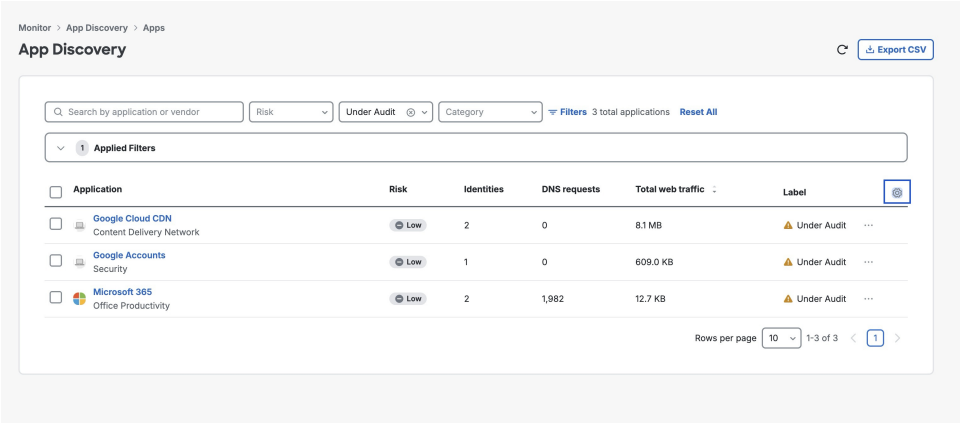
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

You can customize what columns are displayed.

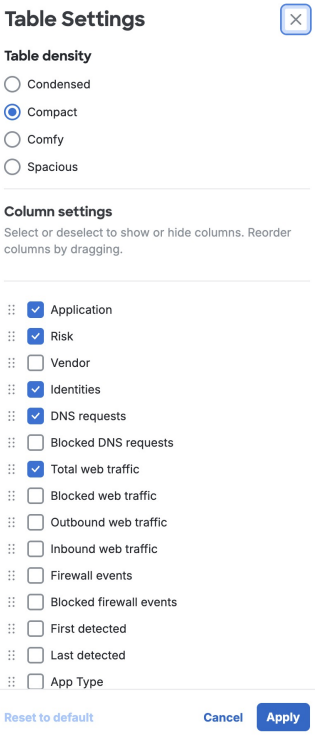
Procedure

1. Click the **Actions** icon.



2. Select columns to display and click **Apply**.

> **Note**
>
> Rearrange the order of settings by dragging and dropping the column fields,



- **App Type**–The type of app: SaaS, PaaS or IaaS.
- **Blocked DNS**–The percentage of DNS requests blocked by Secure Access based on policy configurations.
- **Blocked Traffic**–The percentage of all traffic blocked.
- **DNS Requests**–The number of DNS requests for this app.
- **First Detected**–The date the app was first detected.
- **Identities**–The number of identities affected by the app. Click this number to view the app's details and the list of identities with requests for that app.
- **Inbound Traffic**–Bytes inbound.
- **Last Detected**–The date the app was last detected.
- **Outbound Traffic**–Bytes outbound.
- **Total Traffic**–The total number of bytes inbound and outbound for this app in your environment.
- **Vendor**–The vendor that owns the app.
- **Weighted Risk**–The risk the app poses to the environment.

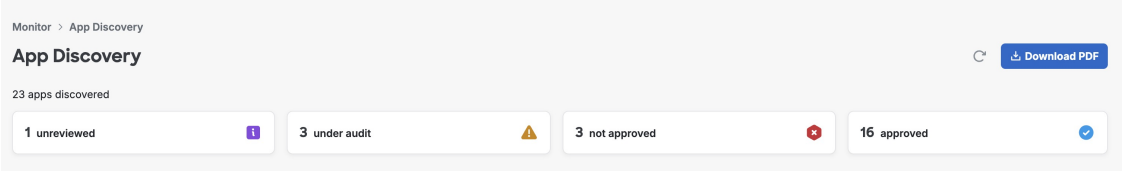
Change the Label of an App

Provides instructions for completing the Change the Label of an App workflow in Cisco Secure Access. Navigate to Reporting Core Reports App Discovery and click one of the app labels to open the Apps Grid.

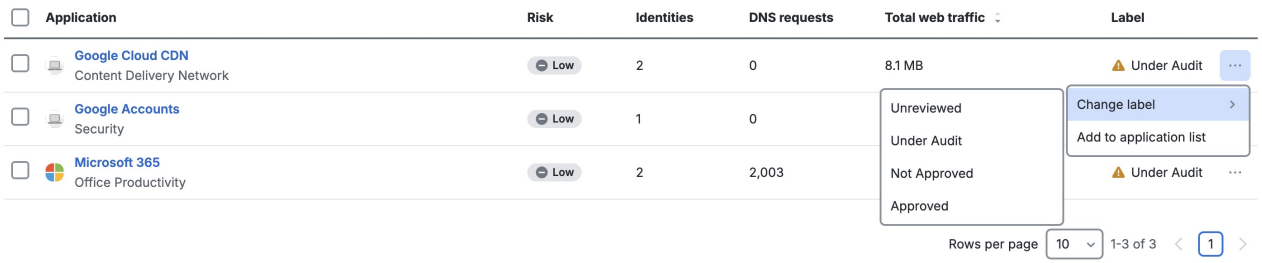
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Check the checkbox for the app or apps you want to change the label of, click the **Label** drop-down menu, and select the new label.



> **Note**
>
> Once you relabel an Unreviewed app, you cannot change the app label back to Unreviewed. Use the Under Audit label for apps that still need review.

> **Note**
>
> Labels do *not* automatically block apps from use. You must configure a rule to block specific apps or apps with specific labels. For more information, see Control Apps.

View App Details

Describes View App Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The details page for an app lists summary information about the app, including:

- The risk score for the app, and the details on how it was calculated.
- The identities that have made DNS requests and seen traffic for the app.

- The detailed attributes of the app, which can help you perform a risk/benefit analysis of permitting the app to be used in your environment.

> **Note**
>
> App details are also accessible from the Third-Party Apps Report.

Procedure

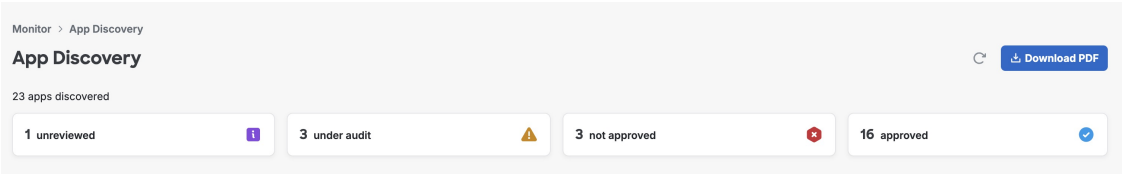
Provides instructions for completing the Procedure workflow in Cisco Secure Access. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

Before you begin

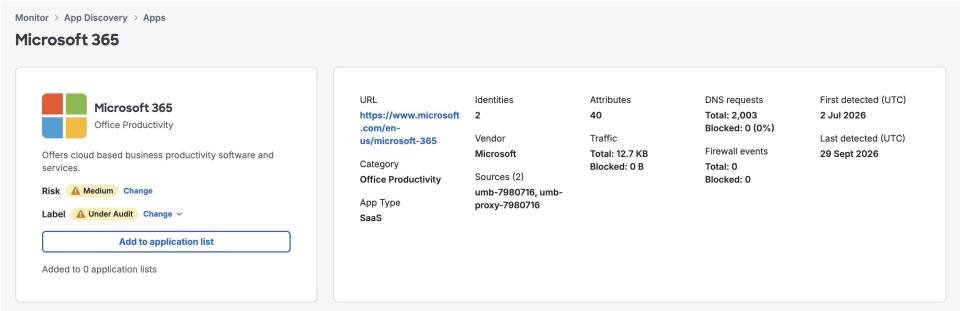
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Click the name of an app to view its details and traffic data for the last 90 days.
3. View the initial details of the app, including the name and a description of the app.



- **Risk Score**–The overall score assigned to the app. This could be calculated by Umbrella or assigned by you.

  The risk summary displays:

  - The Custom risk score, which appears if you have chosen to override the Weighted risk score calculated by Umbrella. To apply a Custom risk score see Change App Details.

    > **Note**
    >
    > If you apply a Custom risk score to an App, it will be noted in the Apps Grid display.

  - The Weighted risk score calculated by Umbrella based on Business risk, Usage risk, Vendor compliance, and Community risk (if available).

  - The Community risk score, which appears if one or more other users have assigned a Custom risk score to the app. Umbrella calculates the Community risk score as a median of the Custom risk scores assigned to the app by all users.

- A label describing the review status of the app for your installation: **Unreviewed**, **Approved**, **Not Approved**, or **Under Audit**. To change the label assigned to the app, see Change App Details.

  > **Note**
  >
  > App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

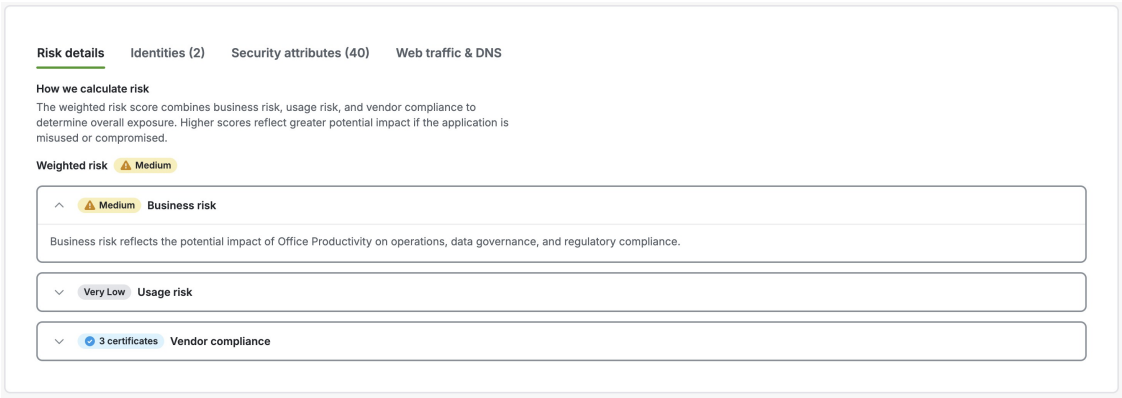
- A link to control the app. The link text may appear as **Control this app**, **Edit app controls**, or **Block this app**.
  - **Control this app**–Available only when **Block** or **Allow** have not been configured for this app. If the app setting is configured but has not yet been applied to a policy, a red tooltip appears.
  - **Edit app controls**–Available only when the app has previously configured application settings and you can enable advanced activities for the application.
  - **Block This App**–Appears when a block has not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.

    For more details, see Control Apps.

- **App URL**–The URL of the app.
- **Category**–The category the app falls under. For more information, see Application Categories.
- **Identities**–The number of sources that accessed the app.
- **Vendor**–The owner of the app.
- **Traffic**–The number of bytes of total traffic and bytes blocked.
- **DNS Requests**–The total number of DNS requests and the percentage of requests blocked by Secure Access.
- **First Detected**–The date the app was first detected.
- **Last detected**–The date the app was last detected.

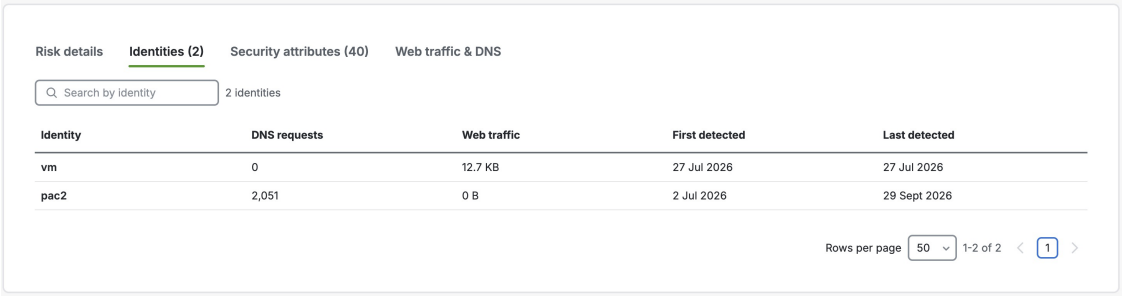
4. Click **Risk Details**.

   The Risk Details tab displays the app's risk score and how it was calculated, including Business Risk, Usage Risk, and Vendor Compliance.



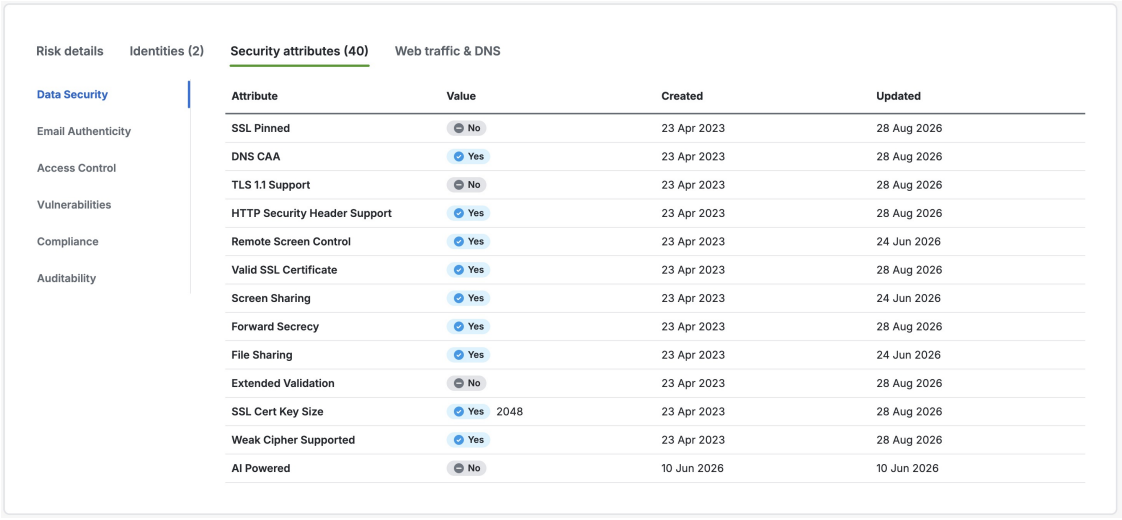
5. Click **Identities**.

   The Identities tab lists your organization's sources that have made DNS requests and traffic for this app.



6. Click **Security attributes**.

   The Attributes tab lists the various attributes associated with this app.



   Attributes are divided into categories. Click a category name to view the attributes associated with it. (Not all applications will show all attribute categories.)

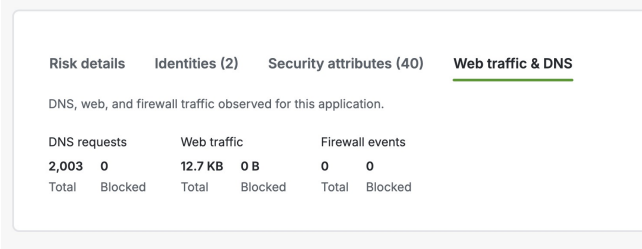
   For each displayed attribute, Secure Access shows whether the attribute applies to the application and the dates when the attribute information was collected and updated. Use the attributes to evaluate the risk that the application will expose your environment to data breaches, identity theft, financial fraud, and other cyber threats.

   The attribute categories are:

   - **Compliance attributes** – Indicate whether the application complies with the requirements of a number of certifications such as GDPR, HIPAA, and FEDRAMP.

- **Vulnerabilities attributes** – Indicate whether the application is vulnerable to exploits that attackers could use to compromise the security of the affected systems, steal sensitive data, or cause other types of damage.
- **Access control attributes** – Indicate the methods the application supports to manage and restrict access based on a user's identity, role, and authorization level.
- **Data security attributes** – Indicate the practices and technologies the application uses to protect data from unauthorized access, use, disclosure, modification, or destruction.
- **Auditability attributes** – Indicate the abilities the application provides for an administrator to review the activity and transactions of a system, to ensure that it is operating in a compliant and secure manner.
- **Email authenticity attributes** – Indicate what methods the app provides to verify that email is actually from the sender that it claims to be from, and that the message has not been tampered with or altered in any way during transit.

7. Click **Web traffic & DNS**.



This pane displays the total and blocked DNS, web, and firewall traffic observed for this application (in bytes).

Change App Details

Describes Change App Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

You can change details about apps from within the App Discovery Report:

- You can change the review status label assigned to an app. Labels help you keep track of the review status of apps, so you know which ones are approved for use in your environment. The possible label values are:
  - **Unreviewed**–The app has not yet been assigned any label.
  - **Approved**–The app may be used in your environment.
  - **Not Approved**–The app should not be used in your environment.
  - **Under Audit**–The app is currently under review.

> **Note**
>
> App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

- You can change the risk score for the app, overriding the value calculated by Umbrella. The possible risk scores are:
  - Very High

- High
- Medium
- Low
- Very Low

> **Note**
>
> Changing the risk score for an app does not change whether Secure Access blocks or allows the app. (You must configure application settings within a policy to block apps. For more information, see Manage the Access Policy or Manage Security Profiles for Internet Access.) Secure Access provides risk scores strictly for your own information, to help you keep track of the risk levels for different apps and decide whether to block or allow them. You can accept the risk levels calculated by Secure Access, or assign different risk scores based on the risk tolerances within your organization.

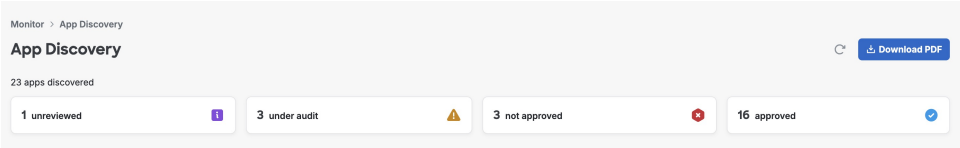
Change the Risk Score for an App

Provides instructions for completing the Change the Risk Score for an App workflow in Cisco Secure Access. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

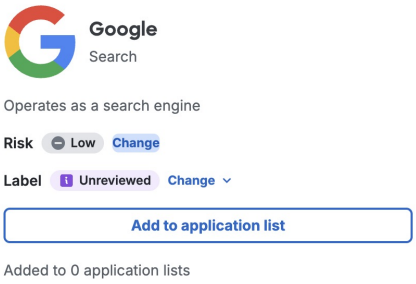
Before you begin
A minimum of Read Only access to the Secure Access dashboard. See Manage Accounts.

Procedure

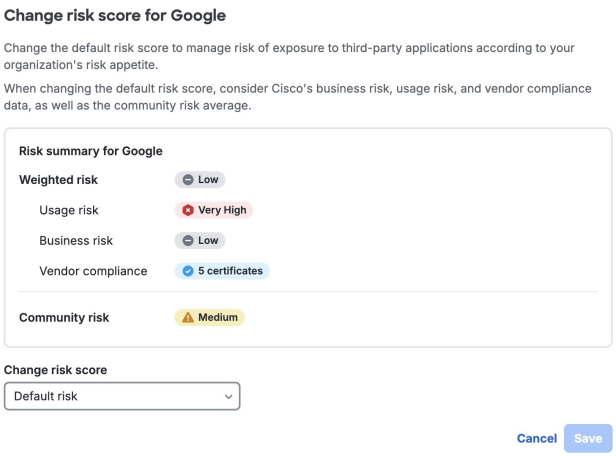
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



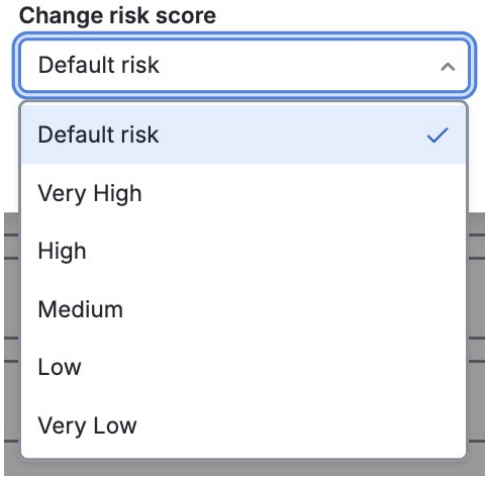
2. To change the risk score for an app from its Details page, click the name of the app on the Apps Grid, then from the Details page hover over the risk score to view the Risk Summary.



3. From the Risk Summary, click on **Change** to display the Risk Score Change dialog.



4. Select the new value to assign:
    - Very High
    - High
    - Medium
    - Low
    - Very Low



5. Click **Save**.

Change the Label of an App

Provides instructions for completing the Change the Label of an App workflow in Cisco Secure Access. Labels within the App Discovery report help you keep track of the review status of apps, so you know which ones are approved for use in your environment.

Labels within the App Discovery report help you keep track of the review status of apps, so you know which ones are approved for use in your environment. You can change the label for an app anytime.

> **Note**
>
> App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

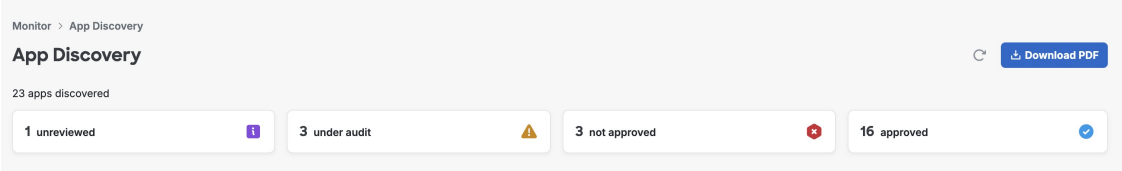
> **Note**
>
> Once an app has been given a label, it cannot be set back to **Unreviewed**. You can use the **Under Audit** label for apps that still need review.

Before you begin

A minimum of Read Only access to the Secure Access dashboard. See Manage Accounts.

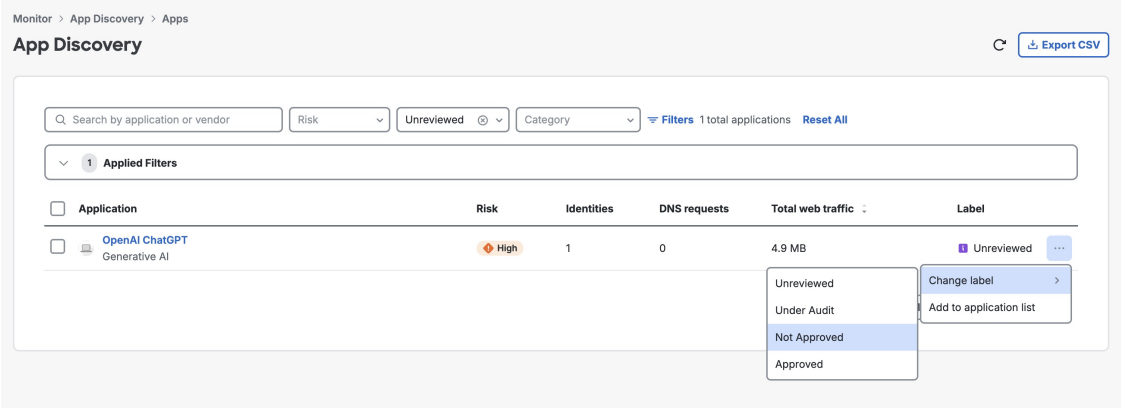
Procedure

1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.

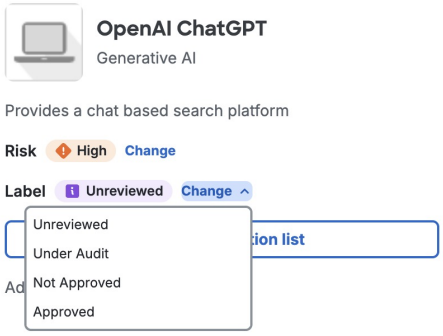


2. You have two choices:

   a. To change the label for an app from the Apps Grid, click **...** and **Change label**.



   b. To change the label for an app from its Details page, click the name of the app on the Apps Grid, then on the Details page, click **Change** against **Label** to view the Label menu.



3. From the Label menu, select your choice of new value to assign:
   - **Approved**–The app may be used in your environment.
   - **Unreviewed**–The app is not reviewed to be used in your environment.
   - **Not Approved**–The app should not be approved for use in your environment.
   - **Under Audit**–The app is currently under review.

Control Apps

Describes Control Apps in Cisco Secure Access. You can control applications through rules and through the App Discovery report in View App Details and the App Grid.

You can control applications through rules and through the App Discovery report in View App Details and the App Grid. The application settings are a rule component that enables controlling of supported apps, regardless of usage, at the policy level. The App Discovery report allows you to review apps in your organization and control apps individually.

> **Note**
>
> App blocking requires enablement within a rule. Apps that are not present in application settings, or do not have the **Edit app controls**, **Control this app**, or **Block this app** options in App Discovery cannot be blocked. If you need to block an app we don't have yet, contact Support to request it.

Procedure

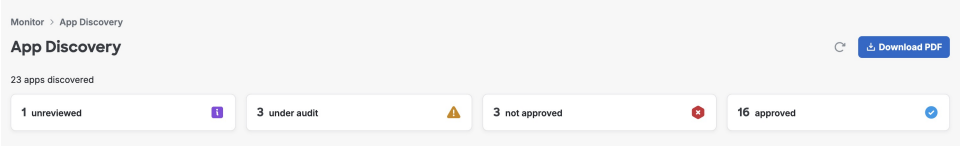
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

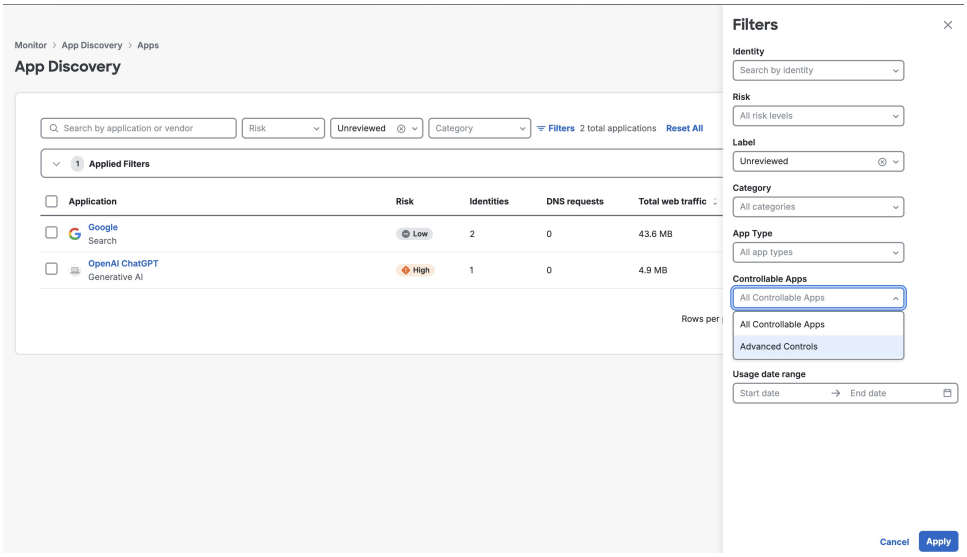
Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **App Discovery**.



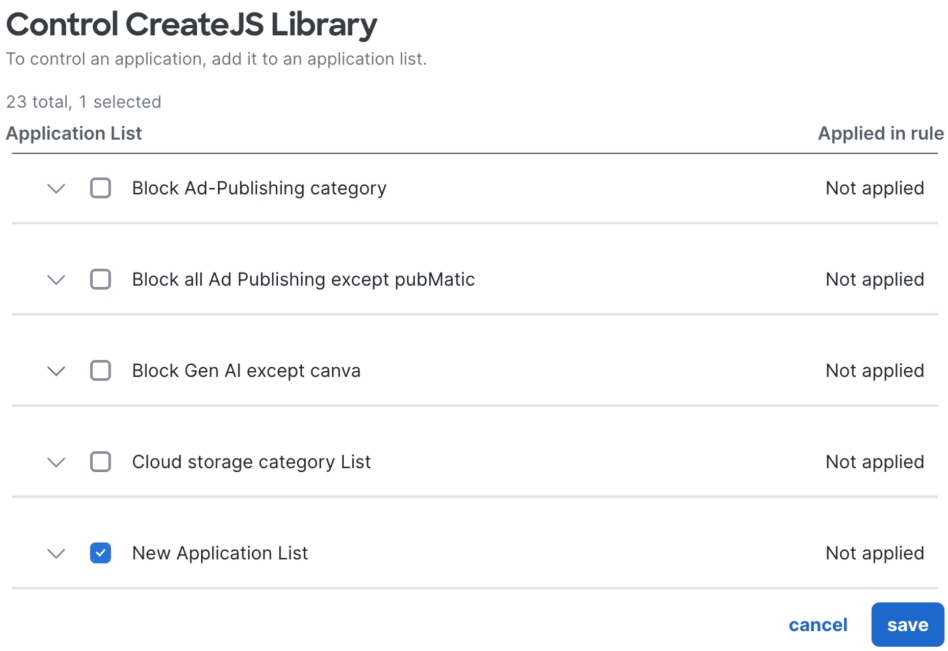
2. From the overview, click **Unreviewed Apps**. The App Grid appears depicting data for the last 90 days.
3. Select a **Controllable Apps** filter: **All Controllable Apps** or **Advanced Controls**.



4. Click **Edit App Controls**, **Control This App**, or **Block This App**.
   - **Block This App**–Appears when a block has not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
   - **Control This App**–Appears when **Block** or **Allow** have not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
   - **Edit App Controls**–Appears when the app has already had settings configured but can be edited.

5. On clicking **Control This App**, the **Control Application Name** window appears. Choose one or more application lists to add this application to and click **Save**. Once saved, the internet access rules set for the application lists are applied to the application.

   The application can only be added to application lists currently active in a policy.



Control Application Lists

Describes Control Application Lists in Cisco Secure Access. You can also configure a rule to block lists of applications and lists of application categories.

You can also configure a rule to block lists of applications and lists of application categories. For more information, see Manage Application Lists and Add an Application List.

For more information about applying application lists to rules, see Manage the Access Policy.

Control Advanced Apps

Describes Control Advanced Apps in Cisco Secure Access. Applications within App Discovery can be blocked or allowed based on risk assessment.

Applications within App Discovery can be blocked or allowed based on risk assessment. In addition to blocking all content for an application, you have the option to instead block only specific content, such as file uploads or posts.

Note

Secure Access Packages

Advanced App Controls are not available to all Secure Access packages. To determine your current package, navigate to Admin > Licensing. For more information, see Determine Your Current Package

You can edit the controls of apps with advanced app controls while reviewing applications in the App Discovery Report. You can filter out apps with advanced controls and edit their application settings in the Apps Grid, or edit the application settings in the app's Details page.

Procedure

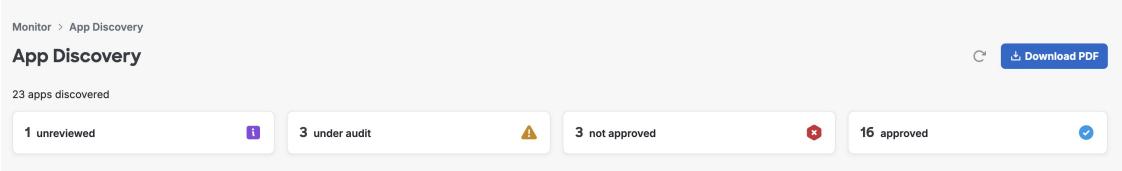
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

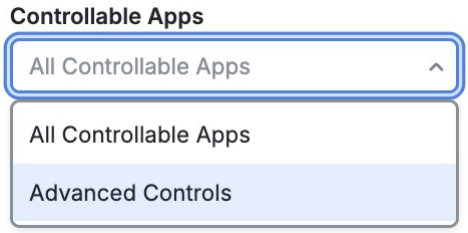
Full Admin user role. For more information, see Manage Accounts.

Procedure

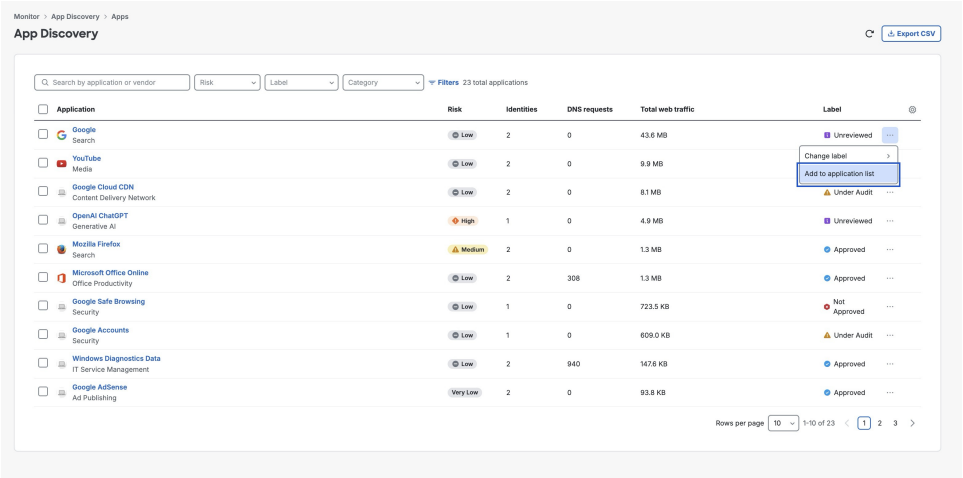
1. Navigate to **Monitor** > **Reports** > **App Discovery**.
2. Click any of the discovered apps labels to enter the Apps Grid.



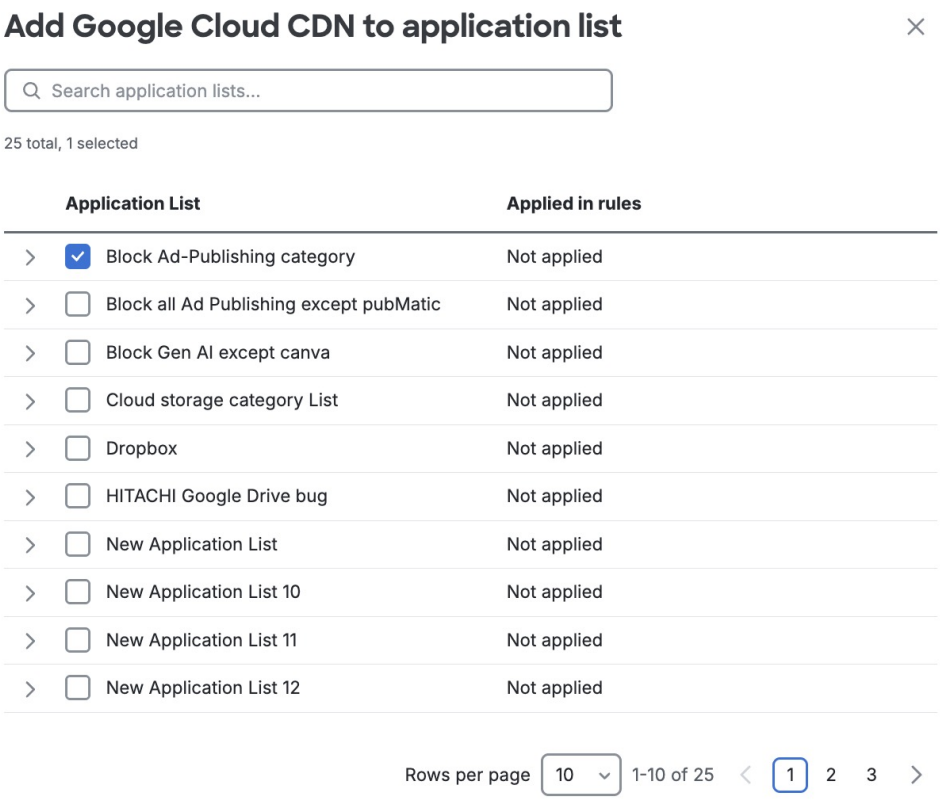
3. Choose **Advanced Controls** under the **Controllable Apps** filter.



4. Choose an app to control and click **Add to application list**.



5. On clicking **Control This App**, the **Control Application Name** window appears. Choose one or more application lists to add this application to and click **Save**. Once saved, the internet access rules set for the application lists are applied to the application.



The application can only be added to application lists that are currently active in a policy.

View Traffic Data Through SWG Service

Describes View Traffic Data Through SWG Service in Cisco Secure Access. App Discovery provides traffic data through the Secure Web Gateway (SWG) service.

App Discovery provides traffic data through the Secure Web Gateway (SWG) service. Traffic is reported in bytes in and bytes out.

View Traffic

Provides instructions for completing the View Traffic workflow in Cisco Secure Access. Navigate to Monitor Reports App Discovery and locate the DNS Requests by App Risk graph.

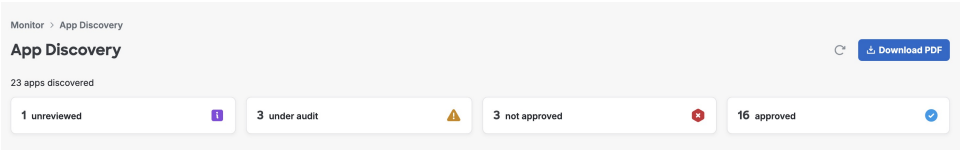
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Navigate to **Monitor** > **Reports** > **App Discovery** and locate the **DNS Requests by App Risk** graph.



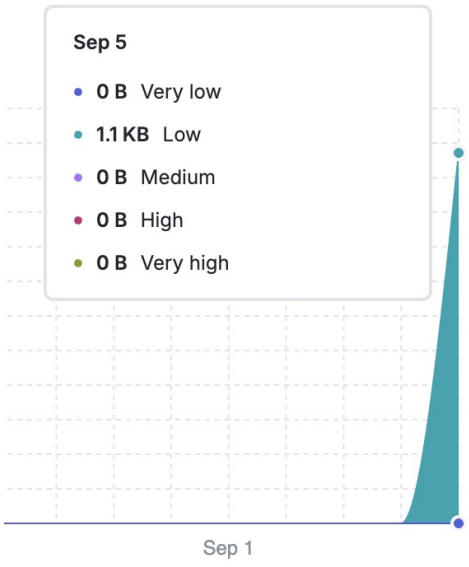
2. Click **Web** to display Traffic by App Risk.



3. Click **All Traffic** to open the drop-down and then choose to view **All Traffic**, **Inbound Traffic**, or **Outbound Traffic**.



4. Hover on a point in the graph to view details about the traffic by app risk for that date.



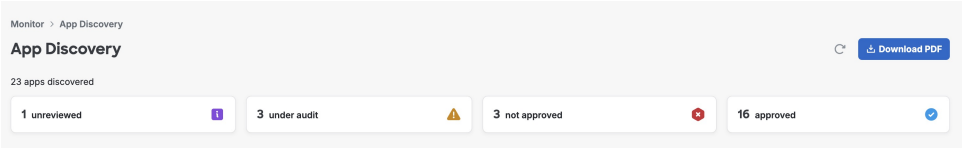
View Traffic in the Apps Grid

Provides instructions for completing the View Traffic in the Apps Grid workflow in Cisco Secure Access. Navigate to Monitor Reports App Discovery and click one of the app labels to open the Apps Grid.

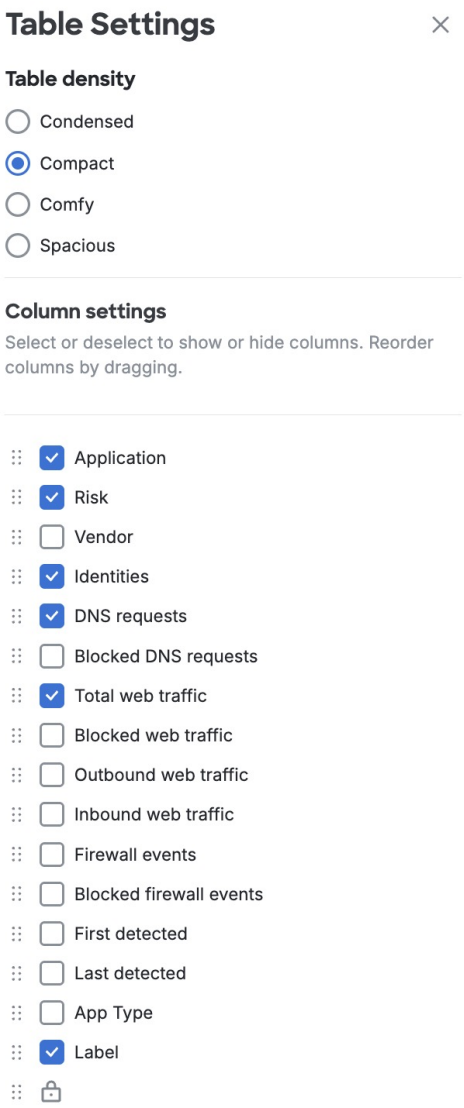
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

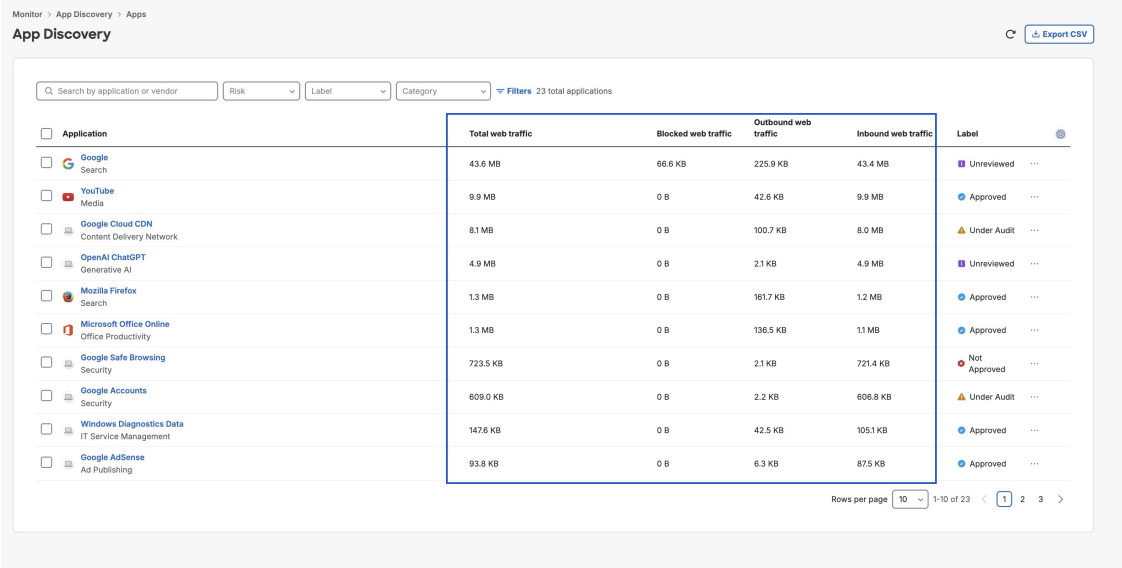
1. Navigate to **Monitor** > **Reports** > **App Discovery** and click one of the app labels to open the Apps Grid.



2. Click the action menu to open the drop-down of options for columns displayed in the grid. Select the columns relevant to traffic and then click **Apply**.



3. View the traffic, bytes in and out, of applications by total, outbound, or inbound traffic.



View Traffic in the App Details

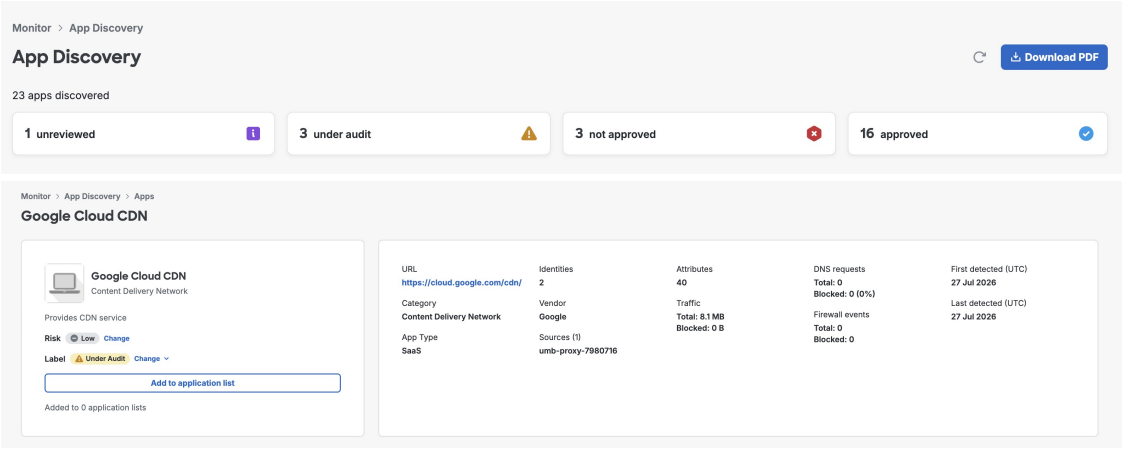
Provides instructions for completing the View Traffic in the App Details workflow in Cisco Secure Access. Navigate to Reporting Core Reports App Discovery and click the name of an app to view its details for the last 90 days.Details include the total and blocked traffic in bytes.

Before you begin

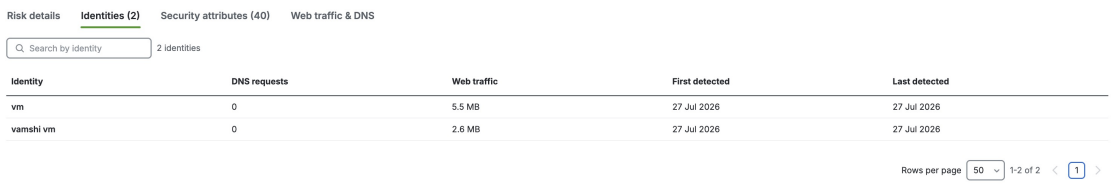
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Reporting** > **Core Reports** > **App Discovery** and click the name of an app to view its details for the last 90 days.



2. Navigate to the **Identities** section of the app details and view the total Web Traffic.



Third-Party Apps Report

Describes Third-Party Apps Report in Cisco Secure Access. The Third-Party Apps report lists third-party cloud applications that have been authorized to access sanctioned tenant applications.

The Third-Party Apps report lists third-party cloud applications that have been authorized to access sanctioned tenant applications. This report provides visibility to the risks to which your system is exposed by third-party app authorizations. From this report admin users can also block or allow access to third-party applications, overriding all existing authorizations and preventing users from authorizing the app in the future.

Currently the report presents information only about third-party applications authorized through Microsoft 365 tenants and Google Drive tenants.

- For Microsoft 365 tenants, you must authorize the tenant application for third-party access detection. For more information, see Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants. Third-Party Apps discovery for Microsoft 365 tenants is aggregated and processed on an hourly basis.
- For Google Drive tenants, you must authorize the tenant application for third-party access detection. For more information, see Enable Cloud Access Security Broker Features for Google Drive. In the case where the Secure Access administrator has blocked access from third-party applications, Secure Access prevents users from authorizing third-party apps by scanning for access granted to third-party applications every 7 minutes. This is necessary because Google Drive does not allow third-party access to be permanently blocked using an API; the frequent scans enable Secure Access to detect and revoke new third-party authorizations. A Google Drive administrator can override an application's authorization manually through the Google Drive interface and permanently block access to any third-party application.

View the Third-Party Apps Report

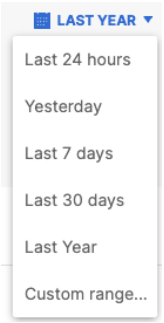
Provides instructions for completing the View the Third-Party Apps Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

Viewing the report requires a minimum user role of Read-Only. To use the block/unblock override feature, you must have the Admin user role. For more information, see Manage Accounts.

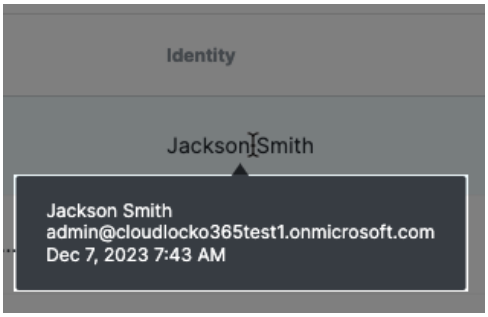
Procedure

1. Navigate to **Monitor** > **Reports** > **Third-Party Apps**.
2. Choose a time frame of application detection events. You can view the results for the last 24 hours, Yesterday, Last 7 Days, Last 30 Days, the Last Year (default), or a Custom range.

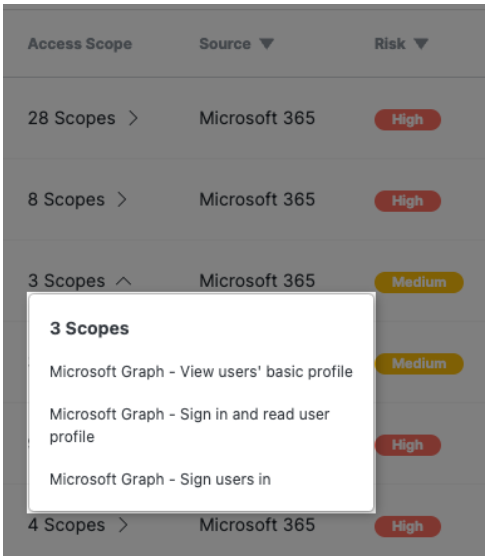


3. View the following columns for information on third-party application access events.

   - **Applications**: The names of third-party applications that users have authorized through the tenant application listed under the **Source** column. For applications whose names appear as links, Secure Access can provide additional information; click the link for an app name to view app details and traffic data for the last 90 days. See View App Details for more information.
   - **Identity**: The names of users that have accessed the third-party applications. Hover over a name to see the email address for the user and the date and time of the access event.

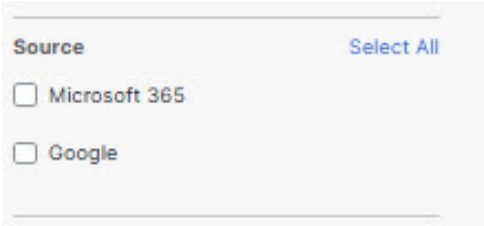


   - **Tenant Name**: The name of the tenant from which authorization originated. (See Manage Cloud Malware Protection for information about authenticating tenant applications.)
   - **Access Scope**: The number of access permission scopes granted to the third-party application. Click on a value in the **Access Scope** column to see the scopes listed by name.

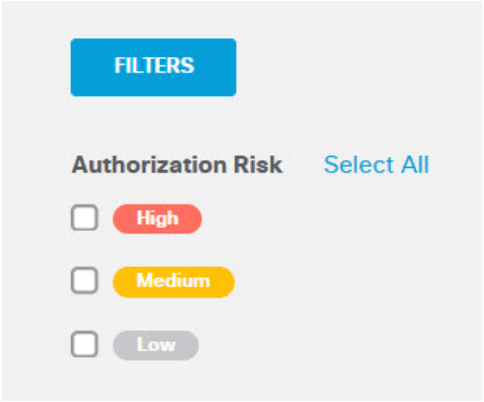


   - **Source**: The tenant application from which authorization originated. The report presents information about third-party applications authorized through Microsoft 365 or Google tenants. For more information, see Enable Cloud Access Security Broker Protection for Microsoft 365 Tenants or Enable Cloud Malware Protection for Google

Drive. You can filter the report results by values in this column using the filter selections on the left side of the screen.



- **Authorization Risk**: The risk scope Umbrella has calculated for the third-party application, based on the access scopes granted by the user that authorized the application to access an application tenant. The possible values are Low, Medium, and High. You can filter the report results by values in this column using the filter selections on the left side of the screen.

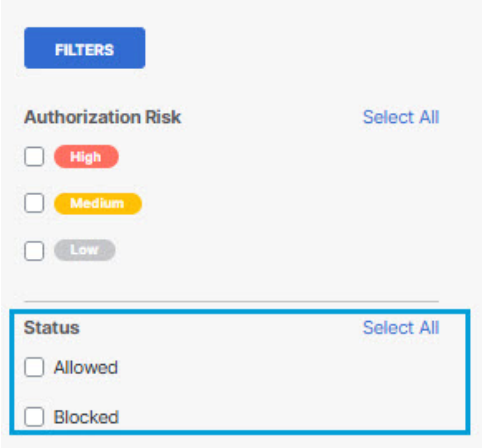


- **App Risk**: The overall weighted risk score assigned to the app. This could be calculated by Secure Access (based on Business risk, Usage risk, Vendor compliance, and Community risk (if available)) or assigned by you. The possible values are Very Low, Low, Medium, High, and Very High.
- **Detected**: The time and date when Secure Access detected the access event.
- **Status**

  Block/Allow status for the third-party application:

  - **Blocked** - The system has blocked users from granting access to the application via sanctioned tenant. (Overriding the access granted by a tenant application.)
  - **Failed to Block** - The system has attempted to block users from granting access to the application via sanctioned tenant, but the block attempt failed. Retry the block action; if it fails again, check that your tenant authentication is active. (You may need to re-authenticate.) If you are still unable to block the application, contact Support.
  - **Allowed** - The system allows users to grant access to the application via sanctioned tenant.
  - **In progress** - A block or unblock action is in progress. (The action in progress will appear dimmed in the **Permissions** column.)

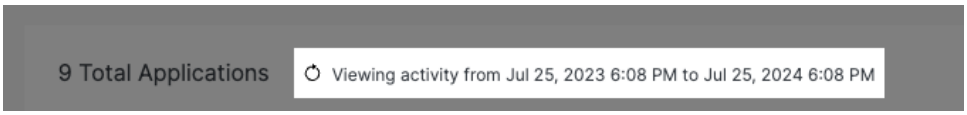
    You can filter the report results by the values **Allowed** and **Blocked** in this column using the filter selections on the left side of the screen.



- **Permissions**: This column offers administrators the ability to override the tenant access granted to third-party apps by another user. The possible actions are:
  - **Block** - Block the third-party applications from accessing the application via a sanctioned tenant, overriding access granted by other users.
  - **Unblock** - Allow the third-party application to access the application via a sanctioned tenant.

  The options in this column will appear dimmed if they are not available for any of the following reasons:
  - The user does not have admin privilege.
  - A block or unblock action is in progress.
  - A block action has failed

4. Sort columns by **Tenant Name**, **Applications**, **Source**, **Risk**, or **Detected**.
5. Click the **Refresh** button at the top of the report to update results.



Search the Third-Party Apps Report

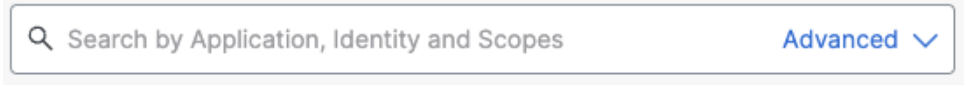
Provides instructions for completing the Search the Third-Party Apps Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

Viewing the report requires a minimum user role of Read-Only. To use the block/unblock override feature, you must have the Admin user role. For more information, see Manage Accounts.

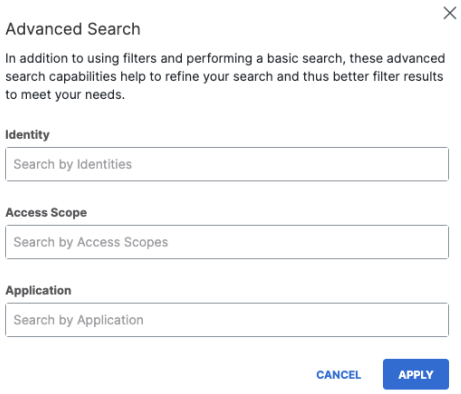
Procedure

1. Use the search bar above the report results to search by a specific application, identity, or permission scope.



Select a search result to apply it as a filter to the report columns **Application**, Identity, or **Access Scope**.

2. Click **Advanced** to perform a targeted search.



Note

- There is a three-character minimum for search terms.
- The search feature does not support wildcards.
- The system does not search detail information from the **Identity** column.
- Search results reflect matches found for all third-party applications that users have authorized. Results are not restricted by the time frame or filters applied to the report.

Export the Third-Party Apps Report

Provides instructions for completing the Export the Third-Party Apps Report workflow in Cisco Secure Access. Click Download CSV at the top right of the report to export results in CSV format.

Click **Download CSV** at the top right of the report to export results in CSV format.

Before you begin

Viewing the report requires a minimum user role of Read-Only. To use the block/unblock override feature, you must have the Admin user role. For more information, see Manage Accounts.

Procedure

1. The export will include results of the time frame and filters applied to the report.
2. The file name format will be **Third_Party_Apps_Third_Party_Apps_YYYY_MM_DD_hh_mmss.sssZ.csv**

   Where:

   - ***YYYY-MM-DD*** represents the date of the download.
   - ***hh_mm_ss.sss*** represents the time of the download.

View App Details

Describes View App Details in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The details page for an app lists summary information about the app, including:

- The risk score for the app, and the details on how it was calculated.
- The identities that have made DNS requests and seen traffic for the app.
- The detailed attributes of the app, which can help you perform a risk/benefit analysis of permitting the app to be used in your environment.

From the App Details page you can change some details assigned to the application by Secure Access.

> **Note**
>
> App details are also accessible from the App Discovery Report.

Procedure

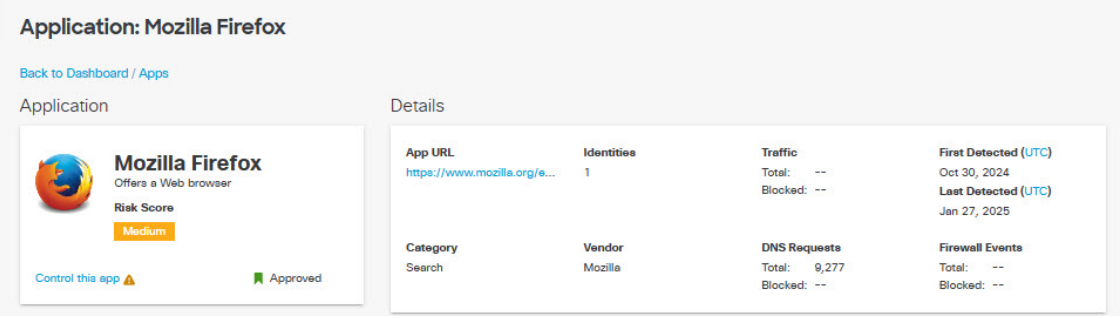
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

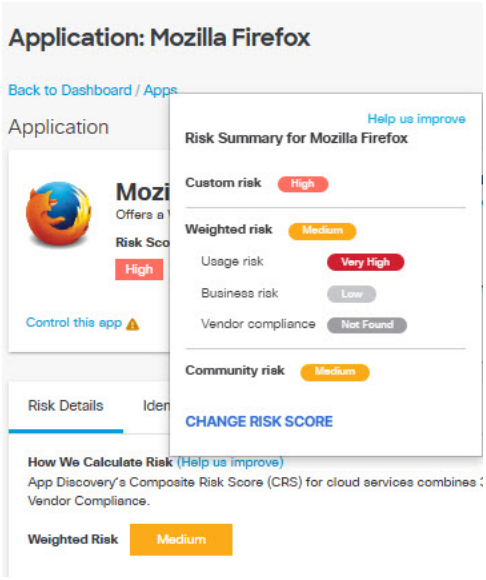
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Third-Party Apps**.
2. For applications whose names appear as links, Secure Access can provide additional information. Click the link for an app name to view app details and traffic data for the last 90 days.
3. View the initial details of the app, including the name and a description of the app.



- **Risk Score**–The overall score assigned to the app. This could be calculated by Secure Access or assigned by you. Hover over the Risk Score icon to display the risk Summary for the app:



The risk summary displays:

- The Custom risk score, which appear if you have chosen to override the Weighted risk score calculated by Umbrella. Too apply a Custom risk score see Change App Details.
- The Weighted risk score calculated by Umbrella based on Business risk, Usage risk, Vendor compliance, and Community risk (if available).
- The Community risk score, which appear if one or more other users have assigned a Custom risk score to the app. Secure Access calculates the Community risk score as a median of the Custom risk scores assigned to the app by all users.

You can click on **CHANGE RISK SCORE** to change the risk score for the app, overriding the value assigned by Secure access. The possible values are **Very High**, **High**, **Medium**, **Low**, and **Very Low**. More for information see Change App Details.

- A label describing the review status of the app for your installation: **Unreviewed**, **Approved**,**Not Approved** , or **Under Audit**. Hover over the status label to override the status assigned by Secure Access. You can change the status label to **Approved**, **Not Approved**, or **Under Audit**. More for information see Change App Details.

> **Note**
>
> App labels are primarily used for tracking and filtering, to help you keep track of the app review process within your organization. They do not of themselves control access to an app. However, if you establish an app risk profile that uses Label Status as a criteria, and that profile is used in an internet access rule, that rule may cause an application to be blocked or allowed based on the value of its app label.

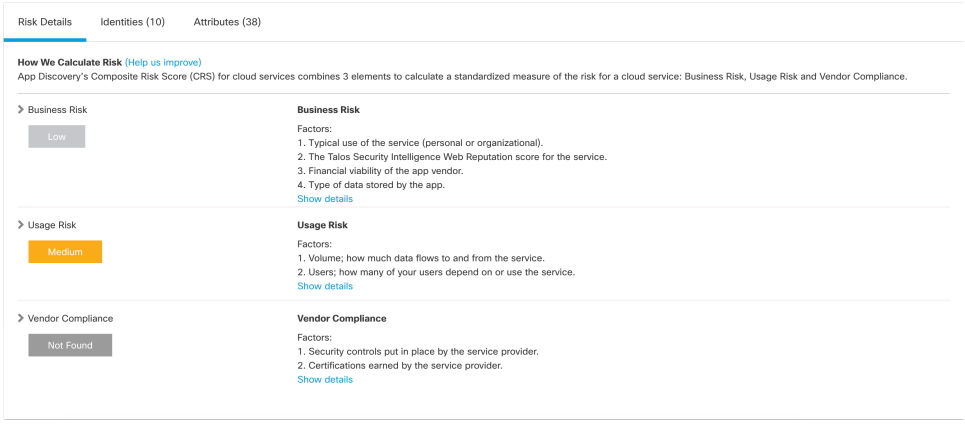
- For controllable apps, click **Edit App Controls**, **Control This App**, or **Block This App** to choose which application lists to add this app to and whether to block or allow it.
  - **Block This App**–Appears when a block has not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
  - **Control This App**–Appears when **Block** or **Allow** have not been configured for this app, or a red tooltip icon will appear if the app setting is configured but has not yet been applied to a policy.
  - **Edit App Controls**–Appears when the app has already had settings configured but can be edited.

For more information see Control Apps.

- **App URL**–The URL of the app.
- **Category**–The category the app falls under. For more information, see Application Categories.
- **Identities**–The number of sources that accessed the app.
- **Vendor**–The owner of the app.
- **Traffic**–The number of bytes of total traffic and bytes blocked.
- **DNS Requests**–The total number of DNS requests and the percentage of requests blocked by Secure Access.
- **First Detected**–The date the app was first detected.
- **Last detected**–The date the app was last detected.

4. Click **Risk Details**.

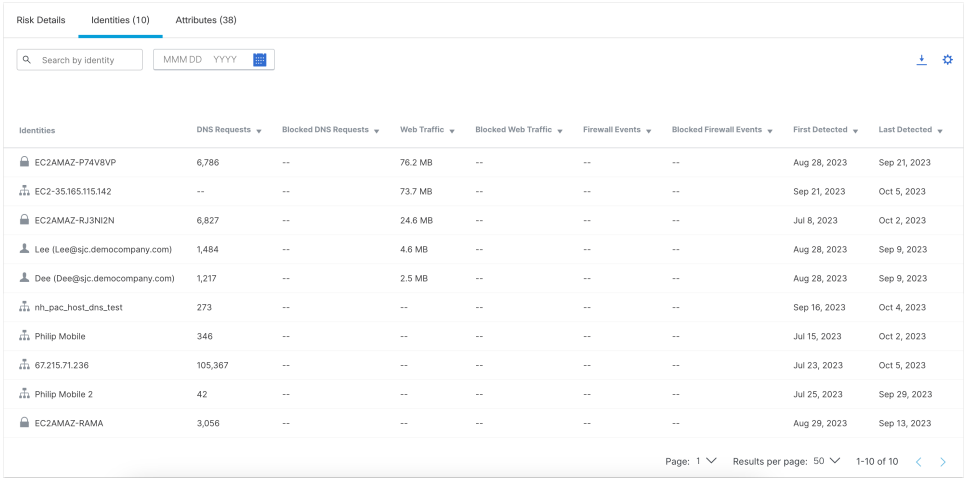
The Risk Details tab displays the app's risk score and how it was calculated, including Business Risk, Usage Risk, and Vendor Compliance.



5. Click **Identities**.

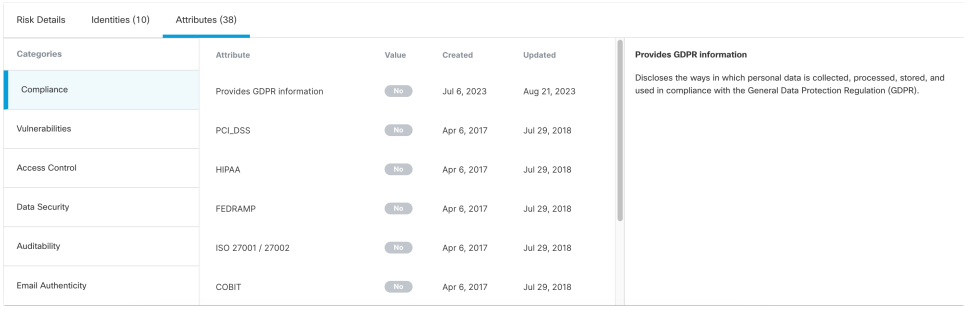
The Identities tab lists your organization's sources that have made DNS requests and traffic for this app.

Click the Download CSV icon to download this information as a CSV file.



6. Click **Attributes**.

The Attributes tab lists the various attributes associated with this app.



What to do next

Attributes are divided into categories. Click a category name to view the attributes associated with it. (Not all applications will show all attribute categories.)

For each displayed attribute, Secure Access shows whether the attribute applies to the application and the dates when the attribute information was collected and updated. Use the attributes to evaluate the risk that the application will expose your environment to data breaches, identity theft, financial fraud, and other cyber threats.

The attribute categories are:

- **Compliance attributes** – Indicate whether the application complies with the requirements of a number of certifications such as GDPR, HIPAA, and FEDRAMP.
- **Vulnerabilities attributes** – Indicate whether the application is vulnerable to exploits that attackers could use to compromise the security of the affected systems, steal sensitive data, or cause other types of damage.
- **Access control attributes** – Indicate the methods the application supports to manage and restrict access based on a user's identity, role, and authorization level.
- **Data security attributes** – Indicate the practices and technologies the application uses to protect data from unauthorized access, use, disclosure, modification, or destruction.
- **Auditability attributes** – Indicate the abilities the application provides for an administrator to review the activity and transactions of a system, to ensure that it is operating in a compliant and secure manner.
- **Email authenticity attributes** – Indicate what methods the app provides to verify that email is actually from the sender that it claims to be from, and that the message has not been tampered with or altered in any way during transit.

75 Cloud Malware Report

Topics:

- Cloud Malware Report

Provides an overview of Cloud Malware Report in Cisco Secure Access, including Cloud Malware Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Cloud Malware Report

Describes Cloud Malware Report in Cisco Secure Access. The Cloud Malware report provides an overview of malicious files within your environment and details the potential risk and exposure these files present.

The Cloud Malware report provides an overview of malicious files within your environment and details the potential risk and exposure these files present. For instructions to initiate malware scanning, see Enable Cloud Malware Protection on page 1739.

To use the Cloud Malware report, you need a minimum user role of Read-only. For more information, see Accounts Overview on page 191.

To find the Cloud Malware report, navigate to **Monitor** > **Reports** > **Cloud Malware**.

View the Cloud Malware Report

Provides instructions for completing the View the Cloud Malware Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Reports** > **Cloud Malware**.

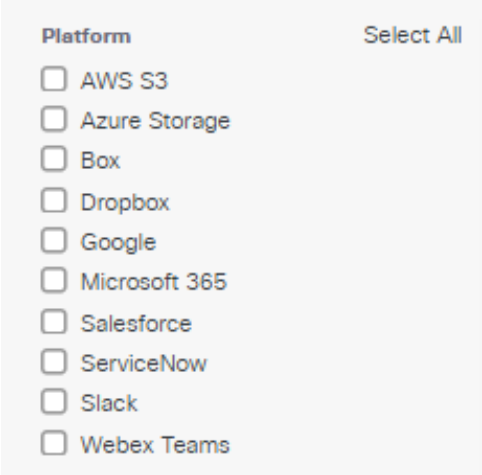


2. View the report's overview of information about the malicious files in your organization.
   - **Total files scanned** –The total number of files in the organization scanned for potential malware. This will also show a status as to whether the scan is complete or in progress.
   - **Platforms**–The platforms where malicious files were found.
   - **Malware found**–The total number of files found deemed malicious.
   - **Users with malware**–The number of users in your environment whose files contain malware.

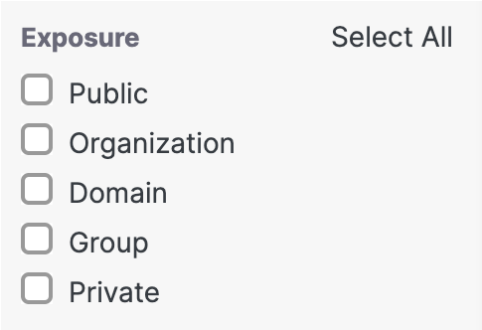
3. Filter by platform.

   The platforms available for Cloud Malware are AWS S3, Azure Storage, Box, Dropbox, Google, Microsoft 365, Salesforce, ServiceNow, Slack, and Webex Teams. You can filter your malicious files' results by selecting any or all of the platforms listed.

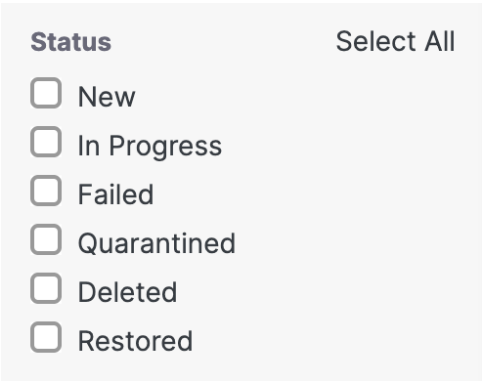
> **Note**
>
> Secure Access supports Cloud Malware protection for Salesforce files and files attached to chatter posts, not for sObjects or for chatter posts.



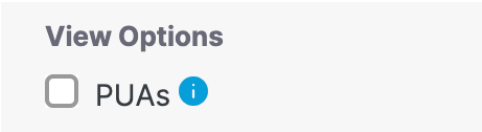
4. Filter by exposure. You can filter your malicious files by the type of exposure they pose to the environment. By default, none are selected, so all exposure types are presented.



5. Filter by status. Each file displays a status depending on whether it is newly discovered, a quarantine is in progress or failed, or that the file was successfully quarantined or deleted.



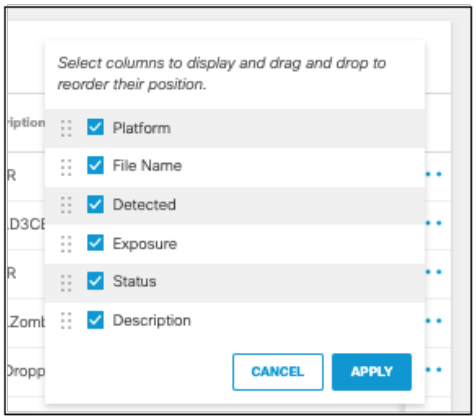
6. Optionally, you can choose to view suspect Potential Unwanted Applications.



7. Sort columns by detection or status.



Click the settings menu icon to select which columns to display and organize them as you choose.



Use the Cloud Malware Report

Describes Use the Cloud Malware Report in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic.

View Detailed Information About a File

Provides instructions for completing the View Detailed Information About a File workflow in Cisco Secure Access. You must have a minimum user role of Read-only.

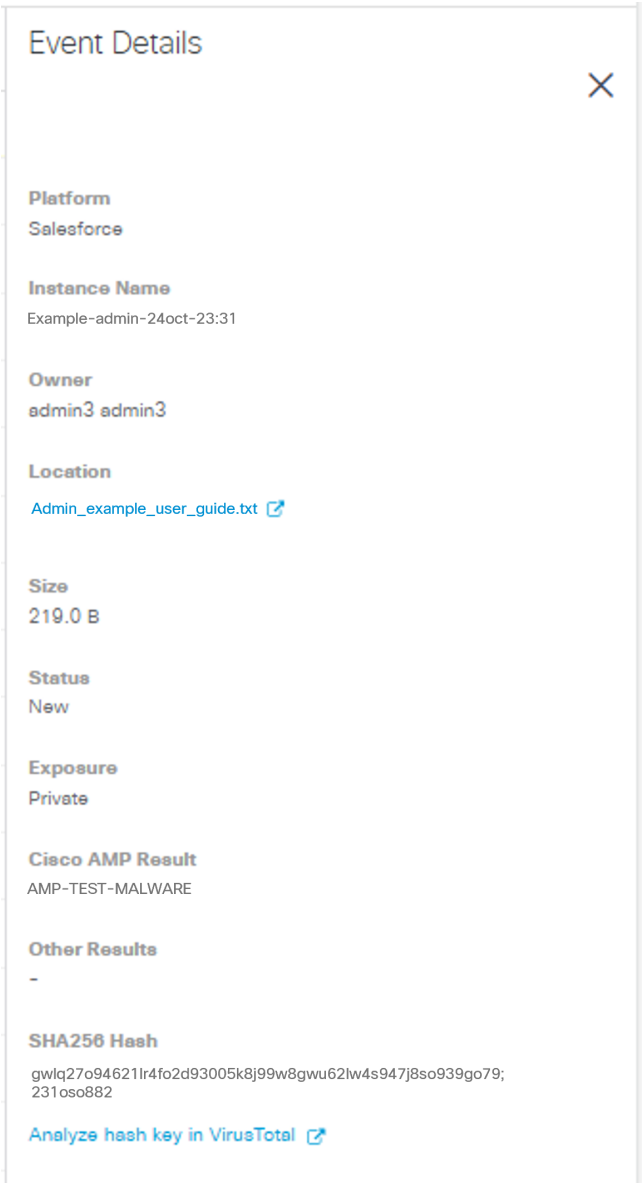
You can use the Cloud Malware Report to view details (such as owner, location, and size) about malicious files within your environment.

Before you begin

- You must have a minimum user role of Read-only. See Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Cloud Malware**.
2. Review the list of files and identify a file of interest.
3. Click the action menu (3 dots) to the right of the file of interest, then select **See Full Details**.
4. Review the information that appears.



Quarantine a Malicious File

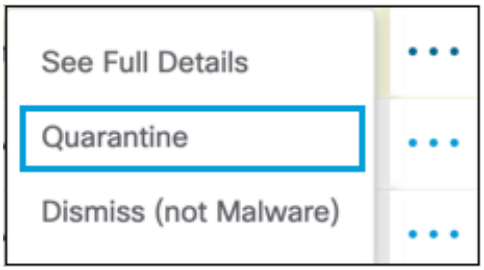
Provides instructions for completing the Quarantine a Malicious File workflow in Cisco Secure Access. On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, Salesforce, ServiceNow, or Google Drive, when a malicious file presents a potential risk and needs remediation, you can manually quarantine the file.

On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, Salesforce, ServiceNow, or Google Drive, when a malicious file presents a potential risk and needs remediation, you can manually quarantine the file. Only the integration user for the platform will have access to the quarantined files.

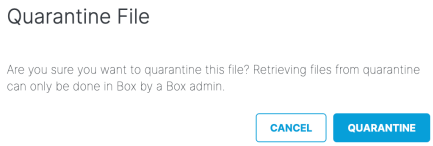
Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the Action Menu to the right of the file that needs to be quarantined, then select **Quarantine**.



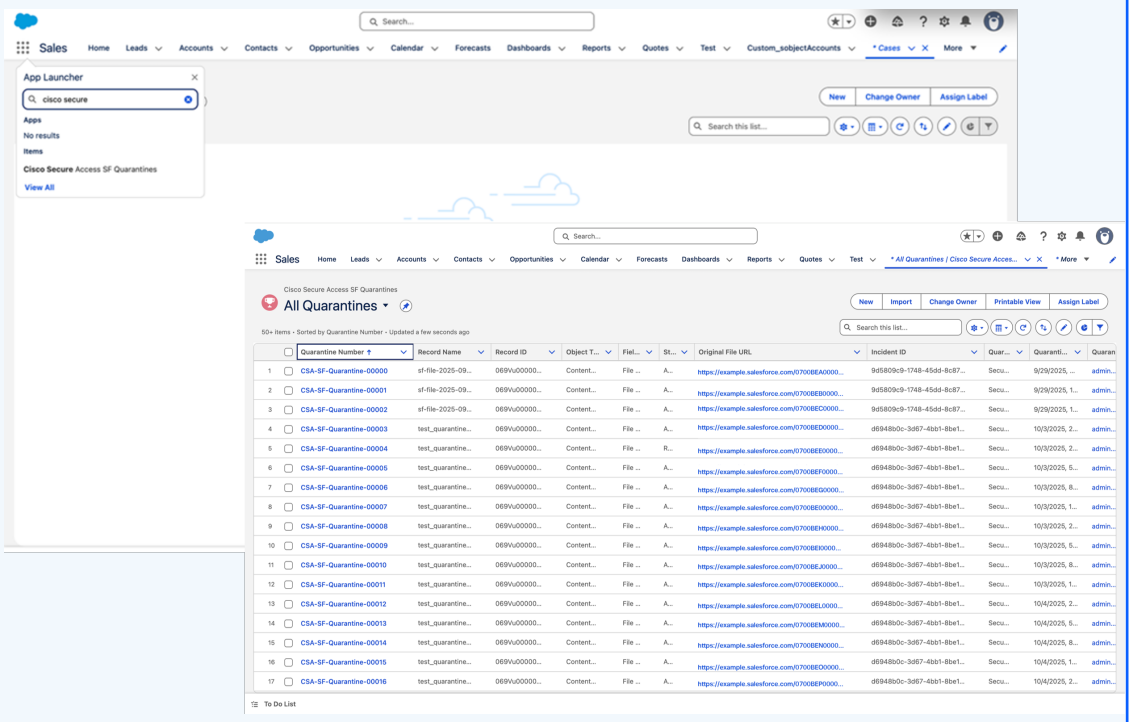
2. A modal appears to verify if this is the file to be quarantined. Click **Quarantine**. The status will update in the report to *Quarantine in Progress* while the quarantine is processing. This process can take up to five minutes; when complete, the status will update to **Quarantined**.



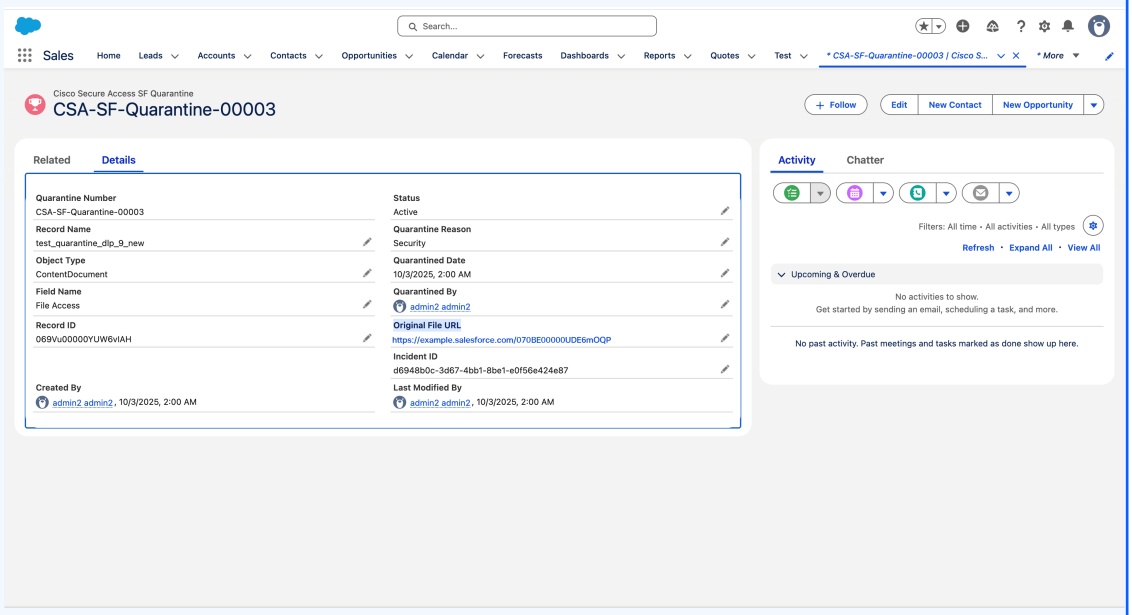
Note

- For Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive:
  - The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Secure Access created in the root path of the Global Admin who authorized the tenant.
  - The user who authorizes access to Secure Access will have access to the quarantine folder. All other accesses and collaborators are removed. Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.
- For ServiceNow:
  - The file identified as exposing sensitive data is moved to a table named Cisco_Quarantine_Malware which can be access only by the admin user who authorized the ServiceNow tenant.
  - A footprint is attached to the notes\activities area of the table the file was originally attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.
- For Salesforce:

  Secure Access applies the **Quarantine** response action to files only (including those attached to chatter posts). Choose **Quarantine** to:
  - Remove all collaborators, and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.



  Click on the listing for an individual file to see the information about it:



- Replace the file in its original location with a text file named ***filename*_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

- Quarantine attempts may fail if the files have been locked or blocked by settings within their native platforms. Settings local to the platform where a file resides take precedence over Secure Access' ability to detect or remediate DLP violations or malware.

Restore a Quarantined File

Provides instructions for completing the Restore a Quarantined File workflow in Cisco Secure Access. On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, ServiceNow, Salesforce, or Google Drive platforms, you can restore a file that has previously been quarantined.

On the Microsoft OneDrive, SharePoint Online, Box, Dropbox, ServiceNow, Salesforce, or Google Drive platforms, you can restore a file that has previously been quarantined.

Note

Once a file has been quarantined and then restored, it cannot be quarantined again.

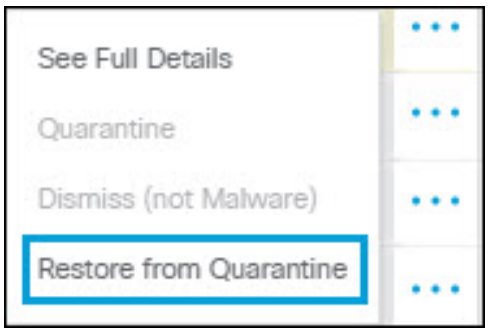
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

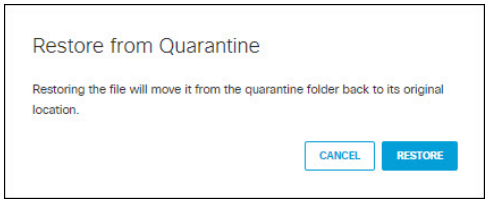
Procedure

---

1. Click the Action Menu to the right of the file that needs to be quarantined, then select **Restore from Quarantine**.



2. A dialog box appears to verify the file is to be restored. Click **RESTORE**. The status will update to **Restoration in Progress** while the file is being processed. This can take up to five minutes; when complete, the status will update to **Restored**.



Note

If your Cloud Malware deployment processes files from Microsoft OneDrive, SharePoint Online, Box, Dropbox, ServiceNow, Salesforce, or Google Drive and you restore a quarantined file that still violates rule criteria, the system will quarantine that file again. To prevent the system from quarantining the file again, remove the file's violation, or update the rule's criteria.

Delete a Malicious File

Provides instructions for completing the Delete a Malicious File workflow in Cisco Secure Access. For the Webex Teams platform, when a malicious file presents a potential risk and needs remediation, you can delete the file.

For the Webex Teams platform, when a malicious file presents a potential risk and needs remediation, you can delete the file.

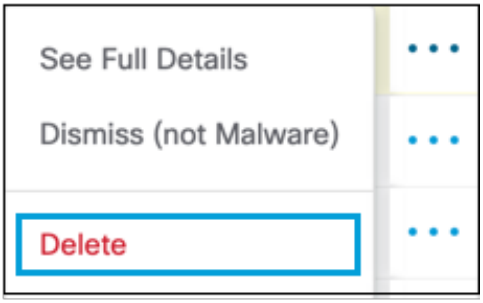
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

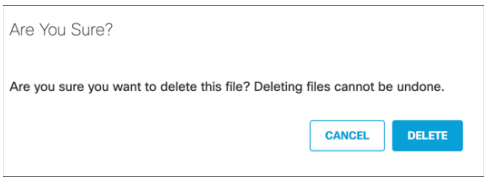
Procedure

---

1. Click the Action Menu for the file that needs to be quarantined and choose **Delete**.



2. A modal appears to verify if this is the file to be deleted. Click **Delete**. The report status is updated to *Deleted*.



Dismiss an Item from the Report

Provides instructions for completing the Dismiss an Item from the Report workflow in Cisco Secure Access. When a reported file is found to not present a risk, you can dismiss the file from the report.

When a reported file is found to not present a risk, you can dismiss the file from the report.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

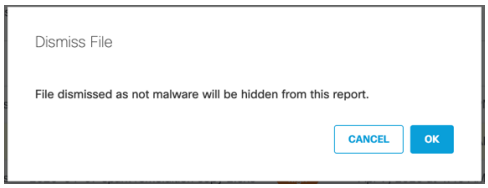
Procedure

---

1. Click the Action Menu for the file that needs to be removed from the report and choose **Dismiss**.



2. A modal appears to verify if this is the file to be dismissed. Click **OK**. The file is removed from the report.



Export a Cloud Malware Report

Provides instructions for completing the Export a Cloud Malware Report workflow in Cisco Secure Access. You can export your Cloud Malware report to a CSV file for your records.

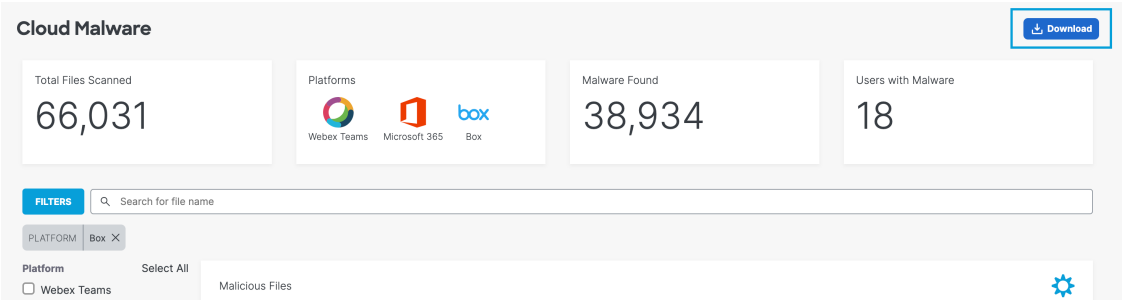
You can export your Cloud Malware report to a CSV file for your records.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

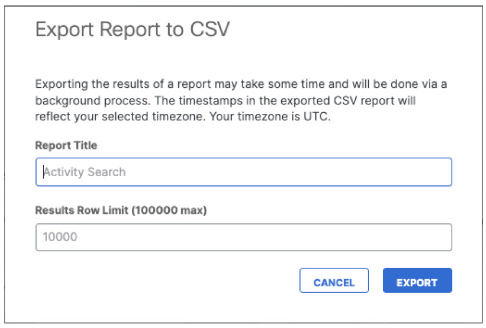
Procedure

1. Click **Download**.



2. Give your report a title and click **Export**.

> **Note**
>
> Data is limited to 100,000 rows when exporting to CSV.



3. When you click **Export**, you are taken to the Exported Reports page. Click the download icon in the download column to download the CSV file.

76 Data Loss Prevention Report

Topics:

- Data Loss Prevention Report

Provides an overview of Data Loss Prevention Report in Cisco Secure Access, including Data Loss Prevention Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Data Loss Prevention Report

Describes Data Loss Prevention Report in Cisco Secure Access. Data violations detected through the Real Time rules SaaS API rules, AI Guardrails rules, and Email DLP rules are logged as part of the unified Events view of the Data Loss Prevention Report.

Data violations detected through the Real Time rules SaaS API rules, AI Guardrails rules, and Email DLP rules are logged as part of the unified Events view of the Data Loss Prevention Report.

The Data Loss Prevention reports window includes these tabs:

- Events
- Discovery

> **Note**
>
> Administrators with De-identification enabled will continue to see identifiable information in the Data Loss Prevention Report.

View Events

Provides instructions for completing the View Events workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Data Loss Prevention**
2. On the **Events** tab, select a time frame to view reports generated in a specific date range. You can also choose a custom date range.



3. Use the available **Filters** for better search results; choose from those listed below:

   File Size–Indicates the size of the file that triggered the event.

   Event Type–Indicates the type of violation that triggered the event: Real Time (for private or internet resources), SaaS API, AI Guardrails, Endpoint DLP or Email processed by Cisco Secure Email Threat Defense.

   Action–The action the system has applied to the content: blocked, deleted, monitored, quarantined, restored from quarantine, revoked access.

   Severity–The severity of the rule that triggered the event.

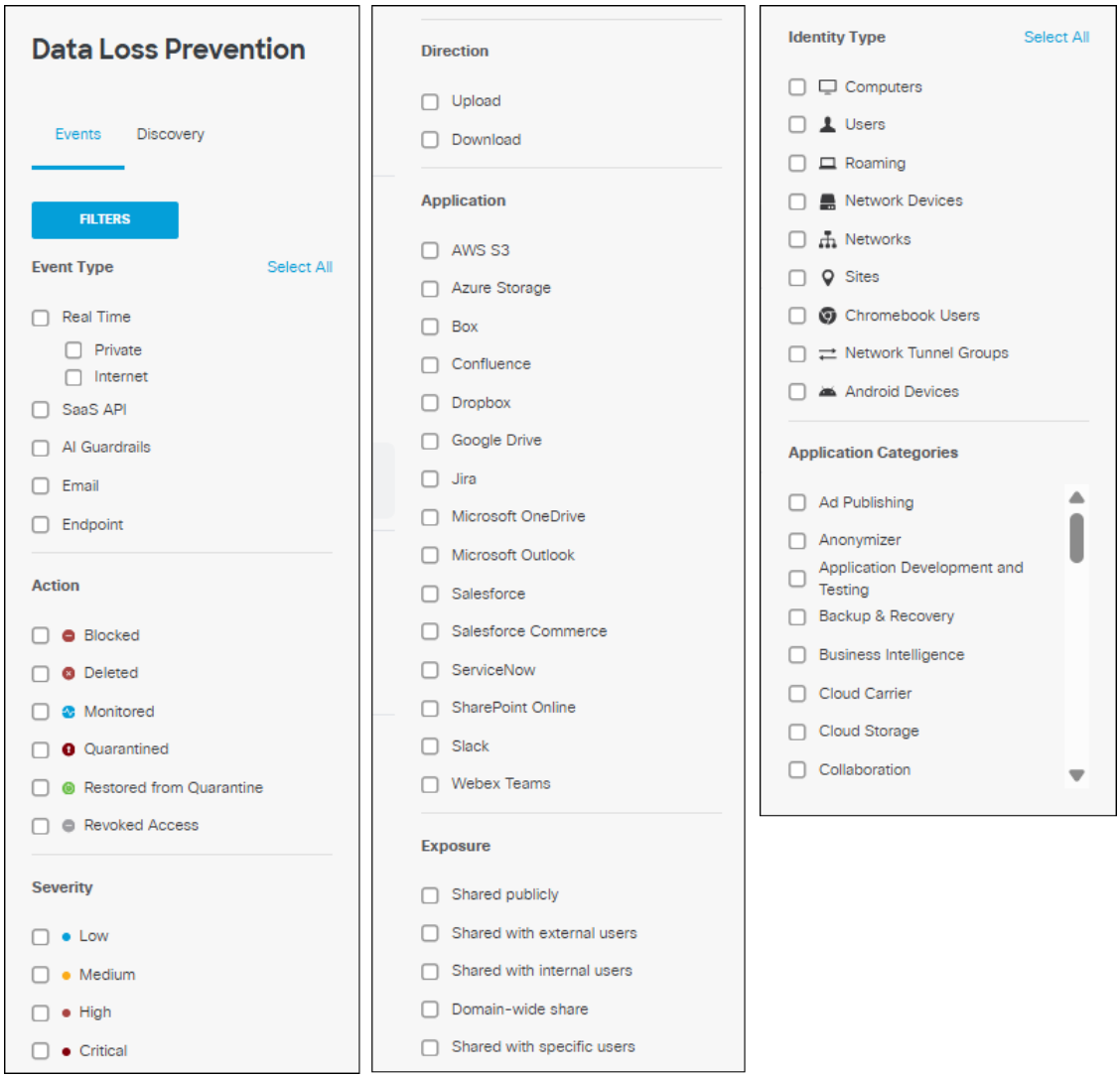
Direction–The direction of movement for the data that triggered the event.

Application–Application for which an SaaS API rule is applied.

Exposure–Exposure of the content scanned.

Identity Type–The type of identity involved in the event.

Application Categories–The category of the application involved in the event. This filter displays only events that occurred after this filter was added to Secure Access, in January of 2024.



4. Click the gear icon to customize and sort the columns of your report.

Event Type– Indicates the type of rule that triggered the event: Real Time, SaaS API, AI Guardrails, Endpoint DLP or Email DLP.

Severity–The severity of the rule that triggered the event.

Identity–The identity that made the request.

File Owner–The owner of the file that created the violation in the vendor. (For Email DLP, this displays "N/A.")

Event Actor– The user who performs an action that triggers a rule violation. (For Email DLP, this displays "N/A.")

File Name–The name of the file or attachment where a classification match was found. (This includes attachments to email messages, Jira pages and comments, and Confluence pages, but not attachments to comments on Confluence pages.)

- When content is found in a message, a post, or form data, the File name displays `Message`, `Content`, or `Form`.
- For Salesforce chatter posts, the **File Name** displays `Chatter Post`.
- For Salesforce sObjects, the **File Name** displays `SObject - object name`.
- For Confluence and Jira pages, **File Name** displays the title of the page.
- For comments on Confluence and Jira pages, **File Name** displays `Comment - > Page title`.
- For Salesforce Commerce objects, the **File Name** displays `<object type>:<object name>`.

Direction–The travel direction of the data that triggered the violation. For Salesforce Commerce, this displays "N/A."

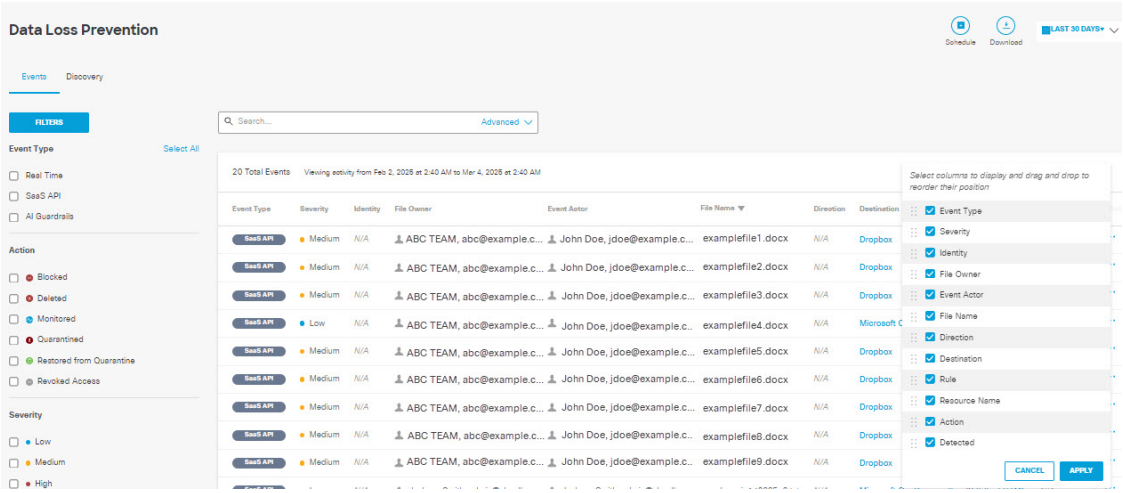
Destination–The destination where the content was scanned.

Rule–The rule that triggered the event.

Resource Name–For AWS S3 this displays the S3 bucket associated with the content that triggered the violation. For Azure Storage this displays the storage account or container associated with the content that triggered the violation. For other applications, this displays the Salesforce instance name.

Action–The action triggered by the rule on detecting a violation.

Detected–The date and time of detection.



5. Click the action menu icon (three dots) to view further details of an event. See View Details

---

View Event Details

Provides instructions for completing the View Event Details workflow in Cisco Secure Access. Click the action menu icon (three dots) for any event to view a menu of options.

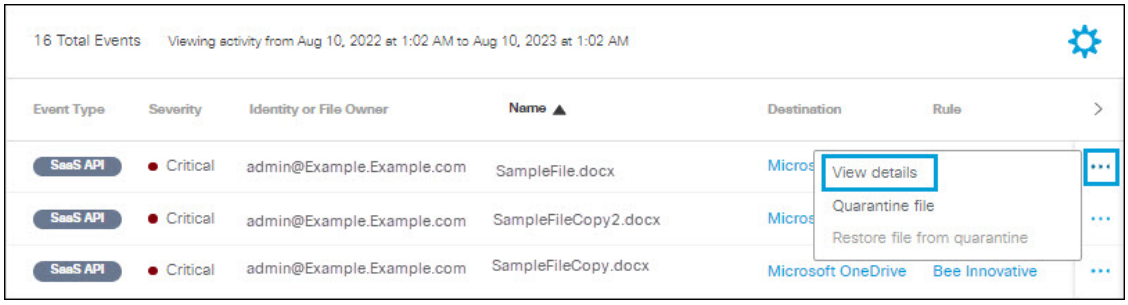
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Click the action menu icon (three dots) for any event to view a menu of options. Click **View details**.



2. The Event Details window displays some of the same content as the report table, with additional information which varies depending upon the Event Type:

Real Time Events

- **Detected**–The date and time the content was detected.
- **Action** –The action triggered by the rule on detecting a violation.
- **File Name**–The name of the file or attachment where a classification match was found. (This includes attachments to email messages, Jira pages and comments, and Confluence pages, but not attachments to comments on Confluence pages.)
  - When content is found in a message, a post, or form data, the File name displays `Message`, `Content`, or `Form`.
  - For Salesforce chatter posts, the **File Name** displays `Chatter Post`.
  - For Salesforce sObjects, the **File Name** displays `SObject - object name`.
  - For Confluence and Jira pages, **File Name** displays the title of the page.
  - For comments on Confluence and Jira pages, **File Name** displays `Comment - > Page title`.
- **Identity** –The identity that made the request.
- **Private Resource**–The private resource where the file was uploaded or posted.
- **Private Resource Group** – The private resource group where the file was uploaded or posted.
- **Destination URL**– For private resources or private resource groups, the URL where the file was uploaded or posted.
- **Destination Port**– For private resources or private resource groups, the port where the file was uploaded or posted.
- **Destination Protocol**– For private resources or private resource groups, the protocol used to upload or post the file.
- **Destination IP**– For private resources or private resource groups, the IP address where the file was uploaded to posted.
- **Application**–The application where the file was uploaded or posted.
- **Application Category**–The category for the application where the file was uploaded or posted.
- **Destination URL**–The URL of the destination for the event.
- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.

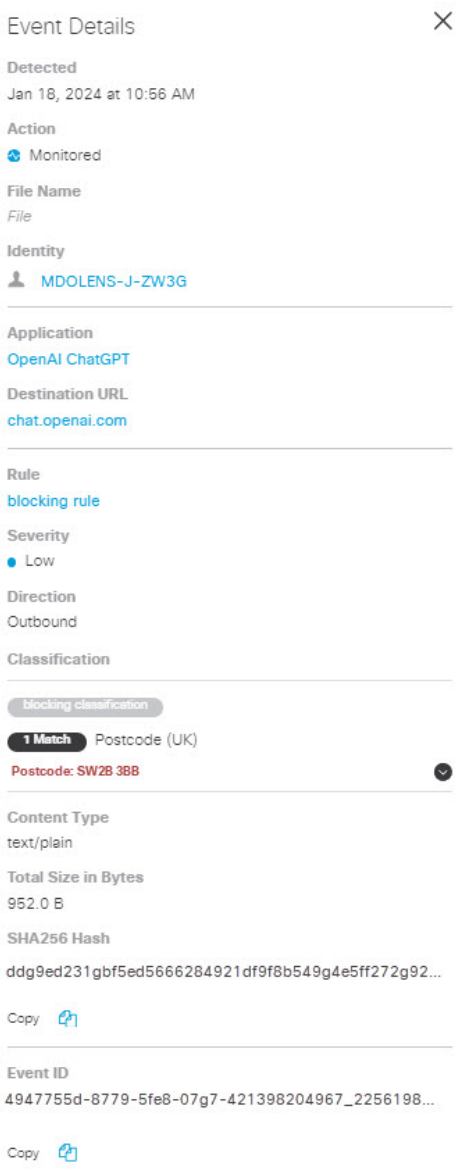
- **File Label**–File label names in the file's document properties. This includes Microsoft Office Document Properties, and AdobePDF Document Properties. For Microsoft 365 or Box tenants this includes Microsoft Office sensitivity labels . (Within the Box application these are referred to as classification labels.)

  For files detected with no labels, this field displays *Unclassified*.

- **Direction**–Direction of traffic.
- **Classification**–The classification that matched the content found in the event. Clicking the caret displays the excerpts where the matches were found. It also displays the threshold type and severity.

  > **Note**
  >
  > The match count displayed for Threshold classification denotes the total number of matches and the match count displayed for Unique Threshold classification denotes the number of unique matches.

- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file. (You may copy this using the **Copy** icon.)
- **Event ID**–A unique identifier for the event. (You may copy this using the **Copy** icon.)



SaaS API Events

The fields displayed vary depending on the platform associated with the event.

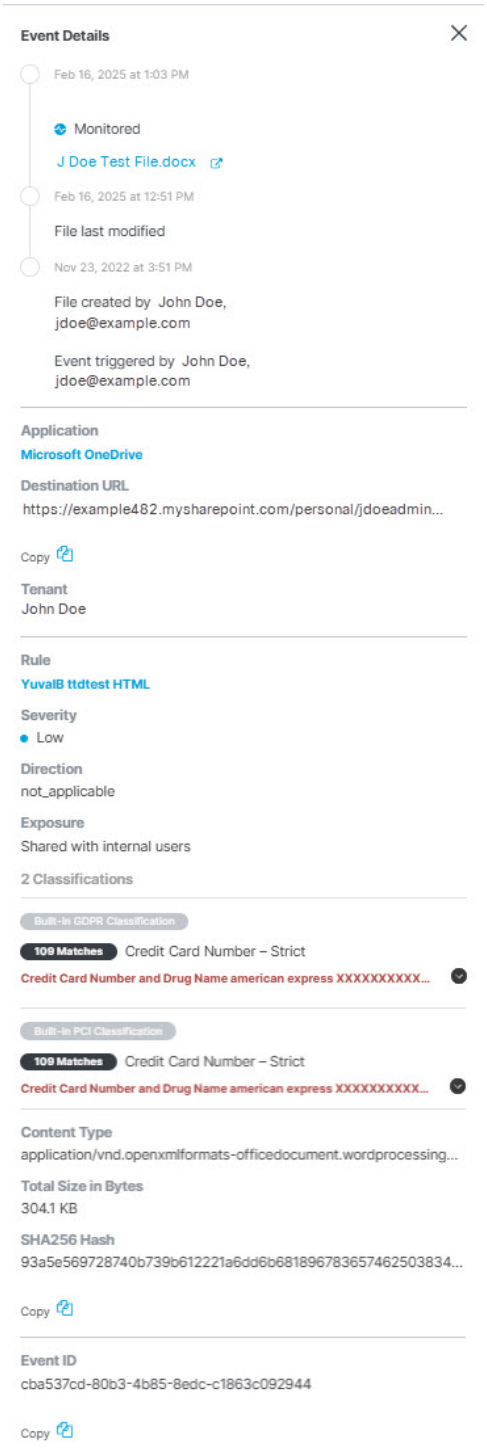
- A timeline of events associated with the file.
- **Application**–The application where the file was uploaded or posted.
- **Tenant**–The Secure Access tenant associated with the event.
- **Resource ID**– The URL for the resource associated with the content that triggered the violation. For Azure S3 the resource is an S3 bucket. For Azure Storage the resource is a storage account or container. For other applications, this displays the Salesforce instance name.
- **Resource Name**–For AWS S3 this displays the S3 bucket associated with the content that triggered the violation. For Azure Storage this displays the storage account or container associated with the content that triggered the violation. For other applications, this displays the Salesforce instance name.
- **Destination URL**–The URL of the destination for the event.

> **Note**
>
> (For some platforms, a single file or message can trigger multiple events that show the same Destination URL for each event.)

- **Direction**–The direction of the message or file that triggered the event: **Incoming** or **Outgoing**.

> **Note**
>
> For Outlook, this will always be **Outgoing**.

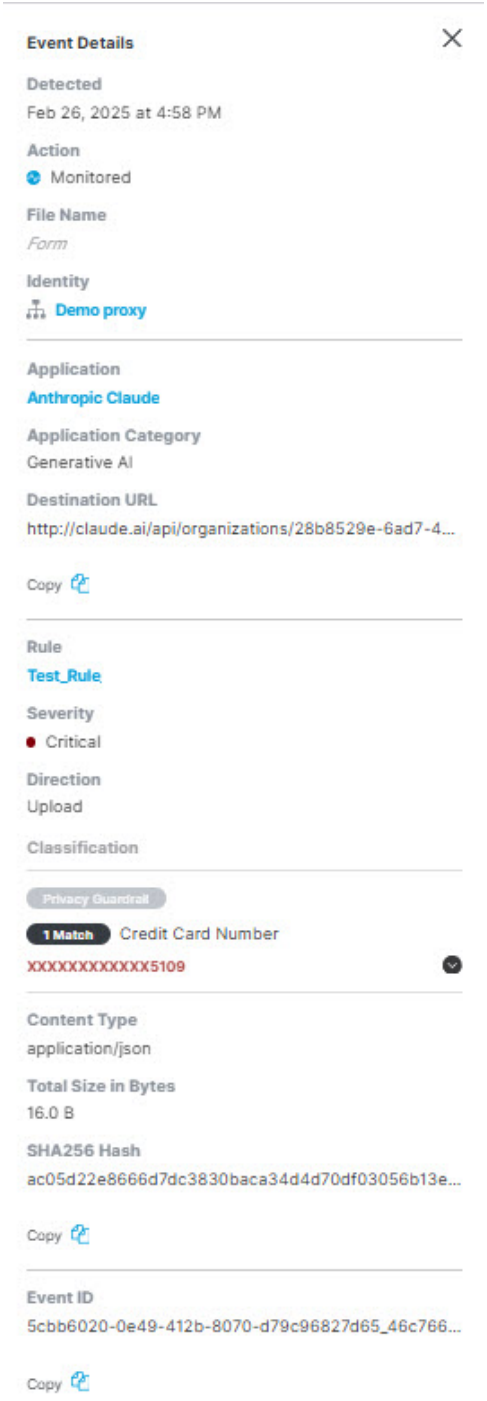
- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.
- **File Label**–File label names in the value of the file's document properties. This includes:
  - MIP and Titus labels in Microsoft Office Document Properties and AdobePDF Document Properties.
  - Microsoft Office sensitivity labels for Microsoft 365 or Box tenants. (Within the Box application these are referred to as classification labels.)
  - For files detected with no labels, this field displays *Unclassified*.
- **Exposure**–An indication of who can see the file–internal or external users.
- **Classification**–The classification that matched the content found in the event. Clicking the caret will display the excerpts where the matches were found.
- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file.
- **Event ID**–A unique identifier for the event.



AI Guardrails Events

- **Detected**–The date and time the content was detected.
- **Action**–The action triggered by the rule on detecting a violation.
- **File Name**–If the classification match is found in a prompt or response, this item displays *Form*. If the classification match appears within an embedded file, the file name appears here.
- **Identity**–The identity that made the request.

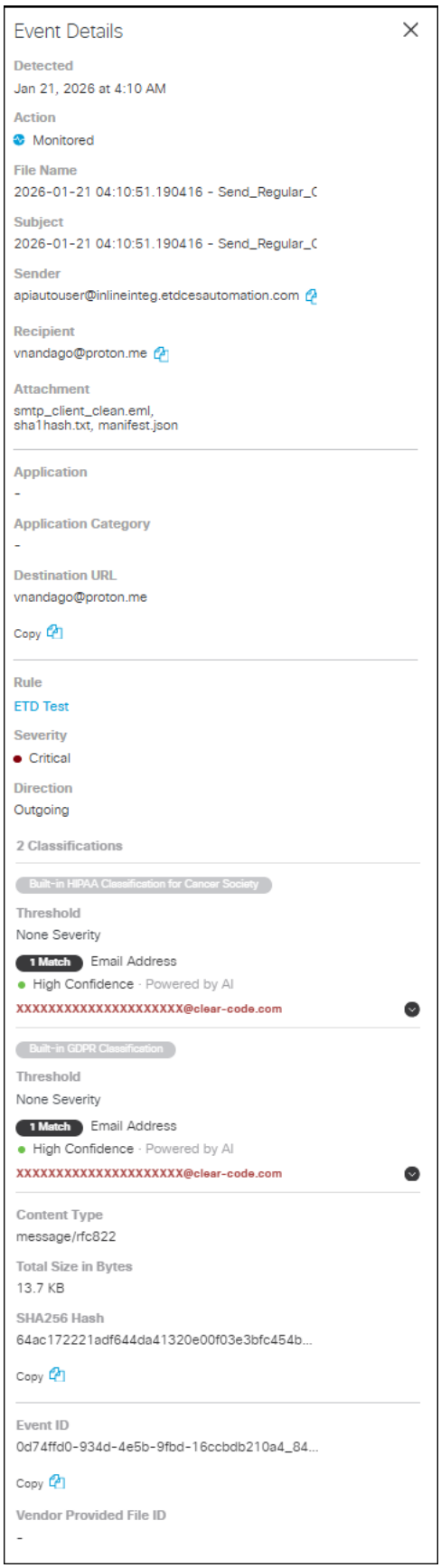
- **Application**–The application where the file was uploaded or posted.
- **Application Category**–The category for the application where the file was uploaded or posted.
- **Destination URL**–The URL of the destination for the event.
- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.
- **File Label**–File label names in the value of the file's document properties. This includes:
  - MIP and Titus labels in Microsoft Office Document Properties and AdobePDF Document Properties.
  - Microsoft Office sensitivity labels for Microsoft 365 or Box tenants. (Within the Box application these are referred to as classification labels.)
  - For files detected with no labels, this field displays *Unclassified*.
- **Direction**–Direction of traffic.
- **Classification**–The AI guardrails data classification that matched the content found in the event. Clicking the caret displays the excerpts where the matches were found.
- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file. (You may copy this using the **Copy** icon.)
- **Event ID**–A unique identifier for the event. (You may copy this using the **Copy** icon.)



Email DLP Events

- **Detected**–The date and time the content was detected.
- **Action**–The action triggered by the rule on detecting a violation.
- **File Name**–The name of the email that triggered the violation.
- **Subject**–The subject line of the email that triggered the violation.
- **Sender**–Email address of the sender.

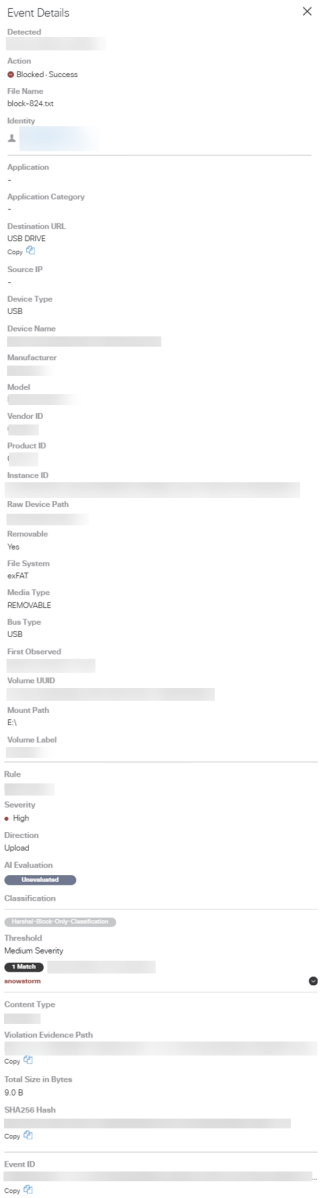
- **Recipient**–Email address of the recipient. (If there are multiple recipients, this displays as a comma-separated list.)
- **Application**–The application where the file was uploaded or posted.
- **Application Category**–The category for the application where the file was uploaded or posted.
- **Destination URL**–The URL of the destination for the event.
- **Rule**–The rule that triggered the event.
- **Severity**–The severity of the rule that triggered the event.
- **File Label**–File label names in the value of the file's document properties. This includes:
  - MIP and Titus labels in Microsoft Office Document Properties and AdobePDF Document Properties.
  - Microsoft Office sensitivity labels for Microsoft 365 or Box tenants. (Within the Box application these are referred to as classification labels.)
  - For files detected with no labels, this field displays *Unclassified*.
- **Direction**–Direction of traffic that triggered the event.
- **Classification**–The classification that matched the content found in the event. Clicking the caret displays the excerpts where the matches were found.
- **Content Type**–The type of data that triggered the event.
- **Total Size in Bytes**–The size of the file that triggered the event.
- **SHA256 Hash**–The unique SHA256 hash for the file. (You may copy this using the **Copy** icon.)
- **Event ID**–A unique identifier for the event. (You may copy this using the **Copy** icon.)
- **Vendor Provided File ID**– Applies to SaaS API events only.



Endpoint DLP Events

The fields displayed vary depending on the platform associated with the event.

- **File Name**–The name of the file on the endpoint that triggered a classification match:
  - For the printer channel, it holds `file name- printing application`, for example, allow-824.txt - Notepad.
  - For clipboard channel, it holds `application filename reading from clipboard` (PID), for example, chrome.exe (9096).
- **Application**–Available only for the Application File Access and Paste to Applications channels..
- **Destination URL**–This field contains the endpoint channel for the event such as BLUETOOTH or NETWORK SHARE.
- **Device Type**–The category of the destination device, for example, USB, printer, network device, application file access, media devices, or media portable devices.
- **Device Name**–The human-readable display name of the device.
- **Manufacturer**–The device manufacturer name.
- **Model**–The hardware model name of the device.
- **Serial Number**–The hardware serial number of the device.
- **Vendor ID**–The USB vendor ID.
- **Product ID**–The USB product ID.
- **Instance ID**– The OS device instance ID or hardware ID.
- **Raw Device Path**–The raw OS-level device path.
- **Removable**–Indicates whether the device is removable.
- **File System**–The file system type of the device.
- **Media Type**– The physical media category of the device, for example, removable, SD, HDD, or virtual.
- **Bus Type**–The bus interface type of the device.
- **First Observed**–The ISO-8601 or epoch time stamp indicating when the device was first observed.
- **Mount Options**– The OS mount options for the device volume.
- **Volume UUID**–The UUID of the mounted volume.
- **Mount Path**–The file system path where the device is mounted.
- **Volume Label**–The display label of the mounted volume.
- **Share Name**– The network share name.
- **Server FQDN**– The fully qualified domain name of the file server.
- **Protocol**–The network protocol used to access the share.
- **Print Server**–The hostname or IP address of the print server.
- **Print Type**–The type of the printer, for example, local, network, virtual.
- **Print To File**–Indicates whether the print job was directed to a file.
- **IP Address**–The IP address of the device.
- **Hostname**– The hostname of the device.



Delete File

Provides instructions for completing the Delete File workflow in Cisco Secure Access. For SaaS API events on Webex Teams and Slack, when a message is monitored and a rule violation is detected, you can manually delete the message or file.

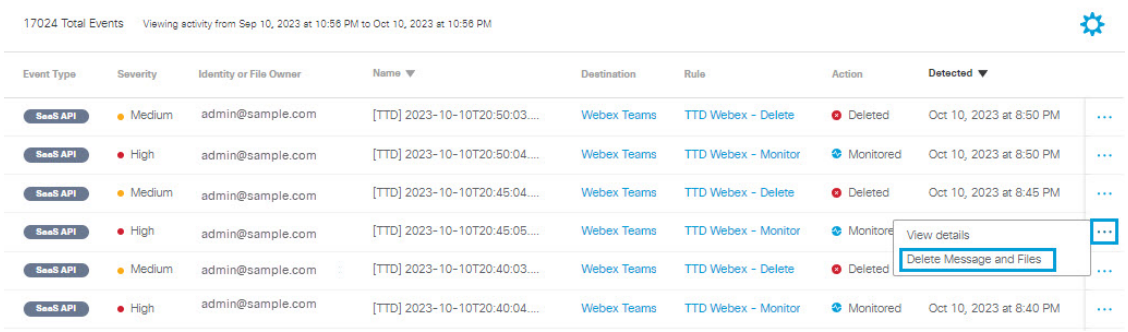
For SaaS API events on Webex Teams and Slack, when a message is monitored and a rule violation is detected, you can manually delete the message or file.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Click the action menu (three dots) for any Webex Teams event that is not marked **Deleted** to view a menu of options. Click **Delete Message and Files**.



2. Click **Delete** to confirm.

Quarantine File

Provides instructions for completing the Quarantine File workflow in Cisco Secure Access. For SaaS API events on Microsoft OneDrive, SharePoint Online, Box, Dropbox, Salesforce (files only), ServiceNow, or Google Drive, when a file is monitored and a rule violation is detected, you can manually quarantine the file.

For SaaS API events on Microsoft OneDrive, SharePoint Online, Box, Dropbox, Salesforce (files only), ServiceNow, or Google Drive, when a file is monitored and a rule violation is detected, you can manually quarantine the file.

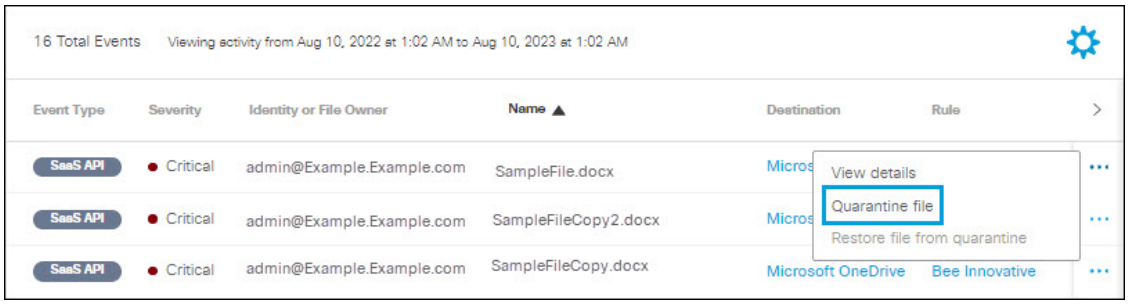
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

1. Click the action menu icon (three dots) for any event to view a menu of options. Click **Quarantine file**.



2. Click **Quarantine**.

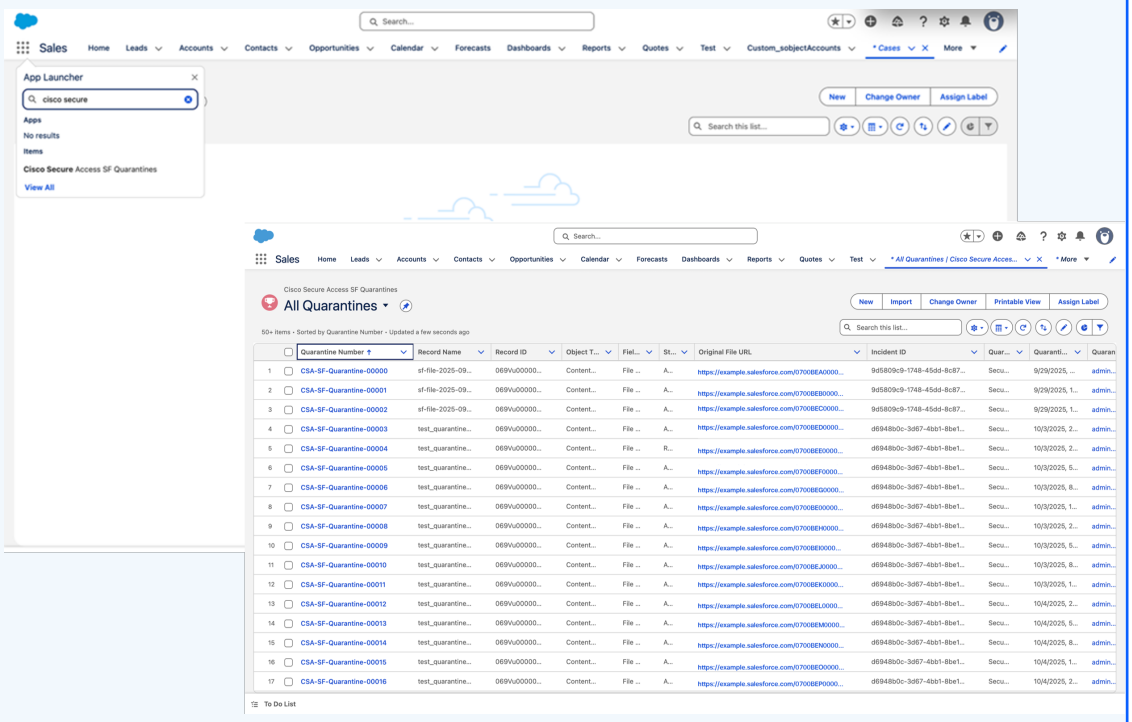


Note

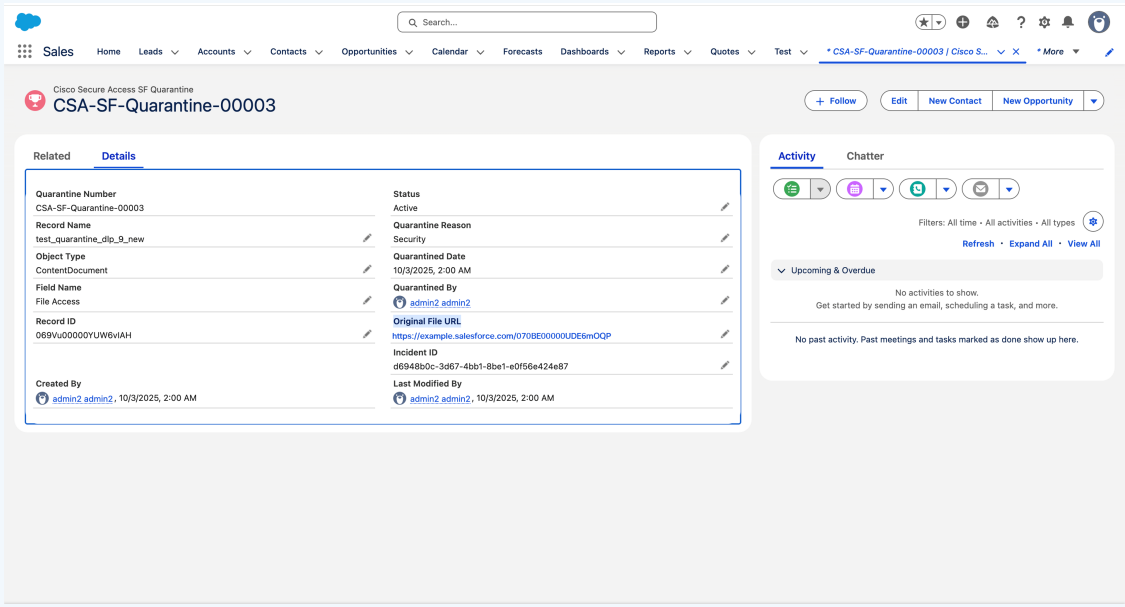
- For Microsoft OneDrive, SharePoint Online, Box, Dropbox, or Google Drive:
  - The file identified as exposing sensitive data is moved to the Cisco_Quarantine/DLP folder Secure Access created in the root path of the Global Admin who authorised the tenant.
  - The user who authorizes access to Secure Access will have access to the quarantine folder. All other accesses and collaborators are removed. Thus, we recommend that the admin add the relevant DLP Admins as additional collaborators to the folder.
- For ServiceNow:
  - The file identified as exposing sensitive data is moved to a table named **Cisco_Quarantine_Malware** which can be access only by the admin user who authorized the ServiceNow tenant.
  - A footprint is attached to the notes\activities area of the table the file was originally attached to. This footprint will notify users that the file has been identified as malware, and for more information they should contact their administrator.
- For Salesforce:

  Secure Access applies the **Quarantine** response action to files only (including those attached to chatter posts). Choose **Quarantine** to:

  - Remove all collaborators, and change the file owner to the Salesforce admin who has performed the authorization, and who has been assigned the permission set for the quarantine app. In Salesforce, the admin can see a list of quarantined files by using the App Launcher to search for "Cisco Secure Access SF Quarantine," then selecting the **All Quarantines** option.

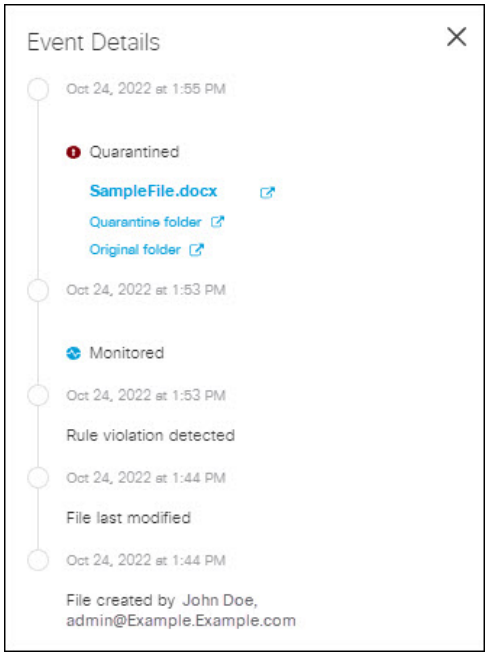


  Click on the listing for an individual file to see the information about it:



- Replace the file in its original location with a text file named ***filename*_Cisco_Quarantined.txt** explaining to the original file owner that the file is identified as malware and for more information to contact their organization administrator.

3. The file is now quarantined. For platforms other than Salesforce, under Events Details, click **Quarantine Folder** to navigate to the quarantined folder.



Restore File from Quarantine

Provides instructions for completing the Restore File from Quarantine workflow in Cisco Secure Access. When a quarantined file is restored, the original location of the file, ownership and permissions are also restored.

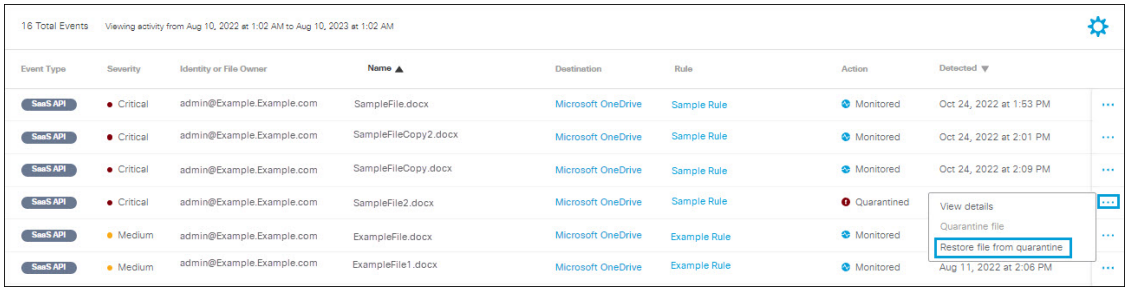
When a quarantined file is restored, the original location of the file, ownership and permissions are also restored.

Before you begin

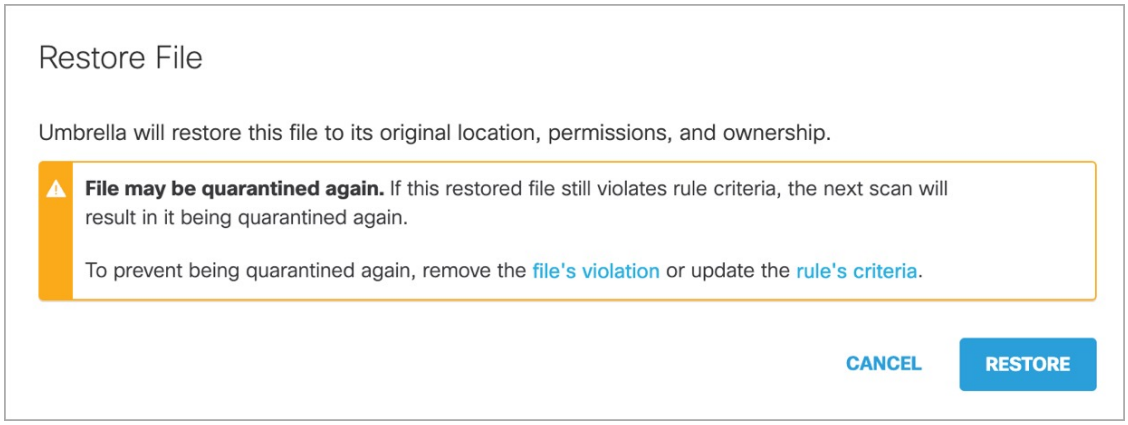
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

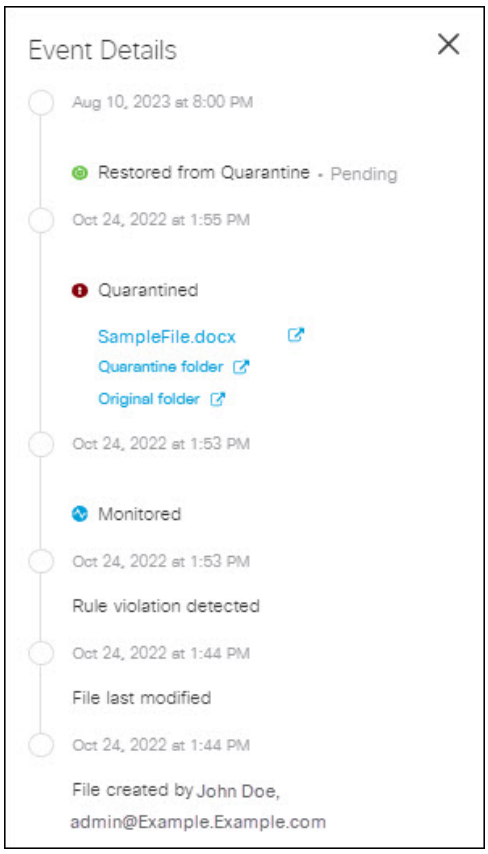
1. Click the action menu icon (three dots) for any event to view a menu of options. Click **Restore file from quarantine**.



2. Click **Restore** to proceed.



3. The file is now restored. You can access the file in its original location under **Event Details**.



Note

If your DLP rules process files from Microsoft OneDrive, SharePoint Online, Box, Dropbox, Salesforce, ServiceNow, or Google Drive and you restore a quarantined file that still violates rule criteria, the system will quarantine that file again. To prevent the system from quarantining the file again, remove the file's violation, or update the rule's criteria.

Use Advanced Search

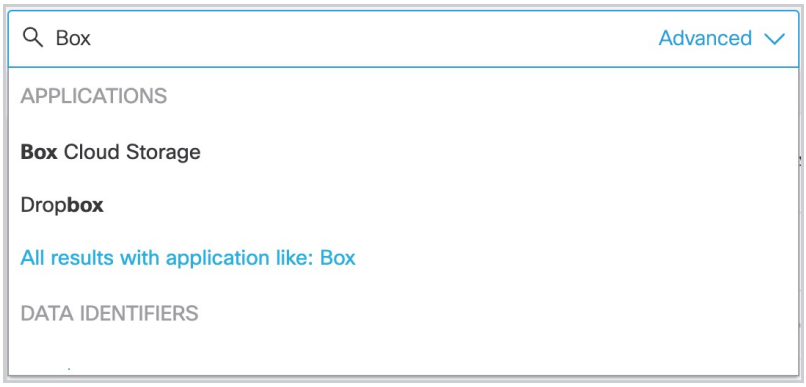
Provides instructions for completing the Use Advanced Search workflow in Cisco Secure Access. You can search the Data Loss Prevention Reports by keywords to find specific events.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. You can search the Data Loss Prevention Reports by keywords to find specific events.



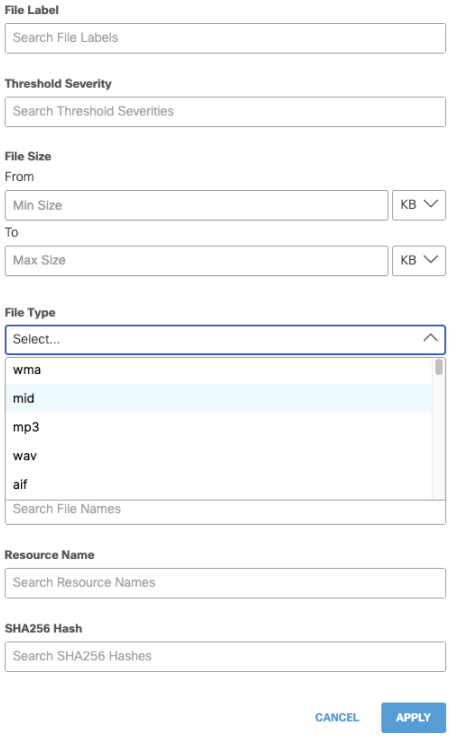
2. Alternatively, click **Advanced** in the search bar to bring up the advanced search. You can search the report choosing any of the following event criteria:
   - **Identity**
   - **File Owner**
   - **Event Actor**
   - **Event ID**
   - **Destination URL**
   - **Application**
   - **Direction** (Applies only to some applications, such as OpenAI API and OpenAI ChatGPT.)
   - **Tenant** (Does not apply to events for Email integrated with Cisco's Secure Email Threat Defense.)
   - **Rule**
   - **Data Classification**
   - **Tenant Profile** For realtme rules only.
   - **Tenant ID** For realtime rules only.
   - **File Label**

     You can search for file label names in the value of the file's document properties. This includes:
     - MIP and Titus labels in Microsoft Office Document Properties and AdobePDF Document Properties.
     - Microsoft Office sensitivity labels for Microsoft 365 or Box tenants. (Within the Box application these are referred to as classification labels.)

     You cannot use this field to search for files that have no labels associated with them.
   - **Threshold Severity** Represents the total number of occurrences of a data identifier that must be detected in a document for Secure Access to generate an incident.
   - **File Size** (When searching for files meeting size criteria, You can choose to include only files that are greater than a minimum size you specify, or include files that are within a range of sizes you specify. (If you specify a maximum size without specifying a minimum size, the minimum size defaults to 0.) You can specify file sizes in KB or MB. The system scans only up to the first 50 MB of plain text for any file; if you specify a minimum size > 50 MB, Secure Access does not scan for other criteria.)
   - **File Type**

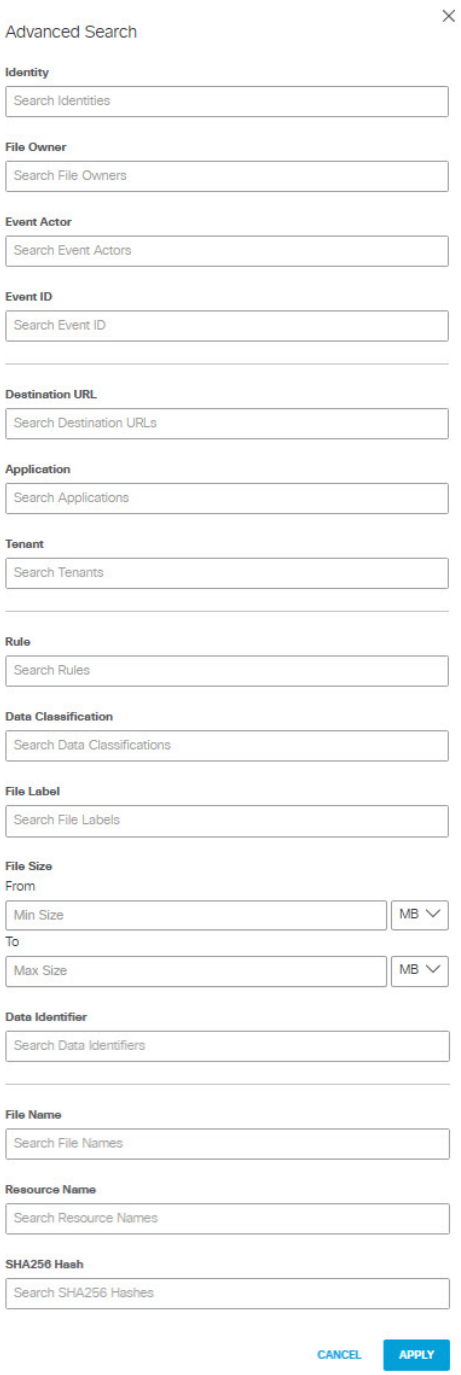
     For Real Time, AI Guardrails, and Email DLP rules, you can choose to include the DLP violations of a particular file type. You can choose to include or exclude DLP violations for specific file types. This helps you to focus on files

that may cause higher security risk. It helps reduce the processing of insignificant events and improve operational efficiency.



- **Data Identifier**
- **File Name**
- **Resource Name** (applies to AWS S3 or Azure Storage tenants only)
- **SHA256 Hash**

3. Click **Apply** to apply the filters to the report.



Discovery

Describes Discovery in Cisco Secure Access. It summarizes the related concepts, procedures, and operational details presented throughout the topic for administrators working with the service.

View a Discovery Scan

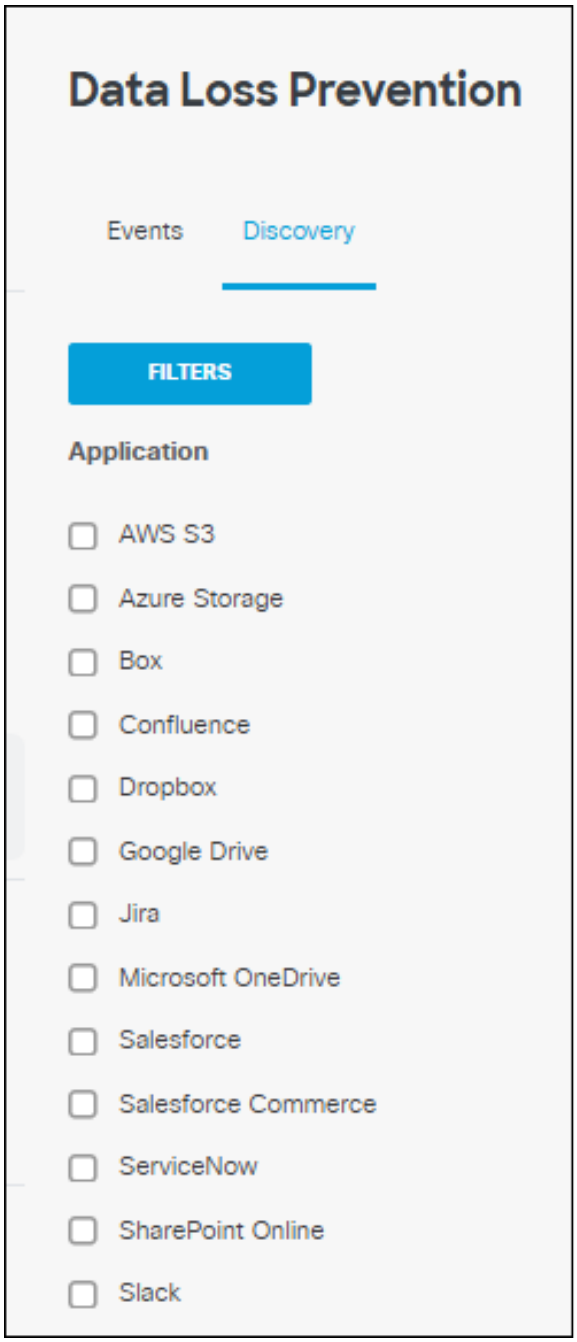
Provides instructions for completing the View a Discovery Scan workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

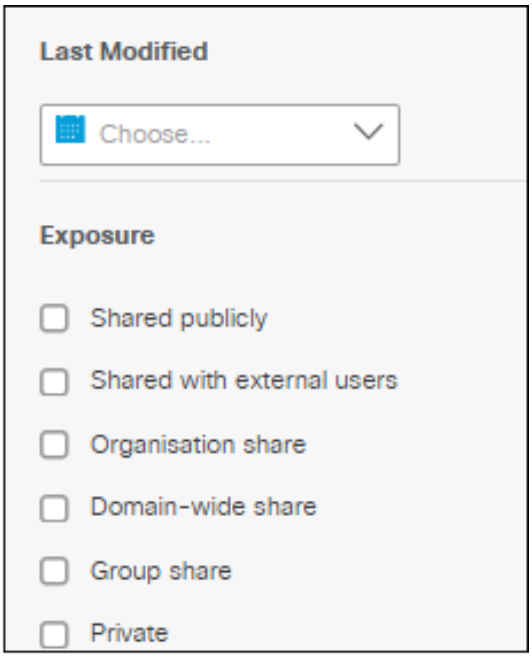
Before you begin

You must initiate a discovery scan as described in Discovery Scan.

Procedure

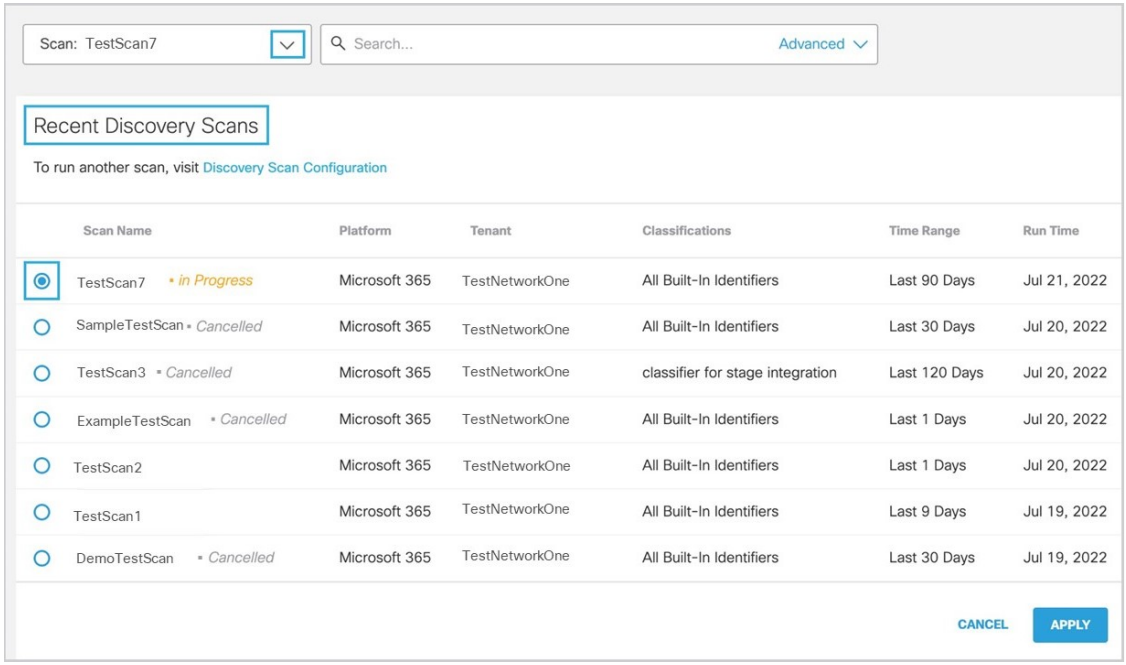
1. Navigate to **Monitor** > **Reports** > **Data Loss Prevention**. Click the **Discovery** tab.
2. Use **Filters** to filter the data by **Application**, **Last Modified**, and **Exposure**.



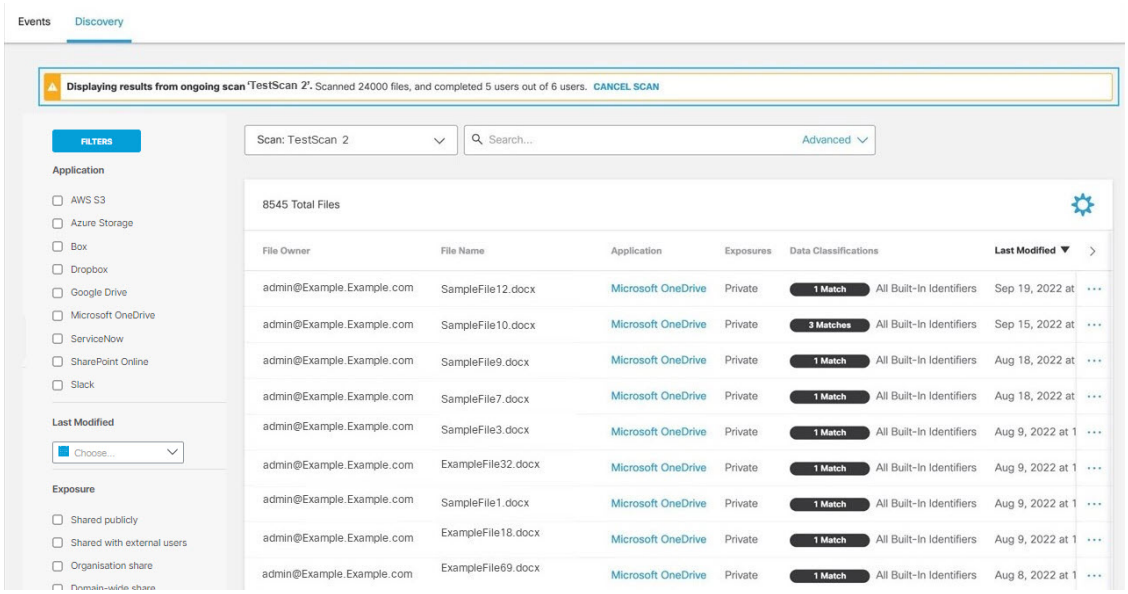


3. Choose a **Scan** from the drop-down. Click **Apply** to view the details.

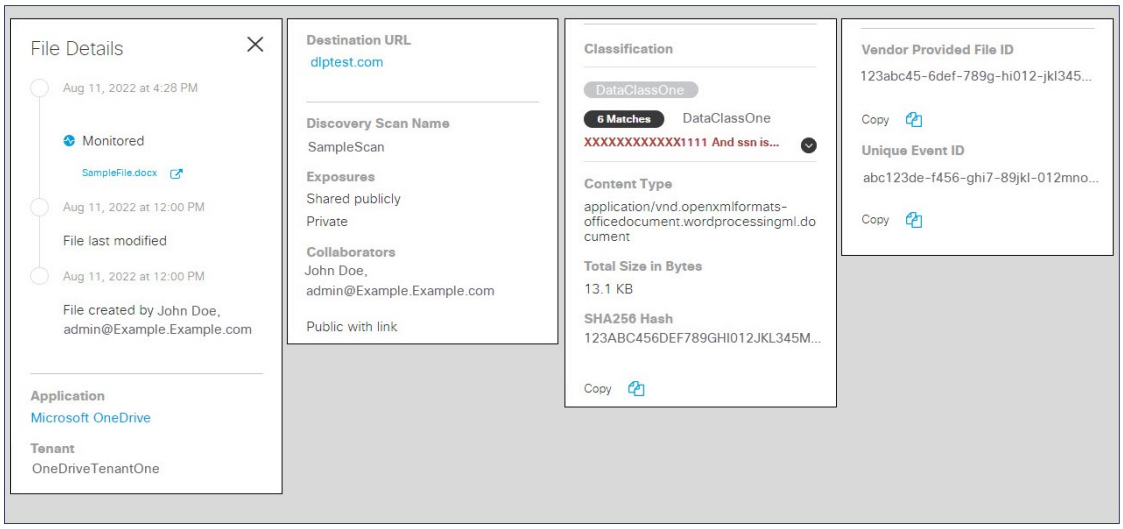
> **Note**
>
> Up to 10 recent scans are displayed. The next triggered Discovery Scan removes the oldest scan results in the list.



4. If there is an ongoing scan, the results are displayed. Click **Cancel Scan** to stop the ongoing scan. (You can only run one scan at a time.)



5. Click the action **menu icon** (three dots) to view further details of a file.


File Details
Aug 11, 2022 at 4:28 PM
Monitored
SampleFile.docx
Aug 11, 2022 at 12:00 PM
File last modified
Aug 11, 2022 at 12:00 PM
File created by John Doe, admin@Example.Example.com
Application
Microsoft OneDrive
Tenant
OneDriveTenantOne
Destination URL
dlptest.com
Discovery Scan Name
SampleScan
Exposures
Shared publicly
Private
Collaborators
John Doe, admin@Example.Example.com
Public with link
Classification
DataClassOne
6 Matches
DataClassOne
XXXXXXXXXXX1111 And ssn is...
Content Type
application/vnd.openxmlformats-officedocument.wordprocessingml.document
Total Size in Bytes
13.1 KB
SHA256 Hash
123ABC456DEF789GHI012JKL345M...
Copy
Vendor Provided File ID
123abc45-6def-789g-hi012-jkl345...
Copy
Unique Event ID
abc123de-f456-ghi7-89jkl-012mno...
Copy

77 Data Security Posture Management Report

Topics:

- Overview
- Data Catalogue
- Insights
- Analytics

Provides an overview of Data Security Posture Management Report in Cisco Secure Access. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Data Security Posture Management (DSPM) provides visibility into sensitive data across supported cloud storage and collaboration platforms. It helps you identify where sensitive data exists, understand the exposure and ownership context, and prioritize remediation actions based on risk.

Overview

Describes Data Security Posture Management in Cisco Secure Access. The Data Security Posture Management overview page combines posture, recommendations, scan coverage, risky asset owners, high-risk assets, and analytics.

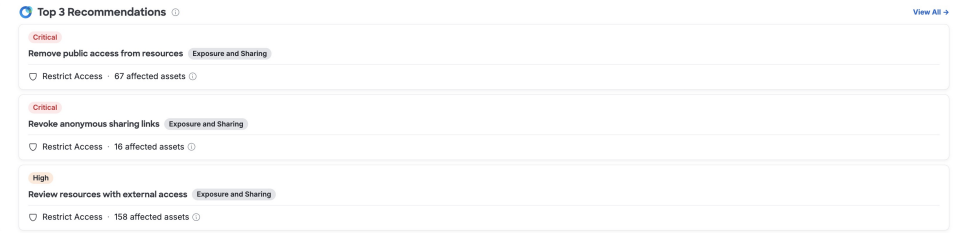
The Data Security Posture Management overview page combines posture, recommendations, scan coverage, risky asset owners, high-risk assets, and analytics. Use this page to identify the highest-priority investigation paths.

Navigate to **Monitor** > **Reports** > **Data Security Posture Management**.

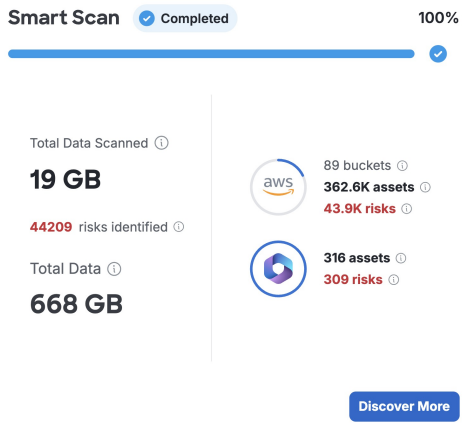
- **Posture Score**: This widget provides a consolidated view of the organization's current data security posture. The score is supported by four operational dimensions.



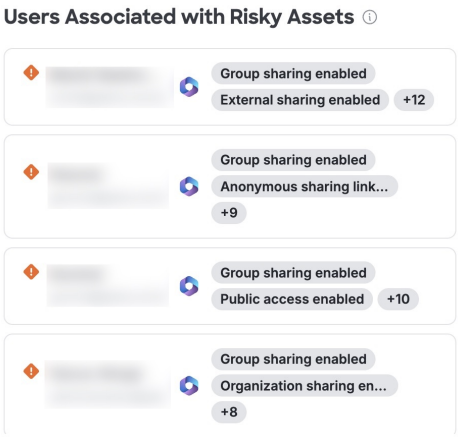
- **Top Recommendations**: Recommendations convert correlated findings into remediation-oriented actions. Each recommendation includes a severity, action statement, risk category, remediation intent, and affected asset count.



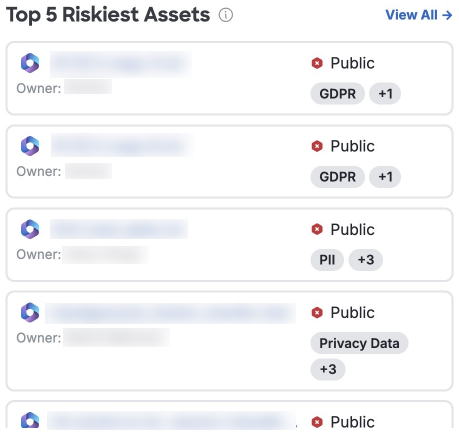
- **Smart Scan**: This widget shows discovery progress and scan coverage. It indicates whether posture and catalogue results are based on completed or in-progress scanning.



- **Users Associated with Risky Assets**: This widget lists asset owners associated with detected exposure conditions or sensitive data classifications. The widget supports ownership-driven investigation, and accountability.



- **Top Riskiest Assets**: This widget provides a prioritized list of assets that require attention. Each entry combines owner, exposure state, and classification tags.

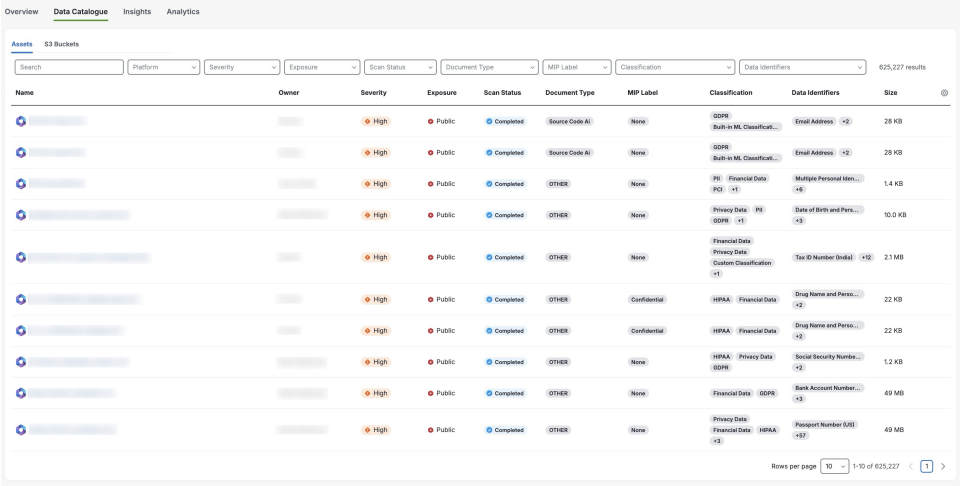


Data Catalogue

Describes Data Catalogue in Cisco Secure Access. Use it to investigate files, S3 buckets, classifications, exposure, scan status, and data identifiers.

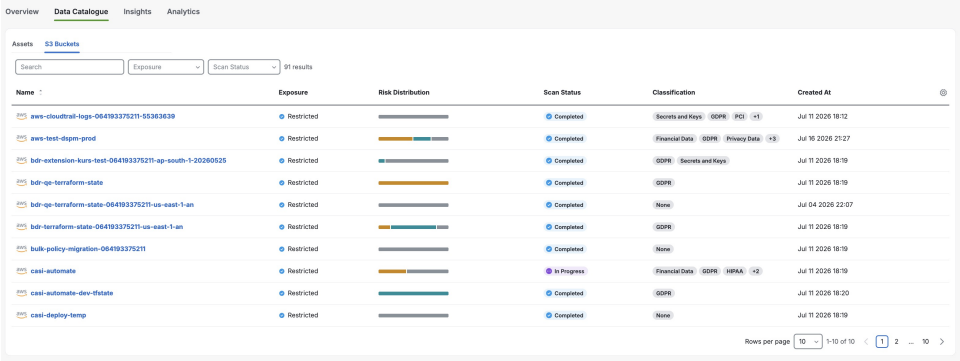
The Data Catalogue is the evidence layer behind posture, recommendations, and insights. Use it to investigate files, S3 buckets, classifications, exposure, scan status, and data identifiers.

- The **Assets** tab lists individual files discovered by DSPM and supports filtering by platform, severity, exposure, scan status, classification, document type, MIP label, and data identifiers.



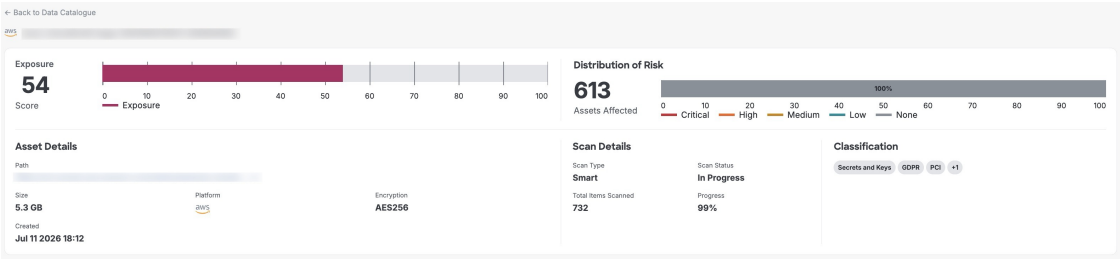
Filter	Function
Search	Find assets by name or partial text.
Platform	Filter by data source.
Severity	Filter assets by severity level.
Exposure	Filter by exposure state.
Scan Status	Filter by scan progress.
Classification	Filter by sensitive data category.
Data Identifiers	Filter by specific detected data identifiers.
Name	Select asset name to open details.
Owner	Owner or associated user.
MIP Label	Filter assets based on applied Microsoft Information Protection sensitivity labels.
Document Type	Filter assets based on the classified document type. **Note** Document Type is generated using Meta Llama 3.
Size	Asset size.

- The **S3 Buckets** tab provides a resource-level view for AWS S3. This view focuses on storage entities and their exposure, risk distribution, scan status, classifications, and timestamps.



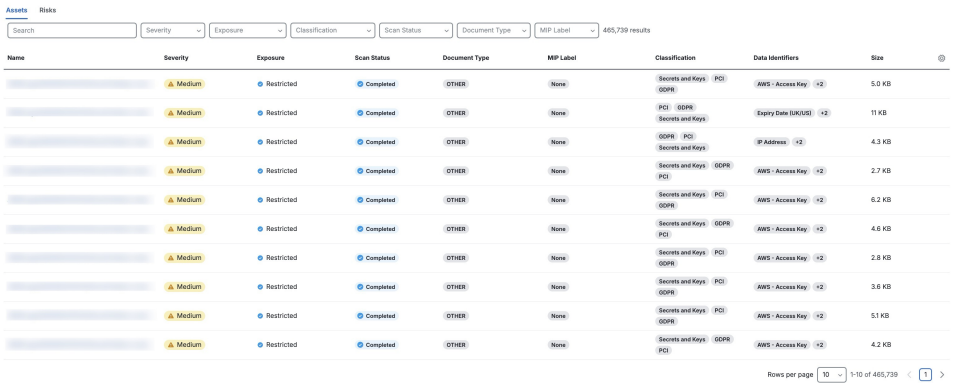
Function	Filter
Search	Find a bucket by name.
Exposure	Filter buckets by exposure state.
Scan Status	Filter buckets by scan status.
Risk Distribution	Visual distribution of risk within the bucket.
Classification	Summary of sensitive classifications detected in the bucket.
Modified At / Created At	Bucket timestamps captured during discovery.

- **S3 Bucket Details**: This page provides context for a single S3 bucket. It shows the bucket exposure score, risk distribution, asset details, scan details, and classifications found within the bucket.



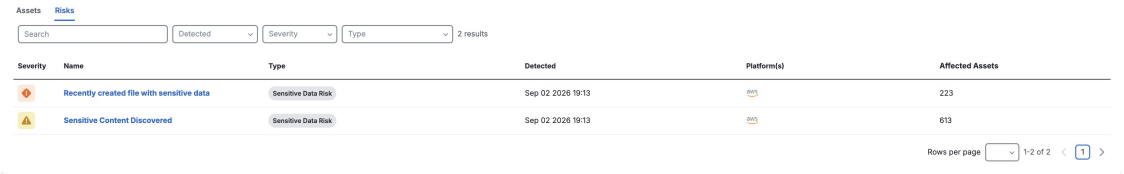
Section	Purpose
Exposure score	Numeric exposure score for the bucket.
Distribution of Risk	Breakdown of risks in the bucket by severity.
Asset Details	Path, size, platform, encryption, creation date, and last modified date.
Scan Details	Scan type, scan status, total items scanned, and progress.
Classification	Sensitive data categories detected in the bucket.

- The **Assets** tab within a selected s3 bucket lists files discovered within the bucket. Use this view to identify the specific files that drive bucket-level risk or classification.



Filter	Function
Name	File path or object name.
Severity	Severity derived from risk context.
Exposure	Exposure state for the file or object.
Scan Status	File scan status.
Document Type	Filter assets based on the classified document type. **Note** Document Type is generated using Meta Llama 3.
MIP Label	Filter assets based on applied Microsoft Information Protection sensitivity labels.
Classification	Sensitive data classification found in the file.
Data Identifiers	Specific identifiers detected in the file.
Number of Risks	Count of risks related to the file.
Size	File size.

- The **Risks** tab shows risk findings related to the selected bucket. Use this tab to understand the risk category, detection time, affected platform, and number of related objects.



Insights

Describes Insights in Cisco Secure Access. Use it to understand which types of risk dominate the environment and how many objects are affected.

The Insights page correlates discovered findings into risk categories and recommendations. Use it to understand which types of risk dominate the environment and how many objects are affected.

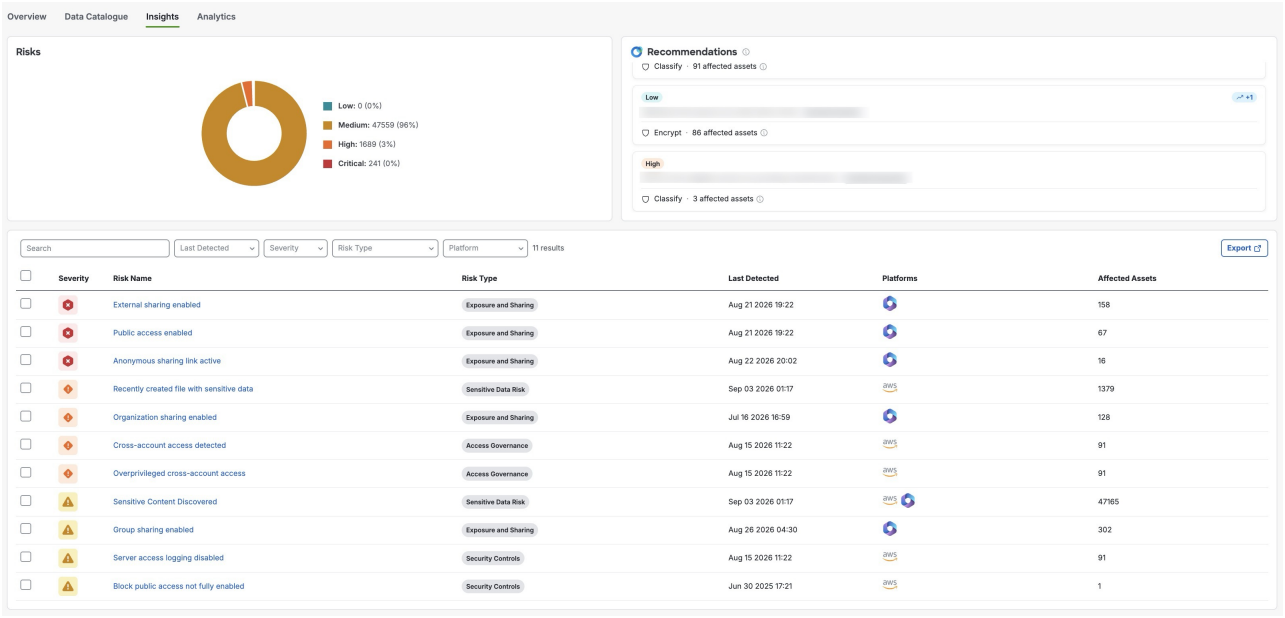
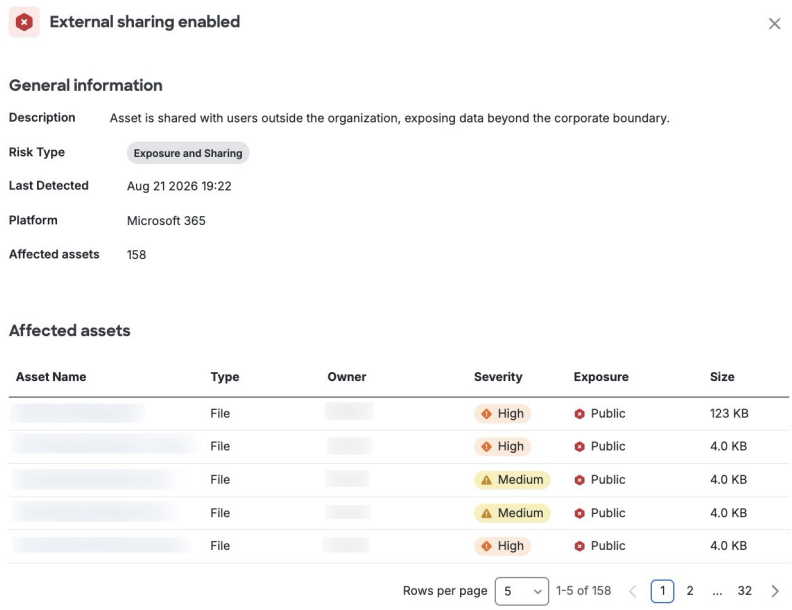


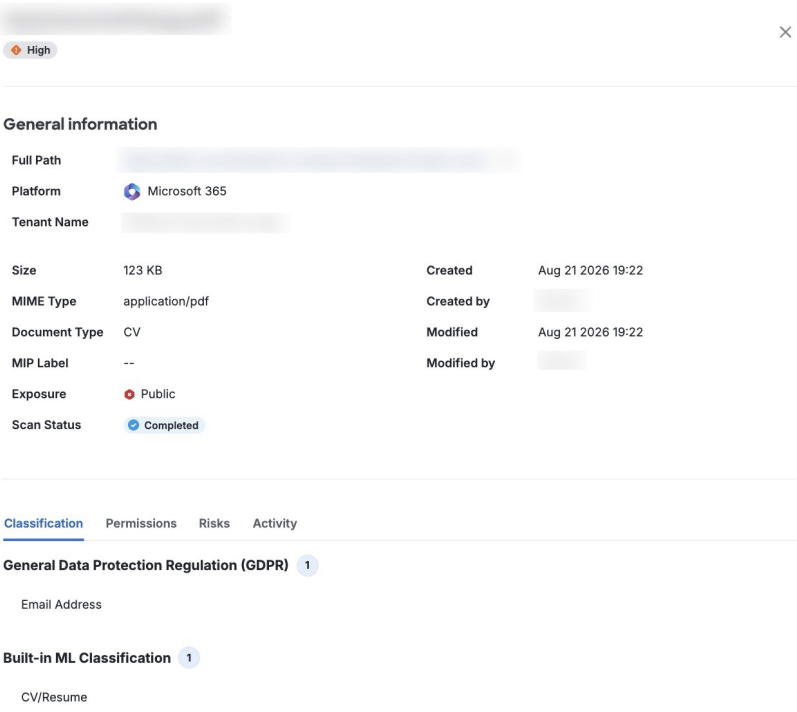
Table 35: Insights Overview

Pane	Purpose
Risks chart	Shows the severity distribution of detected risks.
Recommendations	Highlights prioritized actions based on risk correlation.
Search and filters	Filter risks by detected state, severity, type, and platform.
Risk Table	Lists risks by severity, name, type, detection time, platforms, and related objects.
Export	Exports the currently listed risk data for reporting or offline analysis.

- The **Risk detail panel** explains a selected risk and lists related objects. A classification becomes actionable when it is tied to platforms, detection time, related object count, and affected assets.



- The **Asset detail panel** provides evidence for a single file. It includes general information, exposure, scan status, owner and platform metadata, and tabs for classification, risks, permissions, and activity.

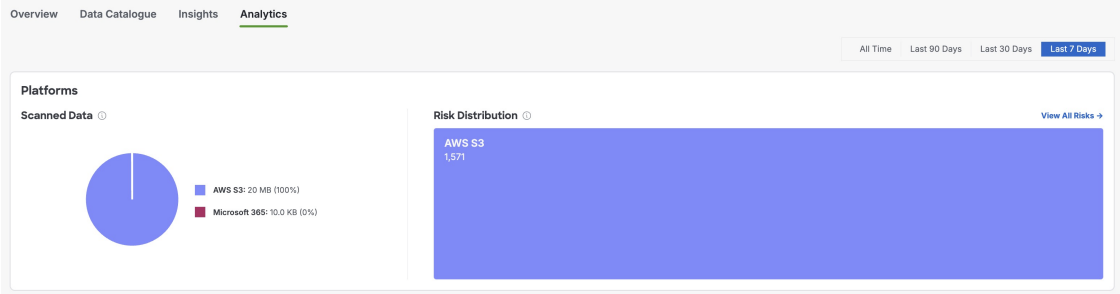


Analytics

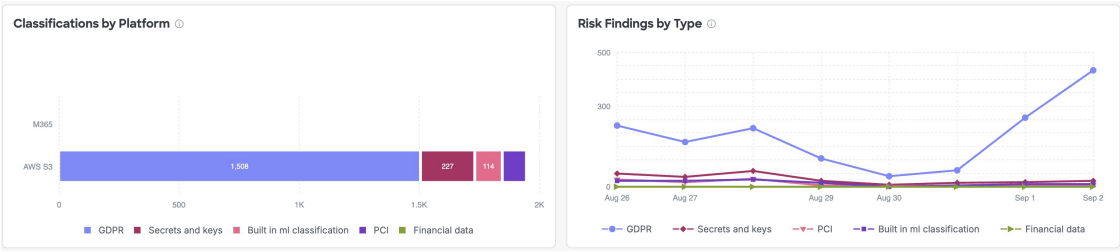
Describes Analytics in Cisco Secure Access. Use it to track scanned data, risk distribution, classification patterns, exposure issues, and risk findings across platforms over time.

The Analytics section is the trend and distribution views for DSPM. Use it to track scanned data, risk distribution, classification patterns, exposure issues, and risk findings across platforms over time.

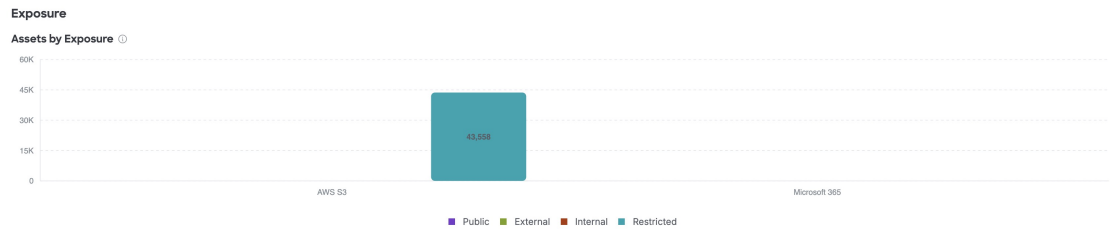
- **Platforms and Risk Distribution**: These analytics compare scanned data and risk distribution across supported platforms. They help you assess whether risk is concentrated in cloud storage, collaboration surfaces, or both.



- **Classification and Risk by Type**: Classification analytics show detected sensitive data categories by platform. Risk-by-type trends show how risk categories change over time. Use these views to identify dominant data types and risk trends.



- **Exposure**: Exposure analytics summarize sharing and accessibility conditions that contribute to posture risk.



78 Events Report

Topics:

- Events Report

Provides an overview of Events Report in Cisco Secure Access, including Events Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Events Report

Describes Events Report in Cisco Secure Access. In today's complex security environments, understanding the full journey of network traffic across multiple security services can be challenging, often requiring manual correlation of disparate logs.

In today's complex security environments, understanding the full journey of network traffic across multiple security services can be challenging, often requiring manual correlation of disparate logs. The Cisco Secure Access Events Report revolutionizes this by providing unified, correlated visibility across all security and network events in your environment.

At its core, the report leverages a unique Event Correlation ID that intelligently stitches together every stage of a traffic flow. This ID is generated at the very inception of a network connection, typically based on its unique 5-tuple (source IP, source port, destination IP, destination port, and protocol). As the traffic then traverses your security stack, this same Event Correlation ID is consistently propagated across various enforcement points. For instance:

- When a packet first hits the Firewall, the Event ID is assigned.
- If that traffic is subsequently handed off to the Secure Web Gateway (SWG) for web filtering, the same ID is carried over.
- Should an Intrusion Prevention System (IPS) inspect the traffic or a Decryption engine process it, their respective logs will also bear this identical ID.
- Even for Zero Trust Access (ZTA) events, this ID ensures a continuous trace.

This powerful service chaining mechanism transforms what would typically be fragmented logs from different services into a clear, cohesive, end-to-end narrative of the traffic's journey from source to destination. This allows you to effortlessly trace the complete lifecycle of a single user request, understanding every security control applied and every action taken along its path.

This comprehensive view empowers you to:

- **Streamline Troubleshooting:** Quickly pinpoint the exact point where an issue occurred, whether it's a block, an allow, or an isolation event, significantly reducing investigation time.
- **Verify Policy Enforcement:** Confidently confirm that your intent-based security policies are being applied correctly and consistently across all services.
- **Enhance Compliance Activities:** Maintain a complete and auditable record of all network activities, providing the detailed insights needed for regulatory requirements.
- **Perform Offline Traffic Flow Analytics:** Export detailed correlated data for in-depth analysis, custom reporting, and automated processing.

By providing a holistic perspective aligned with your intent-based security policies, the Events Report significantly reduces the time and effort required to understand and manage your network's security posture, transforming raw event data into actionable intelligence.

In this section, you will learn about:

- Key Features of Events Report
- How to View the Events Report
- Event Type Specific Details
- Filtering and Search Options
- Known Limitations

Key Features of Events Report

Describes Key Features of Events Report in Cisco Secure Access. Unified Event Log: Correlates logs from Zero Trust Access (ZTA), Firewall, and Secure Web Gateway (SWG) platforms, mapping a single flow across the entire service stack using consistent identifiers.

- **Unified Event Log**: Correlates logs from Zero Trust Access (ZTA), Firewall, and Secure Web Gateway (SWG) platforms, mapping a single flow across the entire service stack using consistent identifiers.
- **Single Action Record**: Each packet flow action (Allow, Block, Isolate) is recorded and reported after eliminating duplicate events for the same packet. Currently, the action is not displayed globally across all correlated events; however, users can use correlation to identify where enforcement actions occur at different enforcement points.
- **Security Events**: The report includes correlated security events.
- **Advanced Filtering and Search**: The Events Report offers flexible filtering options. You can use the search box at the top of the table for quick filtering by event ID, destination IP address, port, rule name, source, and private resource. For more granular analysis, click the **Filters** button on the right of the search box to reveal an advanced set of filtering options on the right side of the page. Additional features include custom time range selection and table column configuration using the gear icon.

View Events Report

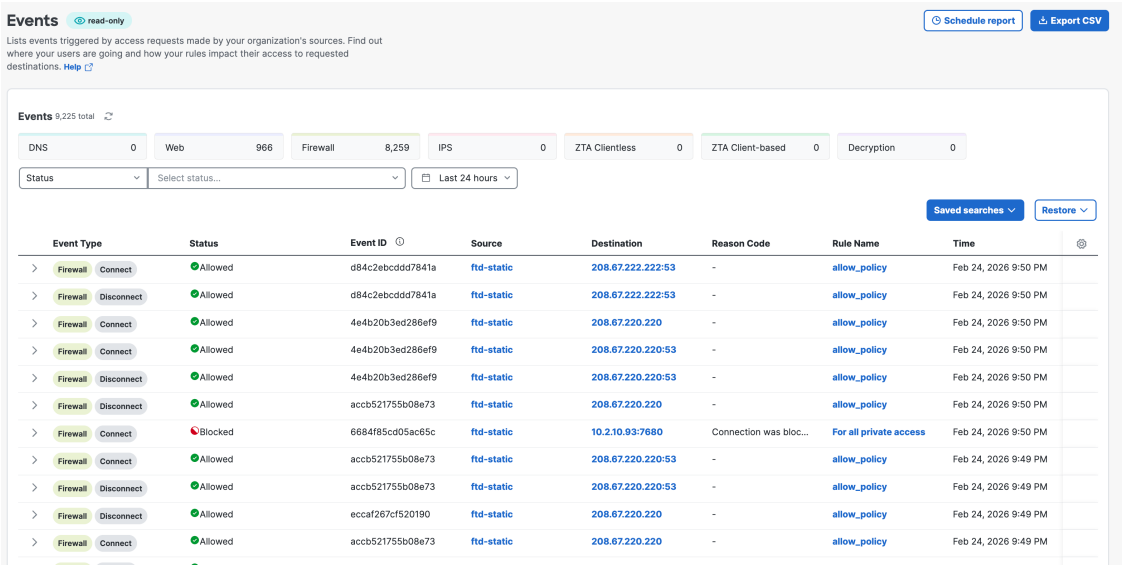
Provides instructions for completing the View Events Report workflow in Cisco Secure Access. Use the Events report to view, filter, and analyze all significant security and network activities across your Cisco Secure Access deployment.

Use the **Events** report to view, filter, and analyze all significant security and network activities across your Cisco Secure Access deployment. This unified report provides a comprehensive record of event types, statuses, source and destination details, rule information, and reasons for actions–helping you troubleshoot issues, verify policy enforcement, and adhere to compliance requirements.

Procedure

1. Navigate to **Monitor** > **Reports** > **Events**.
2. Choose a time frame.

   You can view events over the **Last 15 minutes**, **Last 30 minutes**, **Last 1 hour**, **Last 4 hours**, **Last 12 hours**, **Last 24 hours** (default), **Last 7 Days**, **Last 30 Days**, or a **Custom range**.



For firewall events, the report displays both **Connect** and **Disconnect** actions. A **Connect** event indicates the start of a connection, recorded at the TCP handshake, where application details are typically not yet known by the Firewall. A **Disconnect** event signifies the close of the session, often containing more comprehensive, application-specific information.

Specifically for Firewall Disconnect events, the Destination section of the Event Details Card includes the **Session Bytes Sent** and **Session Bytes Received** fields. These fields show the total amount of data sent and received during the firewall session, providing clear visibility into overall data transfer for each connection. This allows you to quickly assess the volume of data exchanged in a session and supports investigations into unusual or suspicious network activity.

The Events Report table displays key information for each event. For a detailed understanding of each event type, including their unique characteristics, specific status values, and relevant behaviors, see Event Type Specific Details.

- **Event Type**: Category of the event, for example, DNS, Web, Firewall.
- **Status**: Action taken (Allowed, Blocked, Isolated, Connected, or Disconnected).
- **Event ID**: A unique correlation ID generated for each request received by the policy broker, which is propagated downstream to maintain request tracking across network services.
- The Event ID is linked to the 5-tuple (source IP address, source port, destination IP address, destination port, and protocol) of each flow. This ensures that all the packets in the same flow share the same Event ID. However, if two different flows use the same 5-tuple within a short time, they too could get the same Event ID. This usually happens if a client quickly reuses the same source port for requests to the same destination.
- **Source**: Displays the originating identity for the event. This can be:
  - Source IP address (for network-based traffic).
  - User Identity (for authenticated users).
  - Device IP address (for client-based connections, typically representing the public IP address of the client device).
  - Public IP address of the client device (for ZTNA client-based connections). The ZTNA service also logs a specific ZTNA Device ID (a globally unique identifier) for the client, which is distinct from any IP address and helps identify the specific device regardless of its network location.
- **Destination**: The IPv4 or IPv6 address of the destination. Supports both compressed and long-form IPv6 address formats. Applicable to Web, Firewall, and decryption requests.
- **Reason Code**: Cause of a particular event, for example, policy match, threat detected.
- **Rule Name**: The name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
- Click a rule name to view the access policy in which the rule is configured. For more information, see Manage the Access Policy.
- **Time**: Date and time at which the event occurred.
- **Settings**: Gear icon to access table display settings, including options to adjust table density and to show or hide columns in the table.

  Column Behavior:

  - **Sorting**: Most columns can be sorted in ascending or descending order by clicking their header. Columns that are sortable will display an arrow icon (or similar visual indicator) in their header. Some columns, such as **Destination** and **Reason Code**, are currently not sortable to ensure optimal performance.
  - **Resizing**: Column widths can be adjusted by dragging the dividers between column headers.

  Note that the resize functionality is active across the entire column header area.

> **Note**
>
> If you have a block rule, for example, to block social media, and a user tries to access a blocked site such as facebook.com, the Events report will only display a Web block event. The Firewall does not log an event in this scenario because logging both a Firewall allow and a Web block could be confusing. This is intentional. When the Firewall allows the traffic, but the Secure Web Gateway (SWG) blocks it, only the Web block action is shown in the report.
>
> As a result, if you are looking to correlate events between the Firewall and Web layers for this type of traffic, you will not see a corresponding Firewall event. This is expected behavior and does not indicate a system issue.

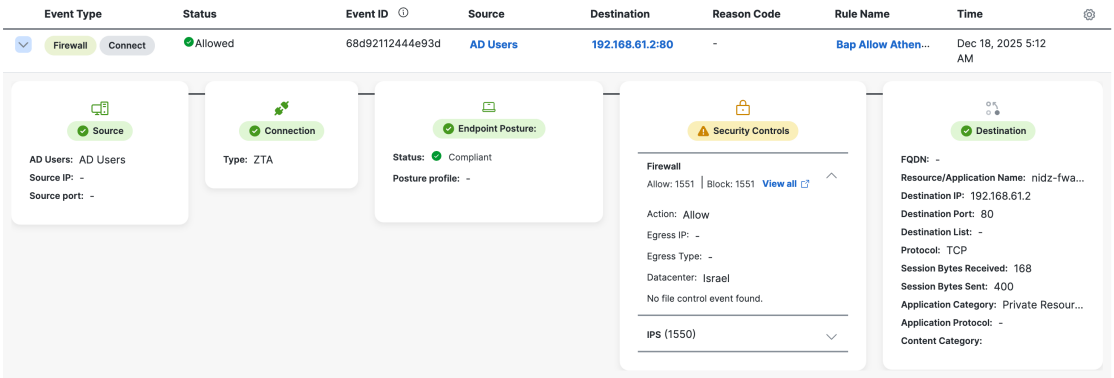
3. Select which security event types you want to view in the report. By default, all event types are selected to display activity for all event types.

   The Events report supports partial results if one or more event type queries (such as Proxy, Firewall, IP, Intrusion, or Decryption) fail due to an internal error. The report displays all available results from the successful queries, rather than showing an error for the entire request. Any unavailable event types will be clearly indicated in a message displayed on the screen.

> **Note**
>
> This feature update ensures continued visibility into available security data, even when certain backend services encounter issues. All retrieved data remains accessible for review and export.

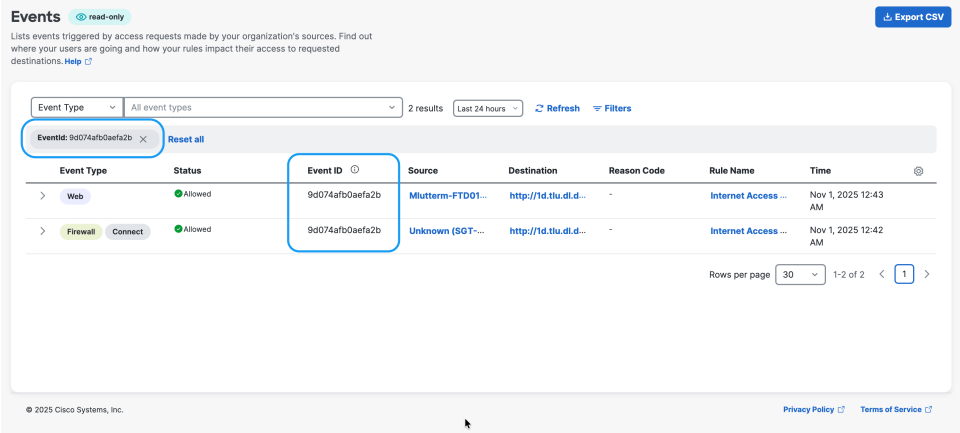
4. Click the **>** icon next to an event to view its Event Details Card.

   This card provides a comprehensive, correlated view of the event, grouped by Source, Connection, Security Controls, and Destination. The card also details applied security controls and the final rule action (e.g., blocked or allowed) for the specific event.



> **Note**
>
> Interactive elements within the Event Details Card may display additional information upon hover or click.

Click on an Event ID within the table to automatically filter the report and display all correlated events.



5. (Optional) Refine your search using advanced filters. For detailed information on all available filtering and search options, see Filtering and Search Options.
6. (Optional) To export the events report, click the **Export CSV** button at the top-right corner of the table. This downloads the current view of the report in CSV format for further analysis or record-keeping. For detailed instructions on exporting report data, see Export Report Data to CSV.

Event Type Specific Details

This topic describes how the Events Report collects, correlates, and presents data from multiple network event types, such as DNS, Web, Firewall, IPS, ZTNA, and Decryption, enabling users to analyze security events efficiently by understanding their distinct characteristics, status values, and filtering options.

The Events Report provides correlated visibility across various event types, each with its own characteristics and specific data points. Understanding these nuances helps in effectively interpreting the report.

DNS Events

- **Characteristics:** DNS events represent Domain Name System queries and responses. Typically, there is only one DNS event per connection.
- **Status Values:** DNS events can have statuses such as Allowed or Blocked.
- **Unique Behavior:**
  - DNS events are generally not shown in the topology map within the Event Details Card.
  - DNS events do not have an Event Correlation ID as they are considered independent events.
- **Relevant Filters:** Filterable by Event Type: **DNS**.

Web Events

- **Characteristics:** Web events capture traffic related to web browsing and applications.
- **Status Values:** Web events can have statuses such as Allowed, Blocked, Isolated, or Warn.
- **Unique Behavior:**
  - **Firewall Event Suppression for Web Blocks (with exceptions)**: Generally, when a Firewall allows traffic that is subsequently blocked by the Secure Web Gateway (SWG) (for example, due to a social media block rule), the Events Report will only display a Web block event. The Firewall does not log an allow event in this specific scenario. This behavior is intentional to prevent confusion from logging both a Firewall allow and a Web block for the same traffic flow. Consequently, for such traffic, you will not see a corresponding Firewall event

when correlating between the Firewall and Web layers. This is expected behavior and does not indicate a system issue.

- **Exceptions to Firewall Event Suppression:** The Firewall will log an event in cases where:
  1. Two engines matched different rules: For example, if the Firewall applied one rule and the SWG applied a different rule to the same traffic.
  2. SWG blocked on a Security Feature: If both engines matched the same rule, but the SWG specifically blocked the traffic based on a security feature (for example, malware detection, IPS signature match) rather than a general policy block.
- The Isolate status may exist alongside Allowed or Blocked statuses.

- **Relevant Filters:** Filterable by Event Type: **Web**. Specific advanced filters include Content Category and Security Category.

Firewall Events

- **Characteristics:** Firewall events detail network connections and their state as processed by the firewall.
- **Status Values:** Firewall events can have statuses such as Allowed or Blocked.
- **Unique Behavior:**
  - Firewall events explicitly display both Connect and Disconnect actions.
    - A Connect event is recorded at the TCP handshake, marking the start of a connection. At this point, application-specific details are typically not yet known by the firewall.
    - A Disconnect event marks the close of the session. It often contains more comprehensive, application-specific information, such as bytes transferred and user details, as it reflects the entire flow.
  - Multiple IPS or file events can occur between a single Connect and Disconnect event, all sharing the same correlation ID.
- **Reason Codes:** The Reason Code field in Firewall events indicates the reason for an Allow or Block action. For allowed events, the Reason Code may display values such as **Unknown Reason**, may remain empty, or may indicate **Pending rule evaluation** under certain circumstances.
  - The **Pending rule evaluation** value appears in the Reason Code field when a network flow ends before the firewall completes rule matching. This happens if the firewall needs more packet inspection to decide the policy. We know the firewall permits the traffic by default and logs the event as **Pending rule evaluation**. You can check the **Rule Name** field to identify the rule that was under evaluation at the time the flow ended.
  - For blocked events, the **Reason Code** field shows the exact policy or condition that caused the block. For example, you see **Access Control Policy** or **Threat Prevention**. If no specific reason exists, the field displays **Unknown Reason** or remains empty.
  - For allowed events, **Pending rule evaluation** overrides other reason codes. For blocked events, the **Reason Code** field always shows the actual blocking condition.
- **Interaction with Secure Web Gateway (SWG) Blocks:** For specific scenarios where the Firewall allows traffic that is then blocked by the SWG, the Firewall event may be suppressed. However, there are important exceptions to this suppression. For a detailed explanation of when Firewall events are and are not logged in conjunction with SWG blocks, refer to the Unique Behavior entry under the Web Events section.
- **Relevant Filters:** Filterable by Event Type: **Firewall**. Specific filters like Port are highly relevant.

IPS Events

- **Characteristics:** IPS events capture actions taken by the Intrusion Prevention System.
- **Status Values:** IPS events can have statuses such as Allowed or Blocked.
- **Unique Behavior:** IPS events are part of the correlated flow, meaning they share the same Event Correlation ID as other related events.
- **Relevant Filters:** Filterable by Event Type: **IPS**. The IPS Signature filter is specific to these events.

ZTNA Events

- **Characteristics:** ZTNA events relate to Zero Trust Network Access, including client-based and clientless access to private resources. Browser-based authorization records are ZTA Clientless; TCP connection records are ZTA Clientless Flow.
- **Status Values:** ZTNA events can have statuses such as Allowed or Blocked. Browser-based flows can have statuses such as Connected or Disconnected.
- **Reason Codes:** A common reason for a ZTNA block is a **mismatch failure to resolve DNS**.
- **Unique Behavior (Trusted Internet Access – TIA):**
  - For traffic classified as Trusted Internet Access (TIA), ZTNA does not generate its own event because it doesn't perform policy evaluation for this traffic. Instead, it forwards TIA traffic to the SWG.
  - Therefore, TIA traffic will typically show up as only a Web event, even if it originated from a ZTNA client. The ZTNA service will still send metadata headers with the correlation ID to ensure the Web event can be correlated.
  - In TIA cases, ZTNA will not perform posture evaluation.
- **Relevant Filters:** Filterable by Event Type: **ZTNA**. Specific filters include Private Resources. For browser-based events, select ZTA Clientless.

Decryption Events

- **Characteristics:** Decryption events indicate whether traffic was successfully decrypted or not.

> **Note**
>
> This report only includes decryption events for traffic that is decrypted and inspected by IPS. Decryption details for standard web traffic (such as HTTPS proxy traffic) are not displayed here, even when Decryption Logging is enabled. Consequently, filtering on **Do Not Decrypt** or other decryption actions will not return entries for standard web traffic.

- **Status Values:** When filtering by Event Type: **Decryption**, the standard Status field may not be present or behave differently. Instead, the relevant information is found in the **Decrypt Action** field.
- **Unique Behavior:**
  - Decryption events are generally considered **neutral** in terms of verdict if no errors occur.
  - If a decryption operation encounters an error or is not performed, the status may indicate a value other than Allowed or Blocked.
  - The **Decrypt Action** field is used to specify the outcome of the decryption process (for example, Decrypted, Not Decrypted).

- **Relevant Filters:** Filterable by Event Type: **Decryption**. The Decrypt Action filter is specific to these events.

View Browser-based ZTA Flow Events

Use the Events report to investigate browser-based Zero Trust Access (ZTA) connections to a private resource. Authorization records show the access decision. Flow records show when an underlying TCP connection is established and terminated. Related records share an Event ID.

An application session can use several TCP connections. Each connection has its own lifecycle records. Connection timestamps do not necessarily identify the times that a user signs in to or signs out of an application.

Procedure

1. Choose **Monitor** > **Reports** > **Events**.
2. Choose the time range to investigate, for example, Last 30 minutes.
3. Select **ZTA Clientless**. To narrow the results, filter by the destination private resource.

   Authorization records appear as **ZTA Clientless**. Connection lifecycle records appear as **ZTA Clientless Flow**.
4. Click the arrow next to an event to open the **Event Details** card.

   Review the available source, connection, security control, and destination information.
5. Click the **Event ID** value and choose **Search**.

   Remove unrelated filters if they exclude records that you need for the investigation. The report displays the authorization record and the related Connected and Disconnected flow records for that connection.
6. Compare the **Time** values on the matching **Connected** and **Disconnected** rows to determine when the connection was active.

   Use the event row timestamps for this comparison. The Session end time field in the detail card can be blank. If a matching Disconnected record has not appeared, the connection might still be open. Connected records remain in the report after their corresponding Disconnected records appear.

   > **Note**
   >
   > Connections can overlap. Do not add connection durations together to calculate the duration of an application session.

7. Expand the **Disconnected** flow record.

   Under Security **Controls** > **ZTA clientless flow**, review Session Bytes Received and Session Bytes Sent.\

   Final byte totals are available when the connection disconnects. They are not available in its Connected record.
8. Review **Reason Code** in the event table or **Reason** in the Connection card for available closure information.

   A normal closure can populate these fields. A populated reason does not necessarily indicate a failed connection. For example, an RDP **End session** action can be followed by `close_event=local_close` and `local_close_reason=triggered_delayed_close_timeout`. Other browser connections can remain open while the application page is loaded. Closing the browser tab can close those connections and produce `close_event=remote_close`.

Schedule an Events Report

Describes Schedule an Events Report in Cisco Secure Access. You can schedule Events Report exports to be delivered to your email at regular intervals.

You can schedule Events Report exports to be delivered to your email at regular intervals. The scheduled report email includes an HTML table preview of the filtered report, a downloadable CSV file with all relevant event data, and a direct link to view the live report in the portal. Any filters and column customizations applied to the Events Report are reflected in the scheduled report, ensuring you receive only the data that matches your requirements.

Any filters, including complex Boolean logic applied via Advanced Search, and column customizations are reflected in the scheduled report, ensuring you receive only the data that matches your specific requirements.

Scheduling is available for all supported event types, allowing you to tailor automated reporting for your organization's monitoring, auditing, and compliance needs. For detailed step-by-step instructions, see Schedule a Report.

> **Note**
>
> Data older than 30 days cannot be included in scheduled or exported reports.

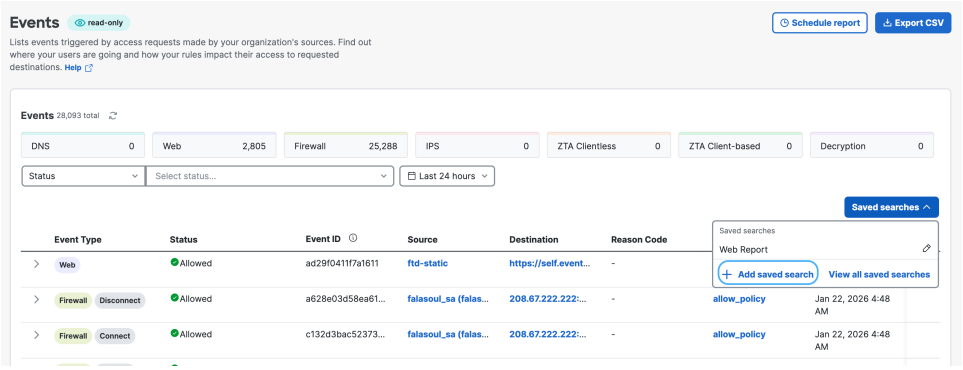
Saving a Search in the Events Report

Provides instructions for completing the Saving a Search in the Events Report workflow in Cisco Secure Access. You can save your filter and column configuration in the Events Report to quickly access the same view in the future.

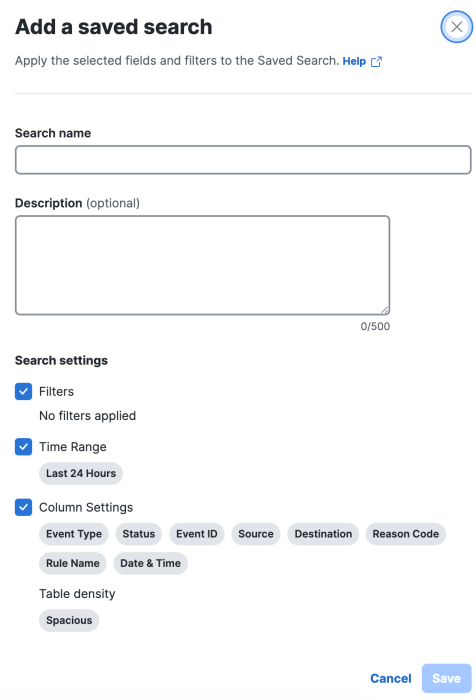
You can save your filter and column configuration in the Events Report to quickly access the same view in the future. This includes any complex Boolean queries constructed through Advanced Search.

Procedure

1. On the **Events Report** page, select the filters you want to use and adjust the column layout as needed.
2. After configuring your view, open the **Saved searches** drop-down menu at the top right and click **Add saved search**.



3. In the **Add a saved search** dialog, enter a name and an optional description to help identify your saved search.



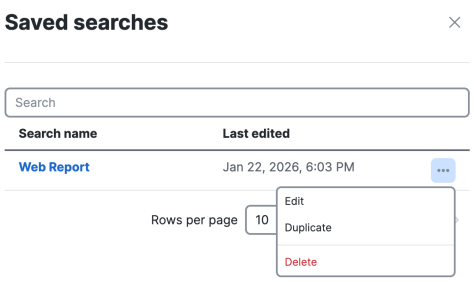
4. Review the filters, time range, and column settings that will be saved with this search.
5. Click **Save**.

   Your search is now available in the **Saved searches** menu for future use.

What to do next

After saving your search, you can further manage your saved searches using the **Saved Searches** menu at the top right of the Events Report page:

- **Apply a saved search:** Select the desired saved search from the **Saved Searches** dropdown to instantly apply its filters and columns to the Events Report. If the saved search includes Advanced Search criteria, the Advanced Search panel will automatically populate with your saved Boolean logic.
- **Update a saved search:** If you modify the filters in an applied saved search, click the **Update saved search** button that appears to save your changes to the current saved search.
- **Edit a saved search:** Click the **Edit** icon next to the saved search in the **Saved Searches** menu to update the search name, description, filters, or columns. To save the changes as a new search, click **Save as new search**.
- **View all saved searches:** Open the **Saved searches** drop-down menu at the top right and click **View all saved searches** to view all the saved searches. From the more options menu (three dots) next to each saved search, you can:



  - **Edit:** Update the search name, description, filters, or columns.

- **Duplicate:** Create a new saved search based on an existing one. Enter a new name and description, then click **Save**.
- **Delete:** Remove a saved search from your list. Confirm the deletion when prompted.

Customize and Manage Saved Searches

Describes Customize and Manage Saved Searches in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The Events Report supports enhanced customization and search management with the following functions:

- **Auto-Save of Search State:** When you apply filters or customize columns, your current view is automatically saved. If you navigate away from the Events Report and then return, your last auto saved state including filters and column selections is automatically restored.
- **Restore Options:** Restore options will appear only when a previous state or changes exist to revert to. Restore options allow you to quickly revert your report view to a previous or default state.
  - **Restore to default Layout:** Revert the report to its original default view.
  - **Restore to Previous State:** Return to your last auto-saved view.

    This option is disabled if no previous state exists (such as on your first visit or before making changes).

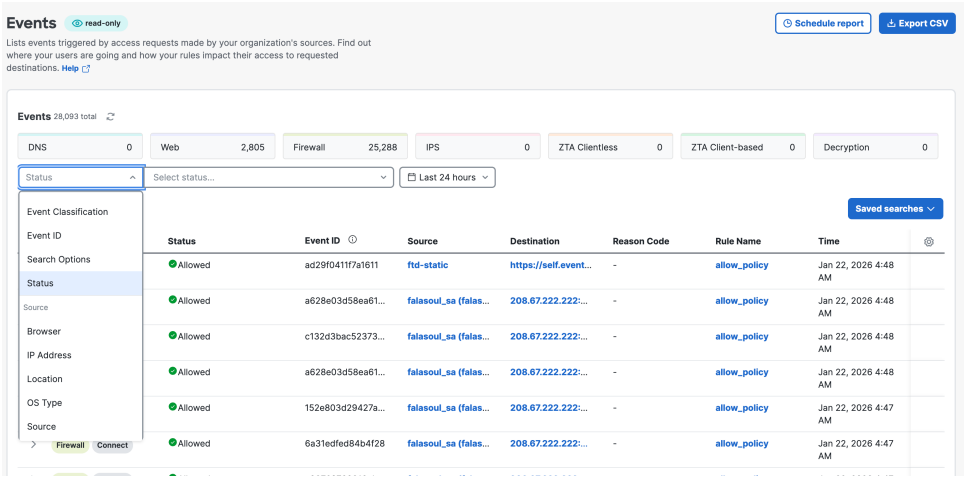
Filter Events Using Basic Search Options

Describes Filter Events Using Basic Search Options in Cisco Secure Access. The Events Report provides robust filtering and search capabilities to help you quickly narrow down and analyze significant security and network activities.

The Events Report provides robust filtering and search capabilities to help you quickly narrow down and analyze significant security and network activities. You can use a combination of basic search box filters and advanced filter options to focus on specific events.

Basic Filters

Located directly above the Events Report table, these filters allow for quick, direct searches on common event attributes.



The following list highlights key filter attributes available in the Events Report. For a complete and current set of filter options, please refer to the Events Report user interface.

- **Event Type:** Filter by one or more categories (for example, DNS, Web, Firewall, ZTNA, Decryption). Event Type filters are displayed as selectable buttons at the very top of the table. Each button displays the event count for that type, and toggling a button instantly applies or removes the filter.

- **Event ID:** Filter by one or more unique correlation IDs. When searching for a specific Event ID, the report displays the complete flow of that request across different event types. You can enter multiple IDs (for example, ID1, ID2, ID3) to return results matching any of the specified IDs.
- **Destination:** Filter by destination IP address or resource (for example, FQDN, URL). When you click on a destination address in the **Destination** column, if it is an IP address, the system automatically converts this into an IP address search for that destination. Destination Country can now be selected from a type-ahead dropdown list, minimizing manual entry and improving accuracy.
- **IP Address:** Filter by a specific source or destination IP address. Currently, IP search is unified—searches are performed across both source and destination IP fields. Wildcard patterns are supported.
- **Port:** Filter by network port number. You can also exclude specific ports by selecting the **Exclude** checkbox.
- **Rule Name:** Filter by the name of the access rule applied to the request. Applicable to DNS, Web, Firewall, IPS, and ZTNA requests.
- **Source:** Filter by user identity or source IP address. IP address search supports wildcard patterns and attempts to match across multiple IP fields. Source Type (such as User, Device, or Network) and Browser/Browser Location filters are available where applicable.
- **Private Resources:** Filter by events related to designated private resources.

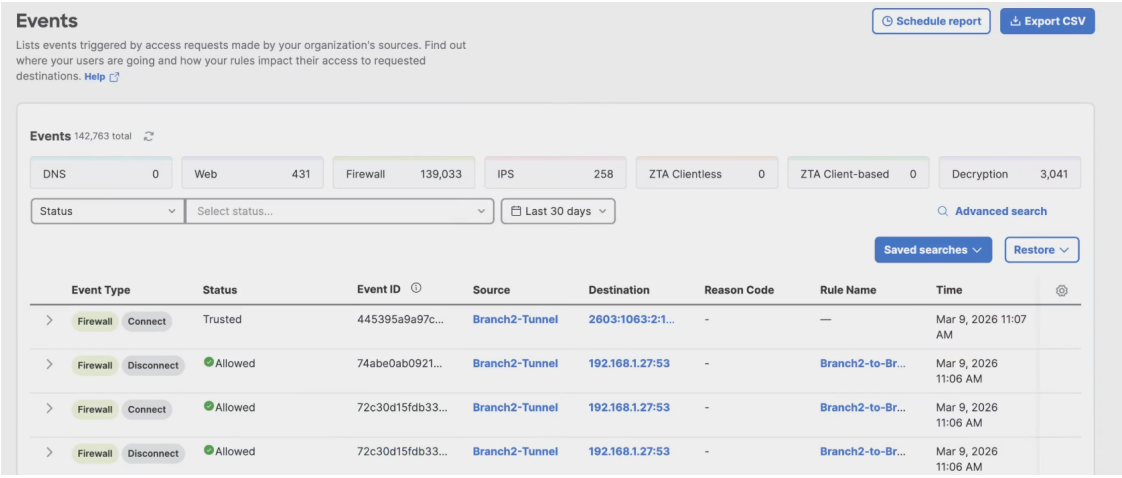
Filter Events Using Advanced Search

Provides instructions for completing the Filter Events Using Advanced Search workflow in Cisco Secure Access. Use this procedure to perform deep-dive analysis of event data by applying multi-condition Boolean logic, organizing filters into groups, and utilizing the top-level Event Type selector.

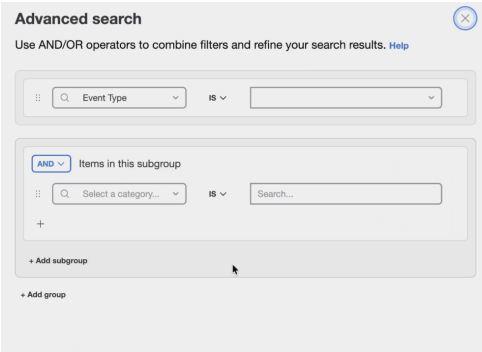
Use this procedure to perform deep-dive analysis of event data by applying multi-condition Boolean logic, organizing filters into groups, and utilizing the top-level Event Type selector.

Procedure

1. Navigate to **Monitor** > **Reports** > **Events**.



2. Click **Advanced search** at the top right of the Events Report table to open the advanced search panel.



When you transition from the basic search to Advanced Search, any filters currently applied in the basic search are automatically carried over to the last active subgroup.

The **Advanced search** panel has options to add filter groups and define Boolean logic (AND/OR operations).

3. From the **Event Type** drop-down menu, choose one or more event types.

   Multiple selections here are processed as **OR** logic and are independent of the group/subgroup logic below.

4. Choose the **AND** or **OR** operator from the dropdown to define how your groups and subgroups interact.
5. Click the dropdown or begin typing to search for available attributes (such as Destination IP, Port, Rule Name, and so on.), then set the desired value for each.
6. Click **Add (+)** to add additional filters.

   Continue adding filters as needed by repeating the dropdown selection process. Each filter you add will refine your search results.

7. Create a Subgroup:
   a) To group related filters, click **Add Subgroup**.
   b) Within the subgroup, add multiple filters.
   c) Choose the Boolean operator for the subgroup. Select **AND** if all filters in the subgroup must match. Select **OR** if any filter in the subgroup can match.
8. Click **Add group** to create a new logical group.

   Groups can contain one or more subgroups and filters. Set the Boolean operator for the group (**AND** or **OR**) to define how its subgroups and filters interact.

   Use a combination of groups and subgroups to build complex queries.

9. Click **Apply** to apply the advanced search filters to perform detailed analysis of events.

   Review the filtered events in the table. You can click **Reset all** at the top of the events table, to clear the advanced search conditions and return to the default view.

Known Limitations

Describes Known Limitations in Cisco Secure Access. To ensure optimal performance and system stability, the Events Report operates with certain known limitations and boundaries.

To ensure optimal performance and system stability, the Events Report operates with certain known limitations and boundaries. Understanding these helps manage expectations and provides context for specific behaviors.

This section details these aspects:

- Data Retrieval Limit (10,000 Offset)
- Understanding Data Availability (Missing Fields)
- Protocol-Specific Correlation Behaviors

- Known Issues and Ongoing Enhancements

Data Retrieval Limit (10,000 Offset)

Describes Data Retrieval Limit (10,000 Offset) in Cisco Secure Access. The Events Report is designed to efficiently retrieve and display a large volume of data.

The Events Report is designed to efficiently retrieve and display a large volume of data. However, to maintain system performance and responsiveness, there is a practical limit to the number of events that can be paginated and displayed in a single session.

- **Limitation:** The Events Report user interface (UI) allows navigation and display of events up to a maximum of 10,000 offsets.
- **Behavior:** If your search results contain more than 10,000 events, the UI will automatically prevent you from navigating beyond this 10,000-event threshold. This means you will not be able to view events that fall outside of this range through direct pagination.
- **Implication:** This boundary is implemented to prevent potential API errors and ensure a smooth user experience. If you need to analyze data beyond this limit, consider refining your search criteria (e.g., narrowing the time frame or applying more specific filters) to reduce the result set, or utilize the export functionality for offline analysis of larger datasets.

Understanding Data Availability (Missing Fields)

Describes Understanding Data Availability (Missing Fields) in Cisco Secure Access. When reviewing events in the Events Report, you may observe that some fields appear blank or are not populated.

When reviewing events in the Events Report, you may observe that some fields appear blank or are not populated. This is expected behavior and typically indicates that the specific data was either not relevant to the event, not collected by the involved security service, or not enabled in your Cisco Secure Access configuration.

The availability of data in various fields depends on several factors:

- **Enabled Services and Features:** Many data points are only collected and displayed if the corresponding Cisco Secure Access service or feature is active and configured for the traffic flow.

  Example: If decryption is not enabled for a particular traffic type, fields related to Decrypt Action will be empty. Similarly, advanced threat-related fields may only be populated if relevant security modules are active.

- **Policy Configuration:** The presence of data in fields like Rule Name or specific Reason Codes often depends on whether a particular policy was matched or a specific security verdict (e.g., block, isolate) was generated. For allowed traffic, a Reason Code might be less specific or even empty if no explicit policy match or threat was involved.

  Posture Enforcement Status: Fields related to device posture, compliance, or specific client attributes will only be populated if device posture checks are enabled and applicable to the connection. If posture is not enabled or not relevant to the event, these fields will be blank.

  Traffic Type and Flow: Different types of traffic (e.g., DNS, Web, Firewall, ZTNA) inherently generate different sets of data. A field highly relevant for a Web event (like Content Category) might be irrelevant or empty for a Firewall event.

  Service Chaining and Data Propagation: While the Event Correlation ID ensures events are linked, not all data points are universally propagated across every service. Each service contributes its specific context to the overall correlated event. For instance, ZTNA may not log certain network-level protocols if its primary role is identity-based access.

What to do if a field is empty:

If you expect to see data in a particular field but find it blank, consider the following:

- **Check your Cisco Secure Access configuration:** Verify that the relevant services, features, and policies are enabled and correctly configured.

- **Consider the traffic type:** Is the field typically relevant for this type of event?
- **Review the event context:** For allowed connections, some fields (like Reason Code) may naturally be less detailed.

Protocol-Specific Correlation Behaviors

Describes Protocol-Specific Correlation Behaviors in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

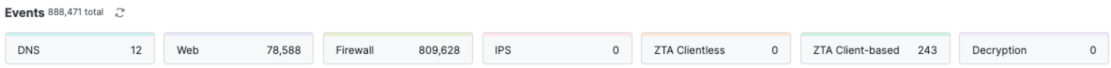
The Event Correlation ID aims to group logically related network activities. For certain protocols, this may result in a single correlation ID representing multiple underlying network events:

- **ICMP Traffic Correlation:** For Internet Control Message Protocol (ICMP) traffic, the correlation logic may group seemingly distinct events (such as traffic from different network hops, as seen in a traceroute) under a single Event Correlation ID. This is an intentional design to represent a single logical ICMP operation (for example, a traceroute or a series of pings) as one correlated event, even if it involves multiple intermediate network responses.

Known Issues and Ongoing Enhancements

Describes Known Issues and Ongoing Enhancements in Cisco Secure Access. Missing User ID in ZTNA Event Logs: In specific situations, particularly when Universal ZTNA (UZTNA) is enabled and an access block occurs before policy remediation, some ZTNA event logs may not include the User ID.

- **Missing User ID in ZTNA Event Logs:** In specific situations, particularly when Universal ZTNA (UZTNA) is enabled and an access block occurs before policy remediation, some ZTNA event logs may not include the User ID. This happens if the application cannot be identified, preventing the policy evaluation context from being fully set, which results in the User ID being absent from the event log.
- **API Timeout Recovery and Graceful Degradation:** While the 10,000 offset limit prevents direct errors, ongoing work aims to improve API timeout recovery and ensure graceful degradation for very large data requests.
- **User-Friendly Error Messages:** Efforts are underway to enhance the clarity and helpfulness of error messages across the application.
- **Traffic Type Count Truncation for ZTA Client-based:** For the **ZTA Client-based** traffic type, the digits in the count display may run out of space and be truncated.



79 Network Connectivity Monitoring

Topics:

- Network Connectivity Monitoring

Provides an overview of network connectivity monitoring in Cisco Secure Access, including how to use network tunnel logs and resource connector logs to track infrastructure health, monitor state changes, and troubleshoot connectivity issues.

Network Connectivity Monitoring

This topic provides an overview of network connectivity monitoring, including how to use network tunnel logs and resource connector logs to ensure secure traffic transmission.

Network connectivity monitoring provides visibility into the health and performance of your network infrastructure. By tracking connectivity events, you can identify connectivity or configuration issues, troubleshoot performance issues, and ensure that traffic is securely transmitted between your devices and Secure Access.

Secure Access provides the following monitoring tools to help you maintain visibility:

- **Network tunnel logs:** These logs track events for each tunnel within your network tunnel groups. Use these logs to monitor tunnel health, confirm secure traffic transmission, and troubleshoot connectivity issues between your devices and Secure Access. For more information, refer to Network Tunnel Logs.
- **Resource connector logs:** These logs provide historical visibility into connector health, connectivity, and update events. Use these logs to track state changes, such as establishment, connection processes, and update events, to maintain a clear history of your resource connector behavior over time. For more information, see Resource Connector Logs.

Network Tunnel Logs

Use this procedure to view, search, and export Network Tunnel Logs entries for detailed visibility into network tunnel activity and connectivity issues.

The Network Tunnel Logs lists events for each tunnel within your Network Tunnel Groups, helping you monitor connectivity and confirm that traffic is securely transmitted between devices and Secure Access. For more information, see Manage Network Tunnel Groups.

You can schedule automatic delivery of Network Tunnel Logs reports or export them as CSV files for further analysis. For more information, see Schedule a Network Tunnel Logs report and Export Report Data to CSV.

The exported CSV file of Network Tunnel Logs includes the following columns: **Network Tunnel Group**, **Data Center**, **IP Address**, **Hub Type**, **Region**, **Severity**, **Service**, **Device Type**, **Details**, and **Time (UTC)**.

Use filters to refine results and identify connectivity or configuration issues.

Procedure

1. To open the log, navigate to **Monitor** > **Connectivity Logs** and then select **Network tunnel logs**.

   Note

   You can also navigate from specific network tunnel groups and hubs to see the log filtered automatically. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups**, click a Network Tunnel Group name, then click **See logs** in the **Summary**, **Primary Hub** or **Secondary Hub** menu.

2. The default view shows the following fields for all network tunnel groups.

Field	Description
Network tunnel group	The name of the network tunnel group in each log entry. Clicking the name opens a drawer menu with more detail about the log entry.

Field	Description
Data center IP address	The IPv6 and IPv4 addresses of the Secure Access data center that this network tunnel group hub connects to.
Hub type	Primary or Secondary.
Region	The geographic region of the Secure Access data center. For more information, see Secure Access Regions.
Severity	Error, Warning, or Info.
Service	The name of the service reporting the event: • **IKE**–Events related to IKE/IPsec • **BGP**–Events related to BGP routing • **ORCH**–Configuration changes reported by the orchestrator
Device type	The type of router configured to establish the network tunnel group by connecting to the Secure Access data center. For more information, see Add a Network Tunnel Group.
Details	The error message or additional information about the connectivity event.
Time (UTC)	The date and time of the event in Coordinated Universal Time (UTC).

3. Click a network tunnel group name in the log to see more detail about the event, including the full event message, remediation information if available, more detail about the network tunnel group, data center and service protocol, and a link to network tunnel group device configuration if available.
4. Search the log by Tunnel Group Name, DC IP Address, or Message.
5. Filter the log by Region, Severity, Service, Device Type, and log event Time Period.

Schedule a Network Tunnel Logs Report

This concept explains how to schedule Network Tunnel Logs reports so you receive regular email updates with a report preview, downloadable data in CSV format, and a direct link to the live report. Filters applied in the log view are reflected in each scheduled report.

You can now schedule Network Tunnel Logs reports to be emailed to you at regular intervals. The scheduled report email includes an HTML table preview of the report, a downloadable CSV file containing all available data, and a direct link to a live version of the report in the portal. Any filters applied in the Network Tunnel Logs view, such as network tunnel group, event details, or identities, are reflected in the scheduled report, ensuring only relevant data is included.

> **Note**
>
> Data older than 30 days cannot be included in scheduled or exported reports.

For step-by-step instructions on how to schedule a report, see Schedule a Report.

Resource Connector Logs

This topic describes how to monitor resource connector health and investigate connectivity issues using historical logs.

Resource Connectors provide the secure connectivity that allows Cisco Secure Access to reach internal private enterprise applications without exposing corporate networks to the public internet. Previously, administrators could view a connector's current status in the dashboard, but had limited visibility into how it reached that state or what changed over time. This made it difficult to investigate intermittent connection problems or analyze connector activity after an event occurred.

With Resource Connector logs, administrators can review a centralized history of connector and connector-group events directly in Cisco Secure Access. Use event details to investigate connector establishment, connection state changes, software updates, and other lifecycle activity. You can search and filter logs to narrow an investigation, export results to CSV for offline analysis, or configure scheduled reports to maintain records for operational reviews.

Key Capabilities

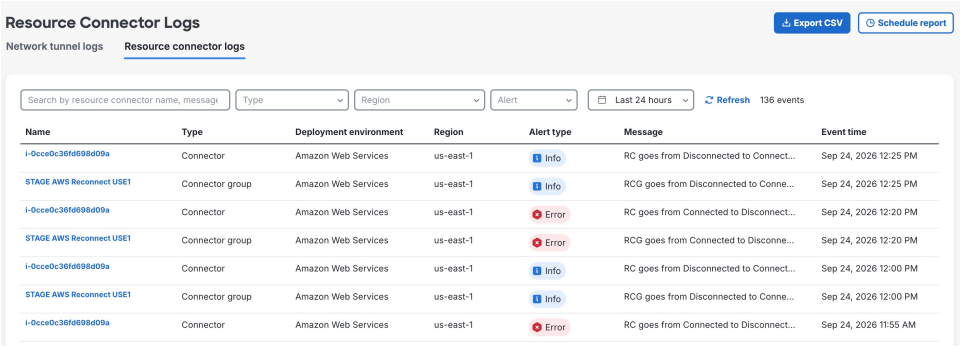
- **End-to-End Lifecycle Tracking:** Track tunnel connection states, disconnects, reconnects, certificate renewals, and automated software updates across all connector instances.
- **Search and filter:** Focus on the activity relevant to an investigation to quickly find specific connector or group events.
- **Event details and troubleshooting:** Open an event to see its details and associated connector or group information, including suggested troubleshooting guidance when available.
- **Flexible Reporting & Scheduling:** Retains up to 90 days of event history, supports custom date filtering (up to 30 days per query), and enables on-demand CSV downloads and recurring email reports. For more information, see Schedule a Report and Export Report Data to CSV.

Use filters to refine results and identify connectivity or configuration issues.

Procedure

1. Navigate to **Monitor** > **Connectivity Log** and then click **Resource connector logs**.

   Alternatively, navigate to **Connect** > **Network Connections**. In the table, click the ellipsis (**...**) next to a connector group or resource connector, and then select **View Logs**. The Resource Connector Logs report opens pre-filtered for that specific connector group or connector instance.



   The default view shows the following fields for all resource connector groups.

Field	Description
Name	The display name or cloud instance ID (such as an AWS EC2 instance ID, Azure VM name, or VMware ID) of the connector or connector group. If the entity was deleted, the table displays **Deleted** along with its historical identifier and the user or client ID that removed it. **Note** If an identity lookup fails, the label may instead display as unavailable or failed.
Type	The entity type, indicating whether the log record applies to an individual connector or a connector group.
Deployment environment	The infrastructure environment hosting the connector (such as AWS, Azure, GCP, or VMware ESXi).
Region	The geographic region where the resource connector operates.
Alert type	The severity level of the event, such as Info, Warning, or Error.
Message	A concise summary of the connectivity event, state transition, or failure condition.
Event time	The date and time the event occurred.

2. Use the filters to refine your results:
   - **Search bar:** Search by resource connector name, message.
   - **Type:** Filter by connector or connector group.
   - **Region:** Filter by the geographic region of the connector.
   - **Alert:** Filter by event severity (error, warning, or info).
   - **Timeline:**Select a preset time range (Last 15 minutes, Last 30 minutes, Last 1 hour, Last 4 hours, Last 12 hours, Last 24 hours, Last 7 days, Last 30 days) or choose the **Custom Range** option.

   Note

   Data Retention and Export Limits: Secure Access retains event history for up to 90 days. However, to ensure optimal performance, the maximum time window for any single query, CSV export, or scheduled report cannot exceed 30 days. To inspect older periods within the 90-day retention window, adjust your start and end dates accordingly. You cannot export the entire 90-day history in a single action.

3. Click **Refresh** to reload the table with the latest live events.
4. To diagnose root causes and review remediation steps, click a record name in the log table to open the **Resource Connector details** side drawer.

Individual Connector Details: When you click a record for an individual connector, the drawer displays the following sections:

- **Header:** Displays the **Instance ID** and exact **Event time**.
- **Event Information:** Displays the event severity (**Info**, **Warning**, or **Error**), a descriptive message, and suggested troubleshooting guidance when available.
- **Connector Status:**
  - **Tunnel Status:** Shows the connection state (**Connected** or **Disconnected**) at the time of the event and the timestamp of the last status update.
  - **Certificate Status:** Displays validity status (such as **Valid**, **Expiring soon**, or **Expired**), expiration timestamp, and instructions for certificate rotation or replacement.
  - **Configuration Status:** Displays cloud synchronization status and troubleshooting tips (e.g., verifying local firewall rules if internal DNS configurations cannot be retrieved).
  - **Connector Version & OS Version:** Displays the installed connector software version and host operating system release.
  - **Added:** The date and time the connector was added to the environment.
- **Connector Details:** Displays the parent **Connector group name**, **Region**, **Deployment environment**, and the count of **Private resources** associated with the connector.

Connector Group Details: When you click a record for a connector group, the drawer displays the following sections:

- **Header:** Displays the **Group Name** and exact **Event time**.
- **Event Information:** Displays the group event message, severity badge (**Info**, **Warning**, or **Error**), and suggested troubleshooting guidance when available.
- **Group Details:** Displays the **Region**, **Deployment environment**, total count of member connectors, status breakdown (**connected** versus **disconnected**), and the total count of associated **Private resources**.

5. Review the **Details** and **Fix** sections in the drawer to identify connectivity issues. If an error occurs, perform the recommended diagnostics, such as verifying firewall rules to ensure the connector can reach Secure Access.
6. (Optional) Click **Export CSV** to download the currently filtered view for offline analysis or auditing. See Export Report Data to CSV.
7. (Optional) Click **Schedule** to set up a recurring email report containing the CSV data. See Schedule a Report.

Schedule a Resource Connector Log Report

This concept explains how to schedule resource connector log reports so you receive regular email updates with a report preview, downloadable data in CSV format, and a direct link to the live report. Filters applied in the log view are reflected in each scheduled report.

You can now schedule resource connector log reports to be emailed to you at regular intervals. The scheduled report email includes an HTML table preview of the report, a downloadable CSV file containing all available data, and a direct link to a live version of the report in the portal.

This CSV is significantly more comprehensive than the portal view and includes the following fields: Date/Time, Name, Type, Deployment Environment, Region, Alert Type, Message, Tunnel Status, Last Update, Certificate Status, Configuration Status, Connector Version, Added, OS Version, Connector Group Name, Private Resources, Connector ID, Group ID, Instance ID, and ACME Cert Expiration.

Any filters applied in the resource connector logs view, such as resource connector name, type, region, alert and timeline, are reflected in the scheduled report, ensuring only relevant data is included.

> **Note**
>
> Data older than 30 days cannot be included in scheduled or exported reports.

For step-by-step instructions on how to schedule a report, see Schedule a Report.

80 Network Tunnel Group Usage Report

Topics:

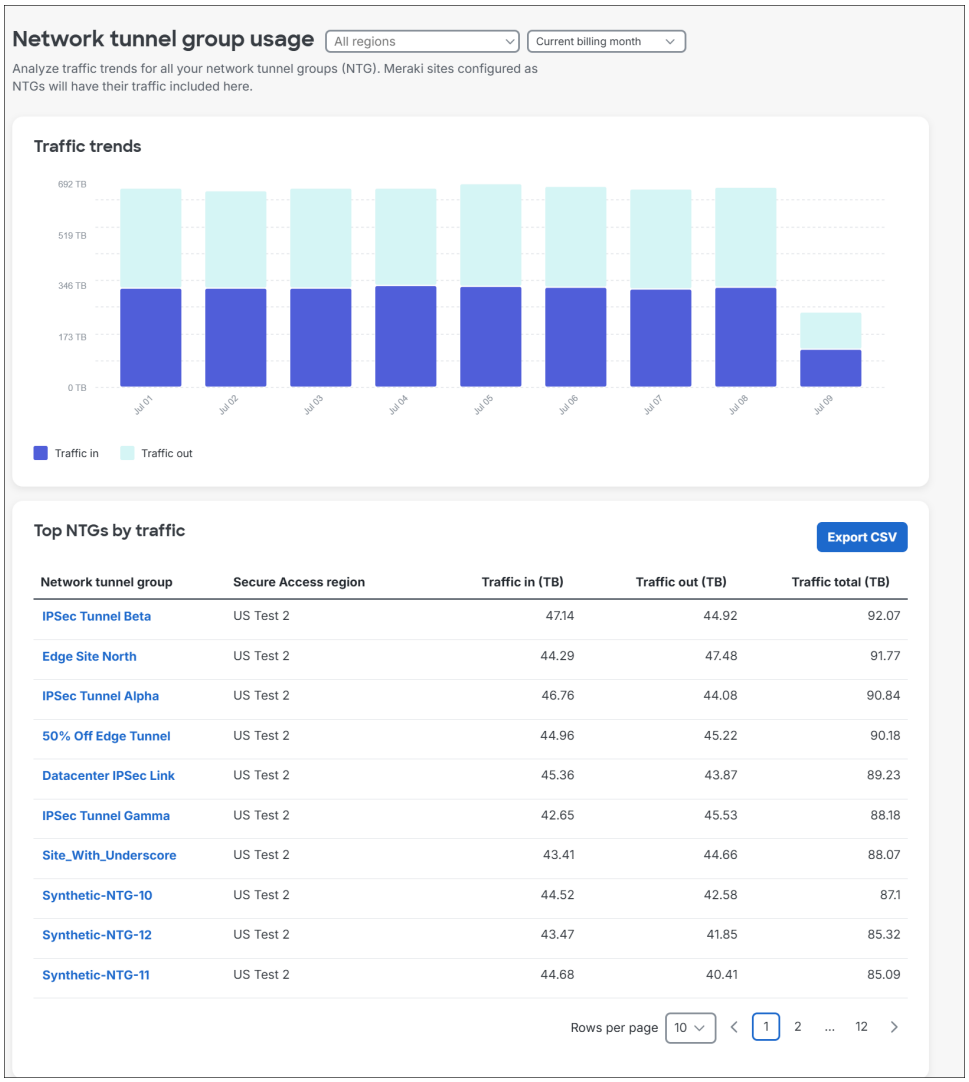
- Network Tunnel Group Usage

Provides an overview of Network Tunnel Group Usage Report in Cisco Secure Access, including Network Tunnel Group Usage. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

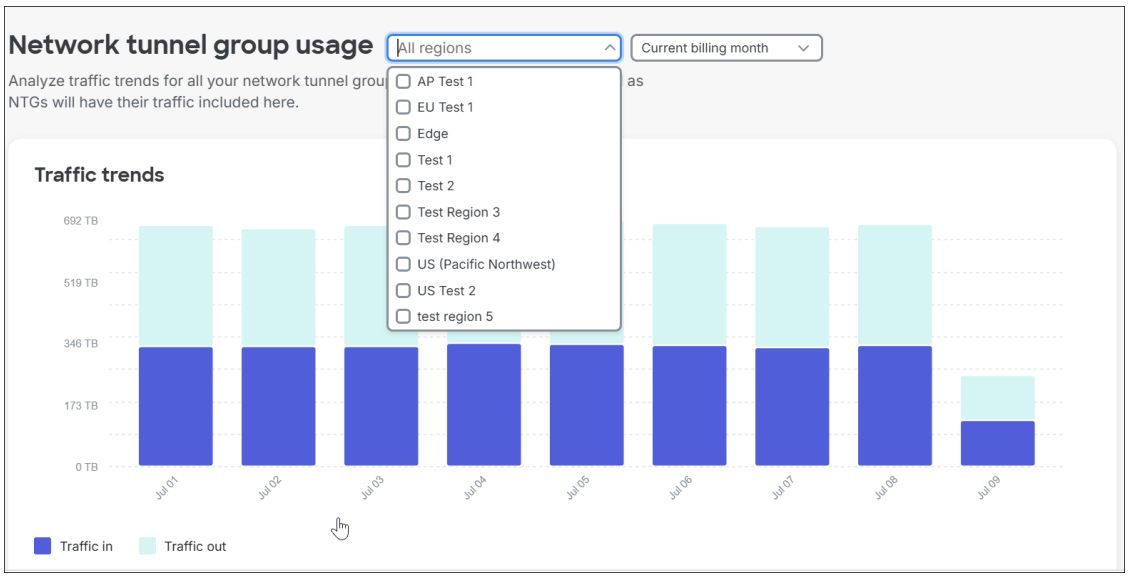
Network Tunnel Group Usage

Gain visibility into your infrastructure by analyzing traffic usage across all configured network tunnel groups. This view helps you monitor traffic usage trends across your network.

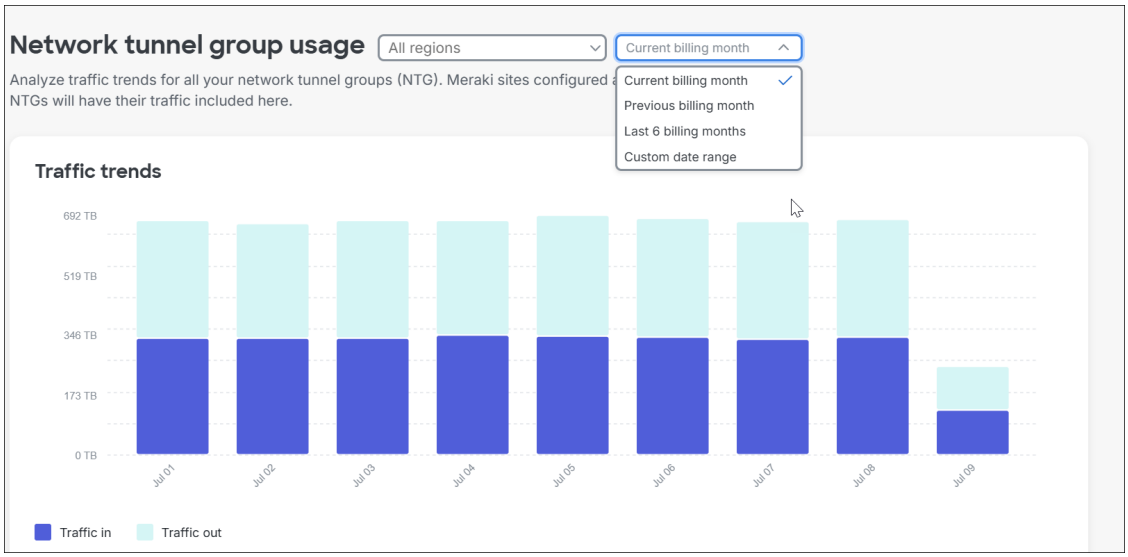
Network Tunnel Group Usage provides visibility into traffic across configured network tunnel groups. It helps you compare inbound and outbound traffic volume, analyze usage trends, and identify traffic patterns across regions during the selected billing period.



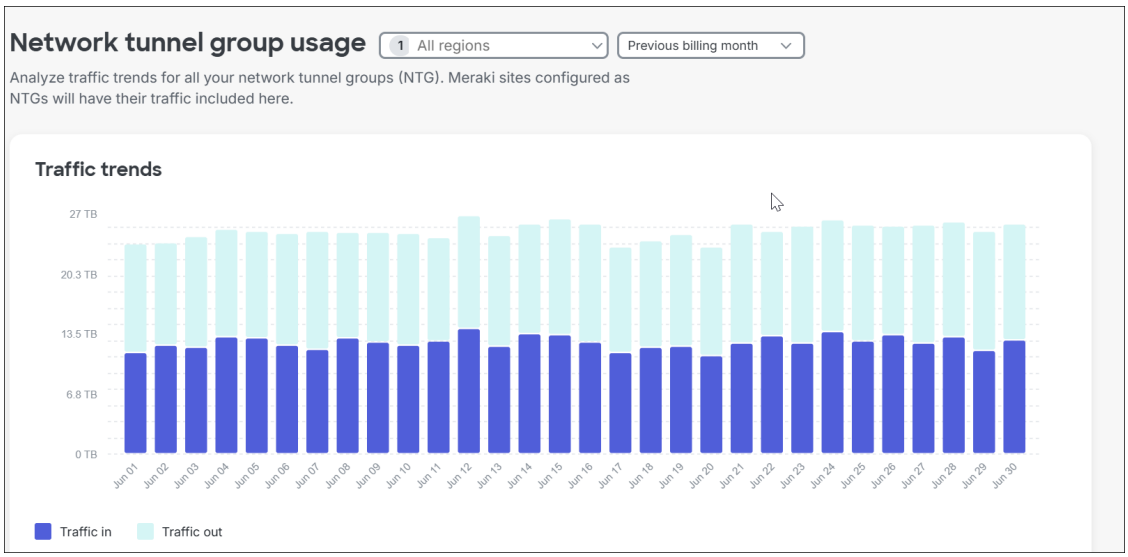
- **Region**: By default, the dashboard displays usage for All regions. You can use the region filter to isolate data for specific geographic areas.



- **Billing period**: Traffic statistics update based on the selected billing period. You can select the current billing month, previous billing month, last six billing months, or a custom date range.



- **Traffic trends**: A visualization of inbound and outbound traffic over your selected period. You can hover over the chart to view specific traffic data for any given date.



Note

The system automatically adjusts traffic units such as KB, MB, GB, TB based on the volume of data to ensure the charts remain readable.

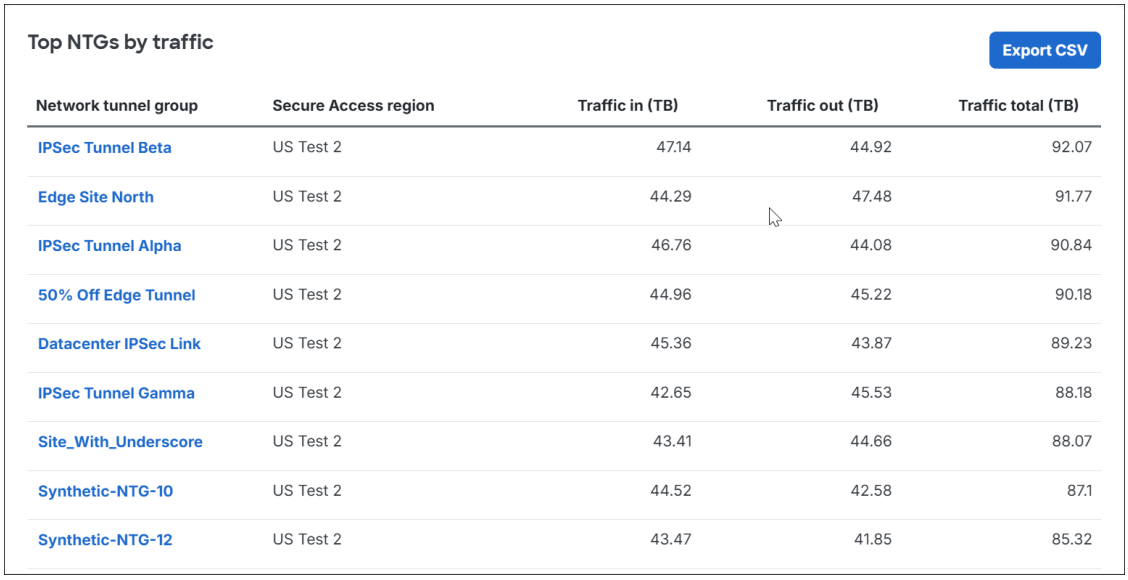
View Top Network Tunnel Groups by Traffic

The Top Network Tunnel Groups by Traffic view identifies the network tunnel groups carrying the most traffic. You can compare inbound and outbound traffic volume, analyze trends, filter results by region and billing period, view details for individual network tunnel groups, and export the results.

Procedure

1. Navigate to **Monitor** > **Network Tunnel Group Usage**.

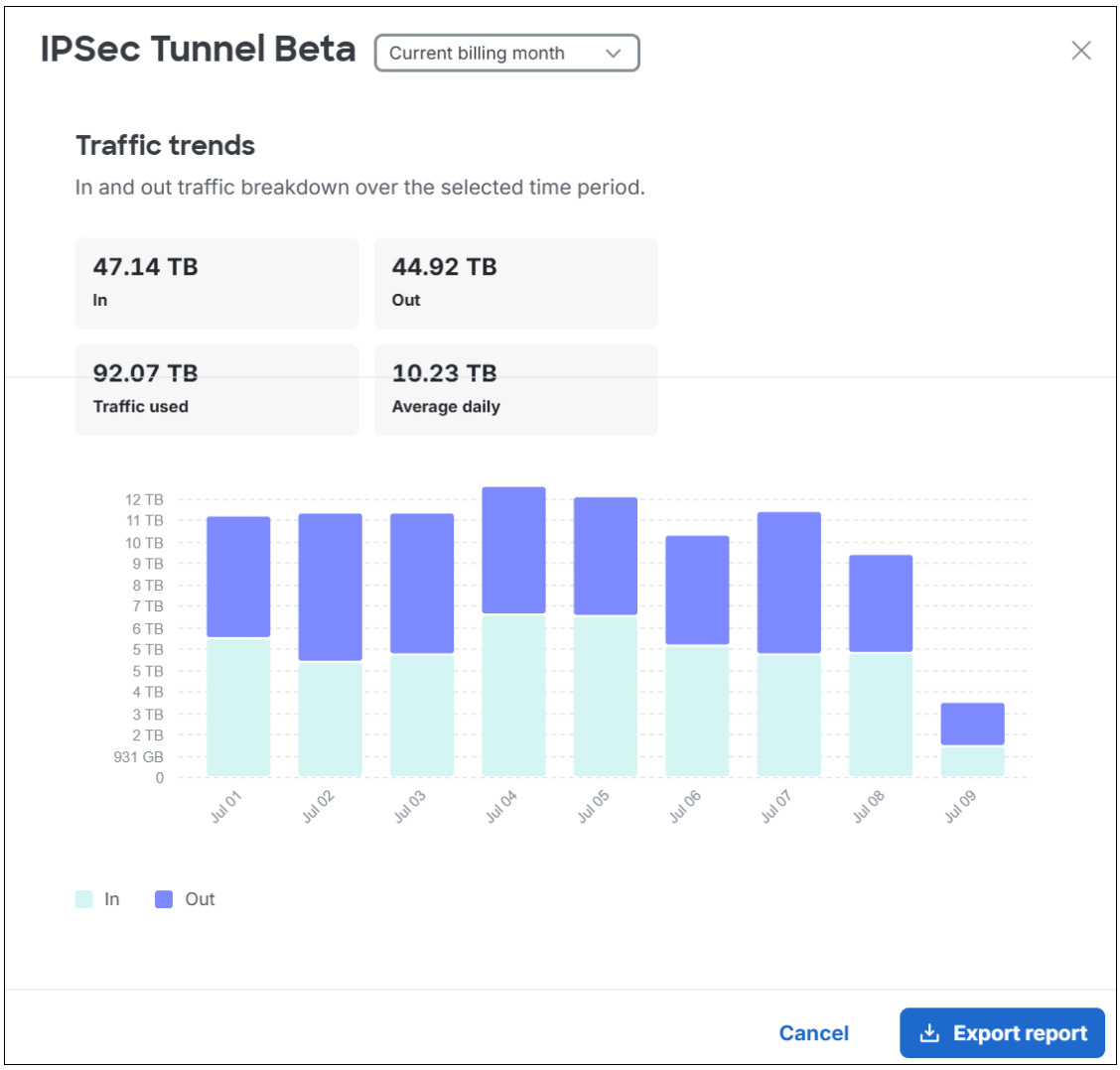
> **Note**
>
> Alternatively, navigate to **Home** > **Overview**, locate the **Network Tunnel Group Usage** tile, and select **View** to open the Network Tunnel Group Usage page.



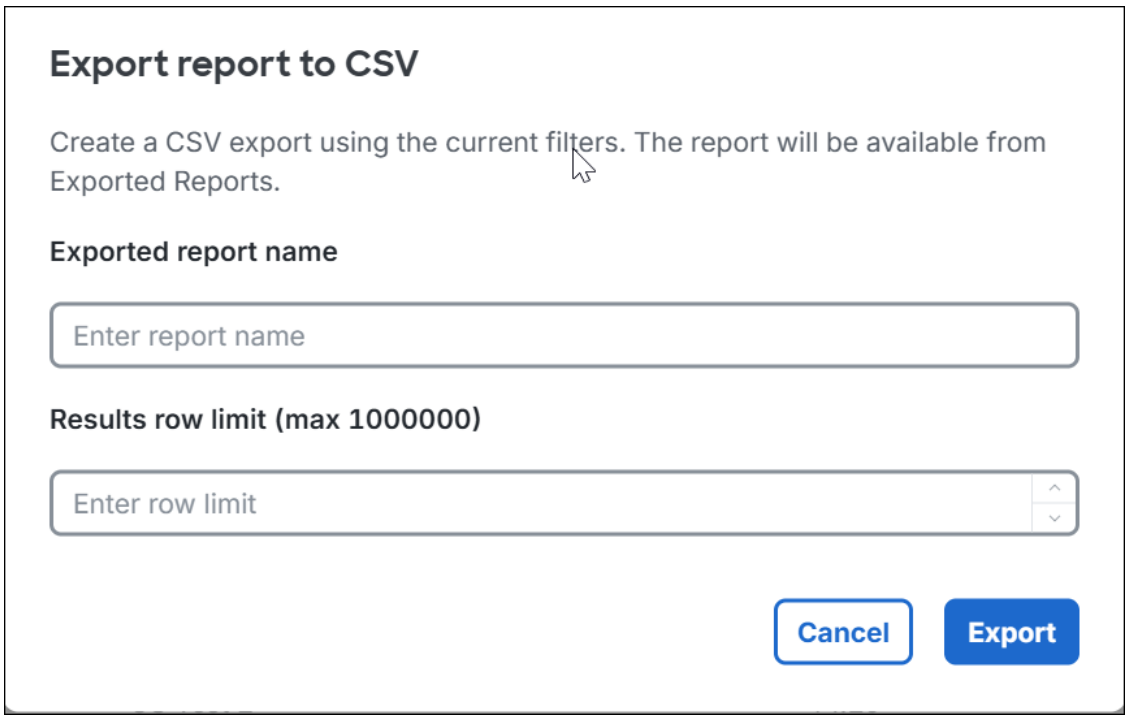
2. Review the following fields for all network tunnel groups.

Field	Description
Network tunnel group	The name of the network tunnel group. Click the network tunnel group name to open a menu displaying detailed traffic information.
Secure Access region	The secure Access data center or region where the Network tunnel group is connected .
Traffic In (TB)	Total inbound traffic received by the Network tunnel group during the selected time in terabytes (TB).
Traffic Out (TB)	Total outbound traffic sent from the Network tunnel group during the selected time in terabytes (TB).
Traffic Total (TB)	Combined inbound and outbound traffic for the Network tunnel group.

3. Click a **Network tunnel group** name to view detailed inbound and outbound traffic, including the total traffic usage for the selected billing period.



4. Click **Export CSV** to export the traffic usage data for further analysis. For more information, see and Export Report Data to CSV.



The exported CSV file includes the network tunnel group, Secure Access region, traffic in, traffic out, and traffic total columns.

81 Remote Access Log Report

Topics:

- About the Remote Access Log Report

Provides an overview of Remote Access Log Report in Cisco Secure Access, including About the Remote Access Log Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

About the Remote Access Log Report

Describes About the Remote Access Log Report in Cisco Secure Access. The Remote Access Log report lists users that have remotely connected to Secure Access and requested access to destinations.

The Remote Access Log report lists connection events for users who connect remotely to Secure Access. Use the report to investigate connection activity, troubleshoot failed sessions, and identify access issues. Some relevant fields include:

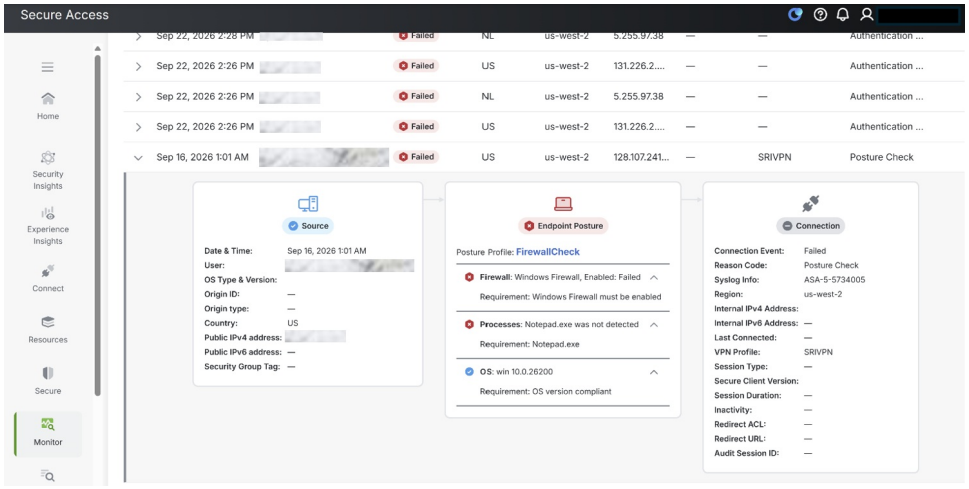
- Display username for failed events – Helps you identify the affected user.
- ASA syslog message ID – Helps you identify the syslog message associated with the event.
- Device ID and device name – Helps you identify the endpoint.
- Machine name – Identifies the client machine when the value is returned for the event.
- Endpoint posture information – Provides posture details for failed events when posture data is returned.
- Connection information – Includes the VPN profile, session type, IP addresses, operating system, and Secure Client version.

Use the time-range control and the filter menu to refine the report. Depending on the selected time range and the data returned for that period, you can filter by user, country, region, posture profile, session type, device name, machine name, IP address, VPN profile, reason code, and Security Group Tag information. Some filters provide fixed choices, some provide values found in the report data, and some accept a value that you enter.

You can also hover over a supported value in a table column and select the search control to add that value to the applied filters. Use table settings to change the visible columns or table density. The report supports sorting for supported columns, including User, Region, and VPN Profile.

Select a row to expand its details. The expanded area can include Source, Endpoint Posture, Connection, and Tunnels information. Endpoint Posture details can include the posture attributes evaluated for the event and the posture profile used for the evaluation. If the posture profile is linked, select the link to open that posture profile.

For failed posture checks, the Remote Access Logs now provide a section in the details panel that include the status, the region, the affected posture profile, and any detected errors such as a disabled firewall or a missing executionable file.



You can schedule automatic delivery of Remote Access Log reports or export them as CSV files for further analysis. For more information, see Schedule a Remote Access Log report and Export Report Data to CSV.

The exported CSV file of Remote Access Logs includes the following columns: Date, Time, User, Device Name, Connection Event, Event Details, Public IP, Internal IP, VPN Profile, Session Type, OS Type and Versions, Secure Client Version, Session Duration, and Region.

View the Remote Access Log Report

Provides instructions for completing the View the Remote Access Log Report workflow in Cisco Secure Access. The Remote Access Log report lists users' connection events that are related to remote access, tracked over distinct time periods.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

The Remote Access Log report lists users' connection events that are related to remote access, tracked over distinct time periods.

Procedure

1. Navigate to **Monitor** > **Reports** > **Remote Access Logs**.
2. Choose a time frame of remote access events.
3. Use the search bar to find remote access events by identity or endpoint device OS version. Identity includes the columns **User** and **Device Name**.

   > **Note**
   >
   > If you have configured rules to traffic originating from IP addresses in network segments that include Security Group Tags, then you can search for connection events by SGT. When present, SGTs will be appended to the **User** column value. For more information, see Integrate ISE with Secure Access and Integrate Catalyst SD-WAN with Secure Access.

4. Refine your search using the following filters to help identify security issues that require attention.

   The filter menu can include the following filter types when they apply to the selected data:

   - Status
     - Connected
     - Disconnected
     - Failed
     - Warning
   - User
   - Machine Name
   - Device Name
   - IP Address
   - Country
   - VPN Profile
   - Posture Profile
   - Region
   - Session Type
   - Reason Code

  - Cert Auth Check
  - Posture Check
  - Authentication Check
  - Authorization Check
  - Addr Assignment Fail
  - TLS Check
  - IKEv2 Check
  - Unknown Failed Reason
  - Geocompliance Check
  - Access Allowed Geocompliance Service Unavailable
  - IP Assignment Failed
  - Unknown
  - AAA
  - User Requested
  - Connection Lost
  - Max Time Exceeded
  - Administrator Reset
  - IPSec Error
  - Client Type Not Supported
  - Connection Preempted
  - SA Expired
  - IKE Delete
  - Certificate Expired
  - Port Error
  - Posture Check Failed
  - Unknown Disconnection Reason
  - DDNS update failed
- OS Version
- Client Version
- **Security group tag** lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs. When present, SGTs are appended to the **User** column value. For more information, see Integrate ISE with Secure Access and Integrate Catalyst SD-WAN with Secure Access.

> **Note**
>
> Some filters provide fixed options, some display values found in the connection data, and some accept a value that you enter. A data-driven filter displays only option values that are present in the connection data for the selected time frame. If no option values are present, the filter remains hidden.

5. The table includes the following categories:
   - **User**–The name of the user in Secure Access.
   - **Device Name**–The name of the device in Secure Access.
   - **Connection Event**–The identity used to determine which policy applied to this activity
   - **Event Details**– The category of activity or action committed. Hover over this column to view the **Reason Code** and any **syslog info** related to the event.
   - **Public IPv4 Address**– The public-facing IPv4 address configured in the VPN profile.
   - **Assigned IPv4 Address**– The internal IPv4 address configured in the VPN profile.
   - **Assigned IPv6 Address**–The internal IPv6 address configured for the VPN profile.
   - **VPN Profile**– The name of the VPN profile associated with the event.
   - **OS Type and Versions**– The OS type and software version of the machine associated with the event.
   - **Secure Client Version**– The version of the Secure Client.
   - **Session Duration**– Duration of the session, if terminated.
   - **Region**– The region configured in the VPN profile that is associated with the event.
   - **Event Time**– The day, year, and timestamp of the event.

View Event Details

Provides instructions for completing the View Event Details workflow in Cisco Secure Access. There are two options to view details of an event.

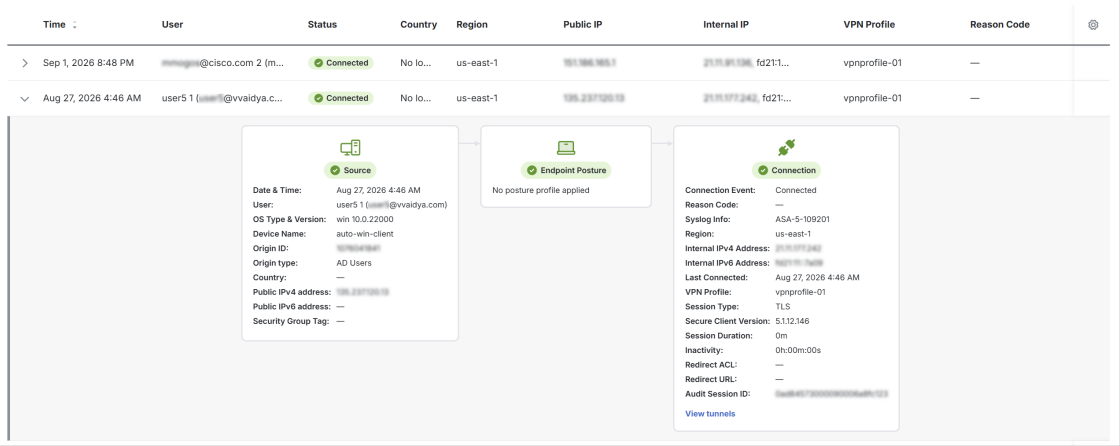
To view details of an event, perform the following steps:

Procedure

---

1. Navigate to **Monitor** > **Reports** > **Remote Access Logs**.
2. Click the expand icon at the start of any row.

   This expands the row and displays the event details.



What to do next

Result: The event details display in the expanded row as Source, Endpoint Posture, and Connection cards.

Extra information is available in the event details:

- **Last Connected** - The timestamp when this user was last connected to the machine.
- **Source** - The Source card can include Date & Time, User, OS Type & Version, Device Name, Origin ID, Origin type, Country, Public IPv4 address, Public IPv6 address, and Security Group Tag.
- **Endpoint Posture** - The Endpoint Posture card displays posture information. It can show the posture profile applied to the event or indicate that no posture profile is applied. Click the link to view the posture associated with the event.
- **Connection** - The Connection card can include Connection Event, Reason Code, Syslog Info, Region, Internal IPv4 Address, Internal IPv6 Address, Last Connected, VPN Profile, Session Type, and Secure Client Version. It can also display session duration, inactivity, redirect, security group tag, and audit session information.
- **Reason Code** - The reason code for VPN incompatibilities.
- **Syslog Information** - Syslog information related to the event you are examiningwith timestamps, syslog server IP, and indication of a logging message.

Review the following additional event details:

- **Duration** - The duration of the session.
- **Inactivity** - The amount of time that the session was inactive.
- **Redirect ACL** - The redirect access control (ACL) that originates from the user or device.
- **Redirect URL** - The URL where a user is automatically sent after attempting to access a different URL.
- **Security Group Tag** - The unique identifier assigned to a device or user, representing their security role or access level within the network.
- **Audit Session ID** - The unique identifier generated and associated with a user's process when they successfully log in or connect.
- **Tunnels** - Select **View tunnels** to view tunnel information. If the event includes more than one tunnel, select the corresponding tunnel tab to view each tunnel's details.

From your search results, you can click an identity or destination and go to its detailed report.

View Zero Trust Access Events in the Remote Access Log

Describes View Zero Trust Access Events in the Remote Access Log in Cisco Secure Access. From the Remote Access Log page (Monitor Reports Remote Access Logs) click the Zero trust Access tab.

View the Enrollment Logs

From the Remote Access Log page (**Monitor** > **Reports** > **Remote Access Logs**) click the **Zero trust Access** tab. This page displays all the enrollment activity and events for the users in your organization. Some columns may not generate data if they are not applicable to the type of device used to enroll.

The following aspects of the event is addressed:

- **Source** - The username that initiated the event or enrollment activity.
- **Event Type** - The type of event that triggered an action. Users are either Enrolled or Unenrolled.
- **Event Status** - The status of the event, whether it was successful or if it failed.
- **Event Details** -The category of activity or action committed. If there are failures, reasons for the failures are displayed here.
- **Public IP address** - The public-facing IP address configured in the VPN profile.
- **ZTA client version** - The version of the Zero Trust Access client.
- **OS Type and Versions** - The OS type and software version of the machine associated with the event.
- **Authentication Method** - The type of authentication used to validate the event. At this time supported authentication methods are SAM or Identity certificate.
- **Event Time** - The day, year, and timestamp of the event.

> **Note**
>
> In some instances, a single enrollment event generates multiple log lines depending on stage of enrollment. All events related to a single enrollment even will have the same **Enrollment ID**. This Enrollment ID field is available in the Event Details.

Columns are customizable. Click the gear icon in the upper right of the display table to modify which columns are included in your view. Ensure you **apply** the changes to save your selection.

Additionally, click the **Filters** button next to the advanced search bar to filter through the available results for specific components of the report. Use the **time range** drop-down option to search for a specific time frame; you can also add conditions through this option for specific dates that are not recent.

> **Note**
>
> You can recall previous searches made in the advanced search bar. Note that the recall feature only remembers searches made from your user account for the organization.

Scheduled Reports

You can schedule a report on the ZTA enrollment data in advance. See Schedule a Report for more information.

Export CSV

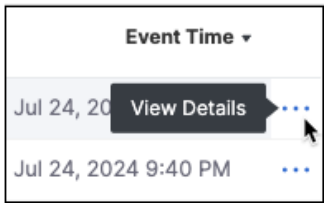
You can export the history of your organization or a specific query. See Export Report Data to CSV for more information.

View Zero Trust Access Enrollment Logging Event Details

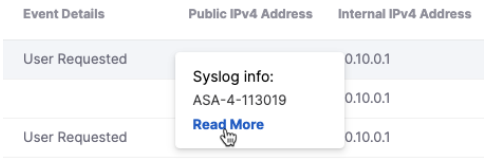
Provides instructions for completing the View Zero Trust Access Enrollment Logging Event Details workflow in Cisco Secure Access. Option 1: Click the View Details icon (the blue ellipsis at the right end of each row).

Procedure

1. **Option 1**: Click the **View Details** icon (the blue ellipsis at the right end of each row).



2. **Option 2:** Hover over an **Event Details** field in any row, then click **Read More** below the ASA syslog message ID.



What to do next

Result: The **Event Details** drawer displays detailed information about an individual event.

Extra information is available in the Event Details window:

- **Date & Time** - The timestamp when this event occurred.
- **Source** - The username that initiated the event or enrollment activity.
- **Event Status** - Denotes whether the action of the event is Successful or a Failure.
- **Authentication Method** - The type of authentication used to validate the event. At this time supported authentication methods are SAM or Identity certificate.
- **Public IP address** - The public-facing IP address configured in the posture profile.
- **Enrollment ID** - The unique Identifier
- **ZTA client version** - The version of the Zero Trust Access client.
- **Device** - The type of device detected in the event. This reflects the device of the user who initiated the event.
- **OS Type and Versions** - The OS type and software version of the machine associated with the event.
- **Event Detail** - A brief description of the category of activity or action committed.

From your search results, you can click an identity or destination and go to their respective detailed report.

Schedule a Remote Access Log Report

Describes Schedule a Remote Access Log Report in Cisco Secure Access. You can now schedule remote access log reports to be emailed to you at regular intervals.

You can now schedule remote access log reports to be emailed to you at regular intervals. The scheduled report email includes an HTML table preview of the report, a downloadable CSV file containing all available data, and a direct link to a live version of the report in the portal. Any filters applied in the Remote Access Logs view, such as connection event, event details, or identities, are reflected in the scheduled report, ensuring only relevant data is included.

Scheduling is supported for both VPN and Zero Trust remote access logs, allowing tailored reporting based on your security and compliance requirements.

> **Note**
>
> Data older than 30 days cannot be included in scheduled or exported reports.

For step-by-step instructions on how to schedule a report, see Schedule a Report.

82 Top Categories Report

Topics:

- Top Categories Report

Provides an overview of Top Categories Report in Cisco Secure Access, including Top Categories Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Top Categories Report

Describes Top Categories Report in Cisco Secure Access. The Top Categories report is a list of the top security and content categories by DNS and firewall requests for your organization over the selected period.

The **Categories** tab in **Top Reports** compares category request and web traffic activity for the selected time range.

> **Note**
>
> **Packages and Feature Availability**
>
> Not all features described here are available to all Secure Access packages. For more information, see Determine Your Current Package. If you encounter a feature described here that you do not have access to, contact your sales representative for more information.

View the Top Categories Report

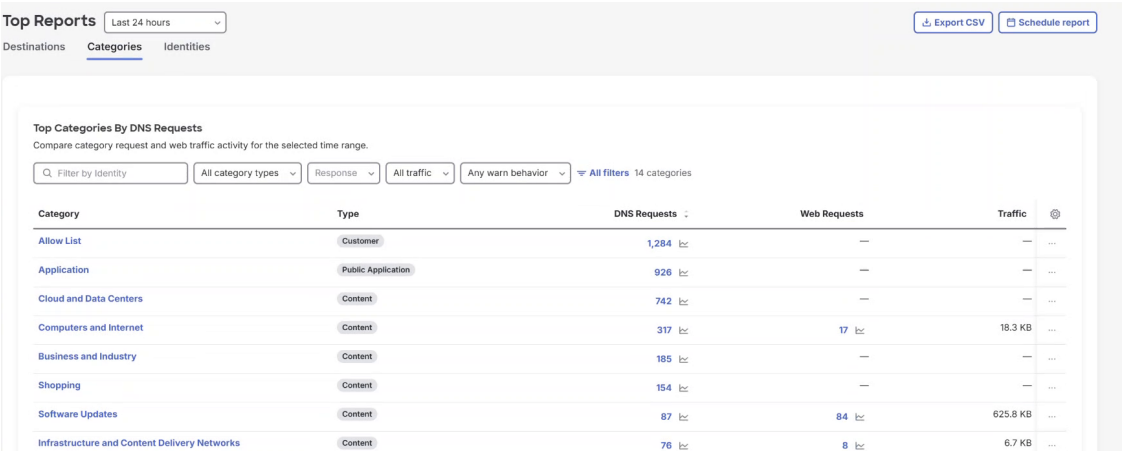
Provides instructions for completing the View the Top Categories Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Reports**, then select **Categories**.



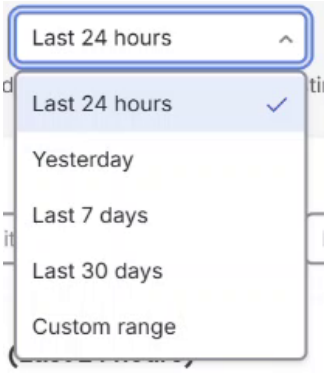
Report Fields

- **Category** –The threat or content category item. Clicking a category name redirects you to the Category Details section.
- **Type**–The category type, such as Security, Content, Customer, or Public Application.
- **Traffic** –The total bandwidth of proxy requests uploaded and downloaded for this category.
- **DNS Requests** and **Web Requests** –Separate request counts for each category. Click a request count to view more information:
  - The total requests for the selected period

- Which of the requests were blocked and which were allowed
- The most active identities (the identities that have requested the category the most)

2. Choose a time range from the drop-down beside **Top Reports**.

   Select a predefined period or Custom range.



3. Select **All category types** above the table to show all category types, Security, or Content.



4. Use **Response** above the table to filter requests by Allowed, Blocked, or both.

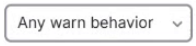
   Leave the choices unselected to show all responses.



5. Select **All** traffic above the table to filter the traffic type.



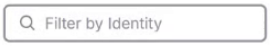
6. Use Any warn behavior above the table, or **All filters** > **Warn Page Behavior**, to filter warning behavior.



7. Open All filters, choose Identity Type, and select the required types. Click **Done** to close Filters.

   With no types selected, all identity types are included.

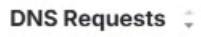
   Search by identity if you know the identity name.



8. Use the sort control beside DNS Requests in the table heading to change the sort order.

   Ascending or Descending Order

   - **Descending** –Show the results in descending order. By default, descending is selected.
   - **Ascending** –Show the results in ascending order.



What to do next

Once you have chosen all filters and sorting options, the report will reflect the appropriate results.

Top Categories Quick View

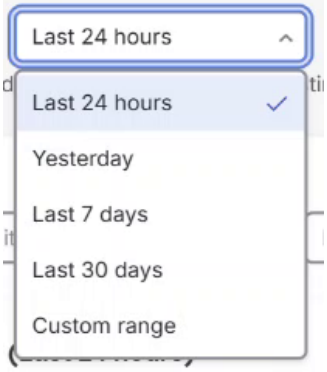
Provides instructions for completing the Top Categories Quick View workflow in Cisco Secure Access. The quick view for Top Categories displays the most active identities and their respective requests for each individual category.

The quick view for Top Categories displays the most active identities and their respective requests for each individual category.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts

Procedure

1. Choose a time frame within which to view the quick view details.You can see details for the last 24 hours, the previous calendar day (yesterday), the last 7 days, the last 30 days, or a custom range within the last 90 days.



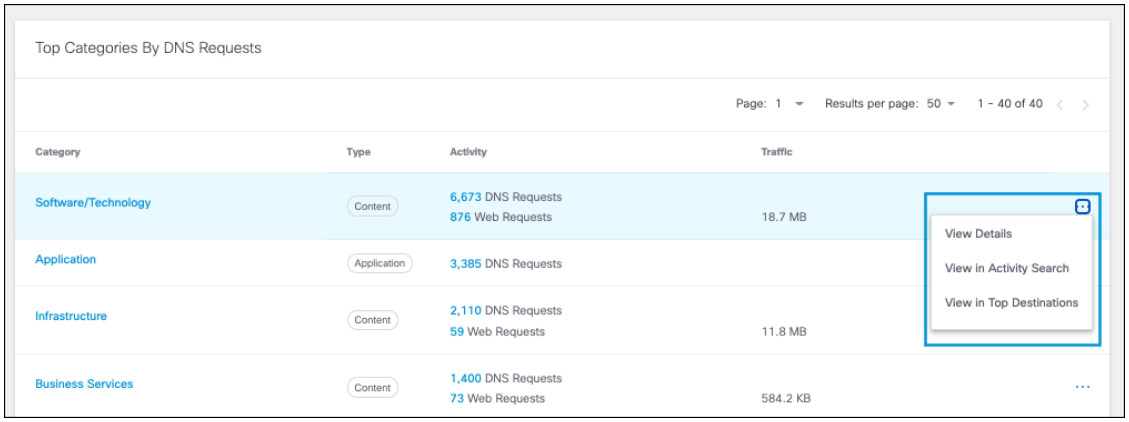
2. Click a request count in the DNS Requests or Web Requests column for the category you wish to examine. A modal appears with a graph displaying the total requests of that traffic type over the selected time period and the total number of allowed requests. The most active identities with requests in this category are also displayed.
3. Optionally, click **Full Details** to open the Category Details for this category.

View Category in Other Reports

Describes View Category in Other Reports in Cisco Secure Access. Viewing the category in other reports provides you with insights into how your organization accesses a destination category and what activities are involved.

Viewing the category in other reports provides you with insights into how your organization accesses a destination category and what activities are involved. In the Top Categories report, each category can be explored further by accessing the View Menu. Clicking this menu (the "...") reveals three options:

- **View Details** – Redirects you to that category's details.
- **View in Activity Search**–Redirects you to the Activity Search report filtered by that category.
- **View in Top Destinations**–Redirects you to the Top Destinations report filtered by this category.



Category Details

Describes Category Details in Cisco Secure Access. The Category Details for an individual category provide you with a focused view of the category's traffic and related sources and domains for a selected time period.

The Category Details for an individual category provide you with a focused view of the category's traffic and related sources and domains for a selected time period.

View a Category's Details Overview

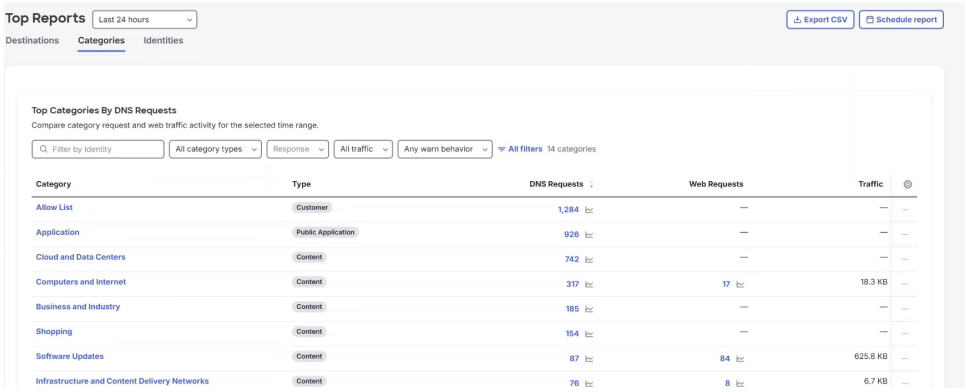
Provides instructions for completing the View a Category's Details Overview workflow in Cisco Secure Access. Navigate to Monitor Reports Top Categories and click one of the listed categories.

Before you begin

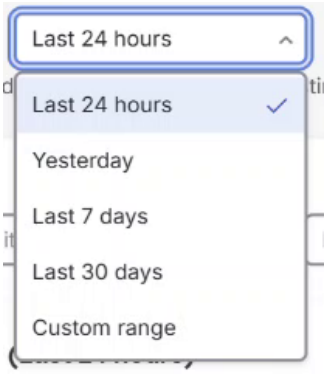
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Reports**, select Categories, and click a category..



2. Choose a time period within which to view the results. The details can be filtered by the last 24 hours, the previous calendar day (yesterday), the last seven days, the last 30 days, or a custom range within the last 90 days.



View a Category's Traffic

Describes View a Category's Traffic in Cisco Secure Access. The first graph depicts the traffic over a selected time period for this category.

The first graph depicts the traffic over a selected time period for this category.

View the Activity Breakdown

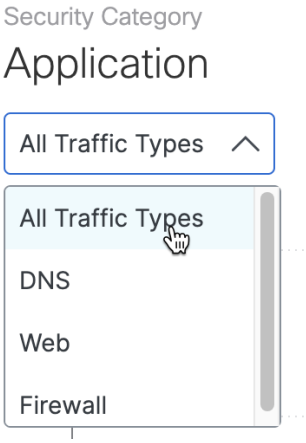
Provides instructions for completing the View the Activity Breakdown workflow in Cisco Secure Access. Click a category and navigate to the traffic graph on the details page.

Procedure

1. Click a category and navigate to the traffic graph on the details page. Select **Activity Breakdown**.

   The Activity Breakdown displays the number of DNS requests and proxy transactions for the selected time period.

2. Filter the Activity Breakdown to view All Traffic Types (default), DNS, Web, or Firewall.



   You can also choose a traffic type from All traffic on the **Categories** tab before opening category details. IP requests are not an option in Category Details.



3. Hover over a date and time to reveal details about the requests made at that time.

The dotted line provides available data that is still being processed. Hover over the point on the graph to see how many requests are currently processed.

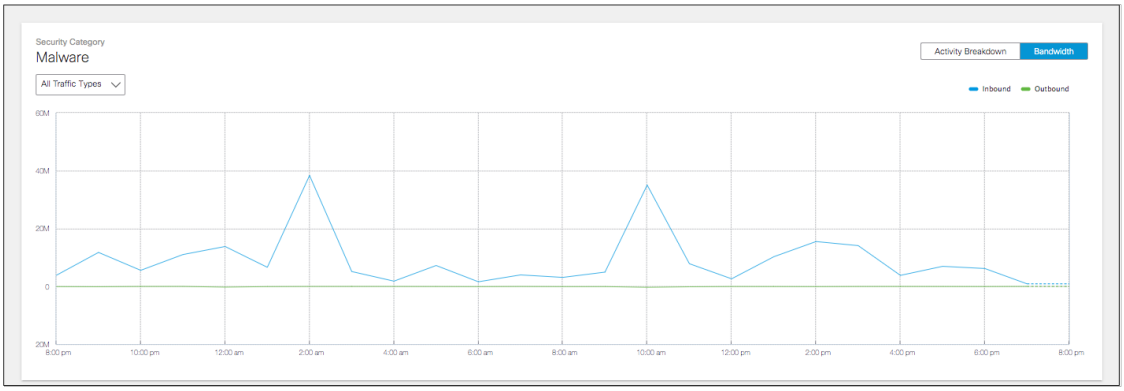
View the Traffic Bandwidth

Provides instructions for completing the View the Traffic Bandwidth workflow in Cisco Secure Access. Click a category and navigate to the traffic graph on the details page.

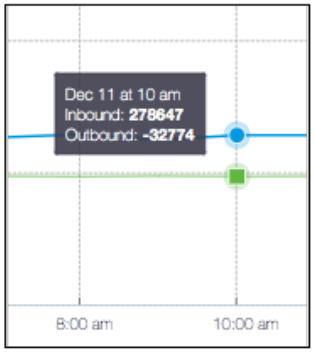
Procedure

1. Click a category and navigate to the traffic graph on the details page. Select **Bandwidth**.

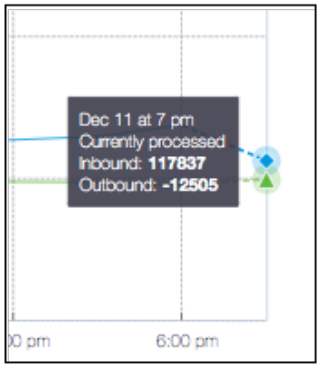
   For proxy transactions, the bandwidth view of the line graph shows the number of inbound and outbound traffic for the selected time period.



2. Hover over a specific date and time to reveal details about the traffic at that time.



   The dotted line provides available data that is still being processed. Hover over the point along the graph to see the inbound and outbound traffic details currently processed.

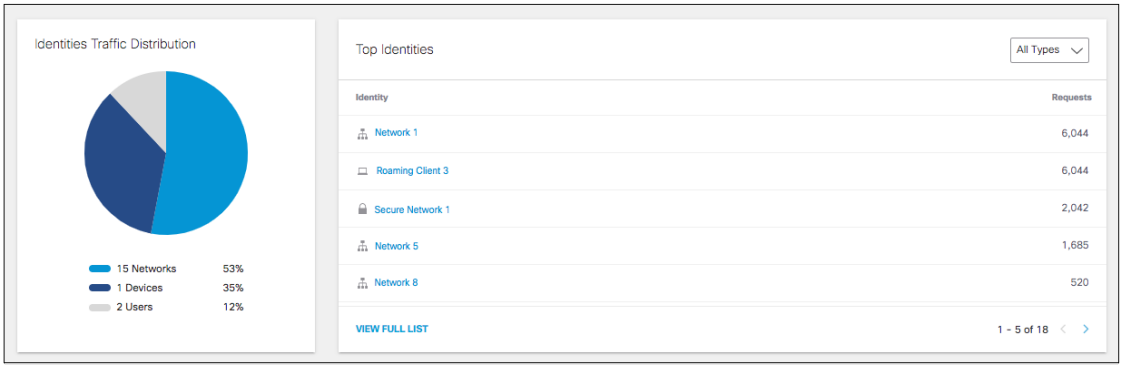


View a Category's Identities

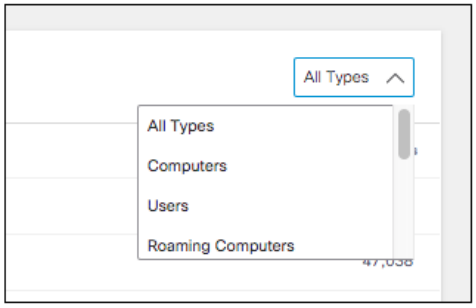
Describes View a Category's Identities in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

1. Navigate to the identities section of the report.
2. View the Identities Traffic Distribution. The pie chart provides a breakdown of the identity types that have made requests for the category for the selected time period.
3. View the top identities making requests associated with this category.

- **Identity** –The name of the identity.
- **Requests**–The number of category requests the identity has made during the selected period.



You can filter which identity types are listed by selecting an identity type from the drop-down.



View the Category's Top Domains

Provides instructions for completing the View the Category's Top Domains workflow in Cisco Secure Access. Navigate to the Top Domains section of the report.

Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

Navigate to the *Top Domains* section of the report. This list depicts the top domains where requests were flagged for this category:

What to do next

- **Domain Name** –The domain name, such as example.com.
- **Other Categories**–If there are other categories associated with the domain in addition to the current category being viewed, they are listed here.
- **Allowed**–The number of requests allowed for this domain for the selected time period.
- **Blocked**–The number of requests blocked for this domain for the selected time period.
- **Requests**–The number of requests made for this domain for the selected period.

Click a domain to open the Destination Details. Click View Full List to open the Destinations tab in Top Reports, filtered by this category.

83 Top Destinations Report

Topics:

- Top Destinations Report

Provides an overview of Top Destinations Report in Cisco Secure Access, including Top Destinations Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Top Destinations Report

Describes Top Destinations Report in Cisco Secure Access. The Top Destinations report lists the top domains your organization has made access requests to over the selected time period.

The Top Destinations report lists the top domains your organization has made access requests to over the selected time period. It is filterable, schedulable, and you can export the results to a CSV file.

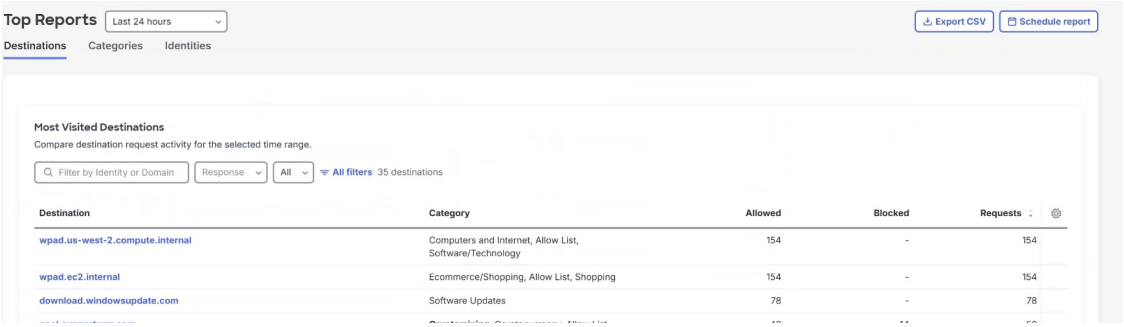
View the Top Destinations Report

Provides instructions for completing the View the Top Destinations Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Reports**, then select **Destinations**.

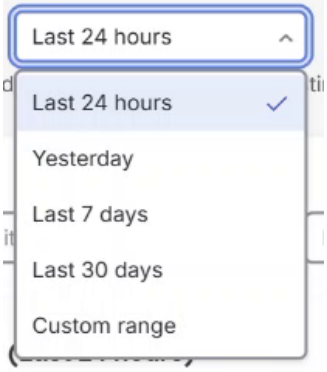
   The Most Visited Destinations table opens.



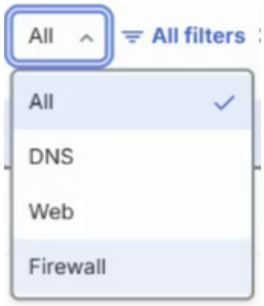
   The following information is displayed for each destination:

   - **Destination**–The domain.
   - **Category**–The category, such as Malware, Business Services, Phishing, and so on.
   - **Allowed**–The number of requests to that destination that were allowed.
   - **Blocked**–The number of requests to that destination that were blocked.
   - **Requests**–The number of requests for the domain for the selected period.

2. Choose a time range from the drop-down beside Top Reports.

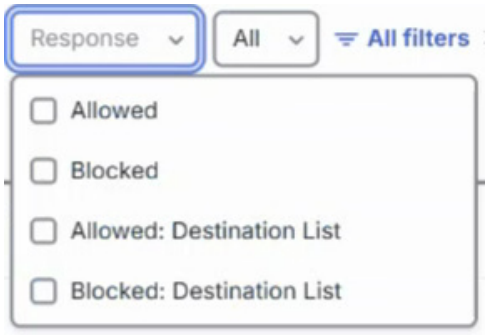


3. Use the traffic drop-down above the table to select All, DNS, Web, or Firewall.

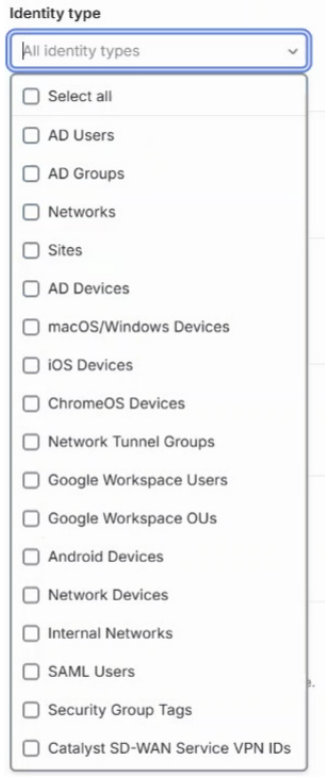


4. Click **Response** above the table and select Allowed, Blocked, Allowed: Destination List, or Blocked: Destination List.

   With no choices selected, all responses are included.



5. Open **All filters**, select **Identity type**, choose the required types, and click **Done**.

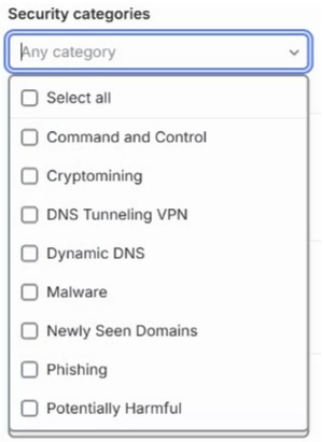


   Alternatively, if you are looking for a specific identity to filter your results, enter it in the search bar. You can also filter by a specific domain.



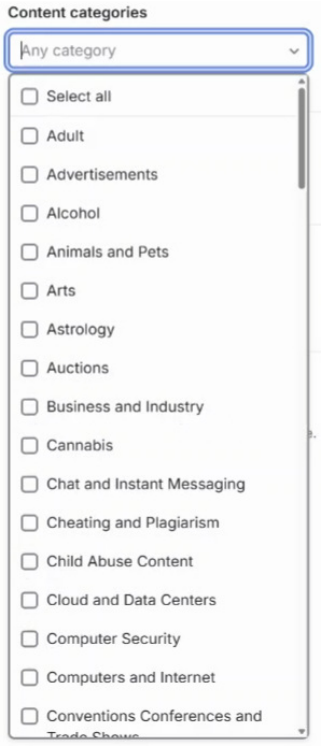
6. In **All filters**, choose **Security categories**, select the required categories, and click **Done**.

   For more information, see Threat Categories.

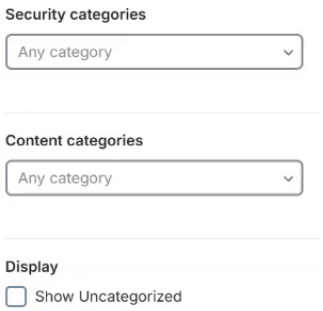


7. In **All filters**, choose **Content categories**, select the required categories, and click **Done**. .

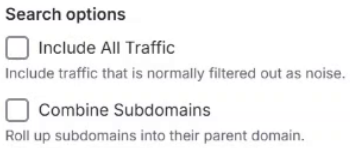
   For more information about content categories, see Manage Content Categories



   Alternatively, select **Show Uncategorized** under **Display** in **All filters** to show requests that do not match a category.



8. Open **All filters** and use **Search options** to select **Include All Traffic** or **Combine Subdomains**.
   - **Include All Traffic**–Includes data from all domains including noisy domains filtered out by default.
   - **Combine Subdomains**–Combines all subdomain requests from a parent domain and lists the combined requests under the parent domain.



Click **Done** to close Filters and review the results. Use Clear filters to reset filter selections.



View Further Details

Describes View Further Details in Cisco Secure Access. Clicking any destination in the report table redirects you to the Destination Details for that domain.

Clicking any destination in the report table redirects you to the Destination Details for that domain.

Destination Details

Describes Destination Details in Cisco Secure Access. The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs.

The Destination Details report provides access to information about the destinations that your identities are visiting, determining which are the most actively requested and when this activity occurs. Here you can explore activity at the domain level, determining who has visited the selected domain and when. This detailed information can help you determine if any computer or networks may be compromised or are connecting to known malicious sites so that you can better protect yourself and others.

View the Destination Details

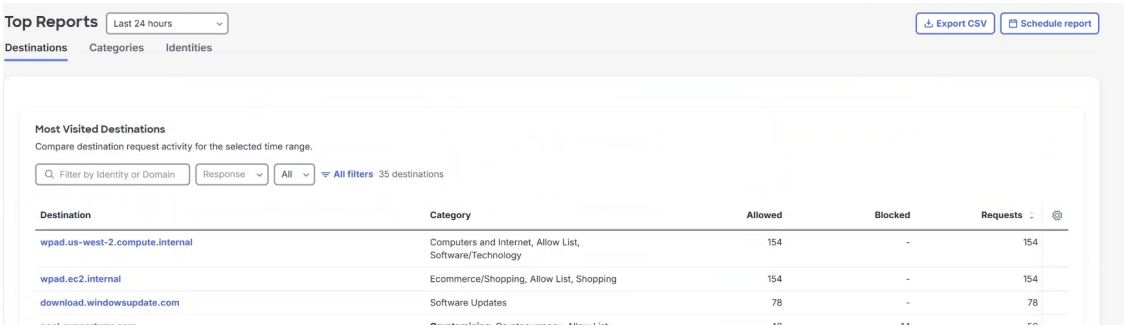
Provides instructions for completing the View the Destination Details workflow in Cisco Secure Access. Navigate to Monitor Reports Top Destinations and click a Destination.

Before you begin

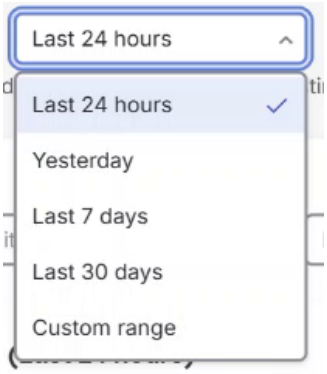
A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Monitor** > **Reports** > **Top Reports**, select **Destinations** and click a destination.

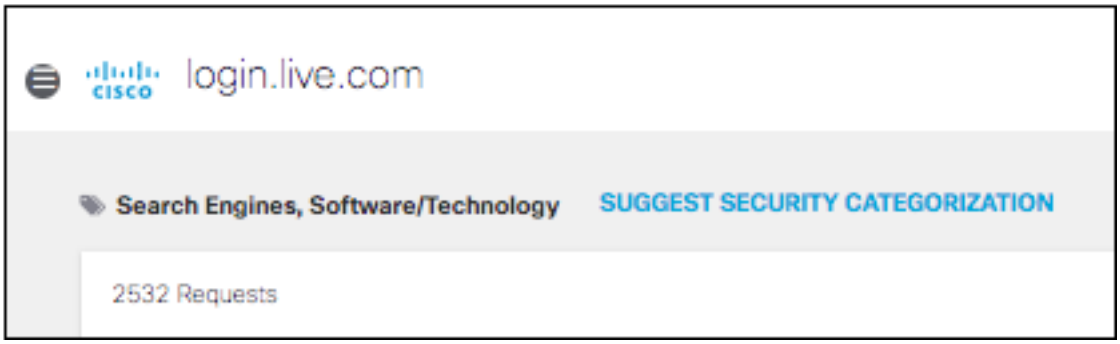


2. Choose a time frame within which data is displayed.

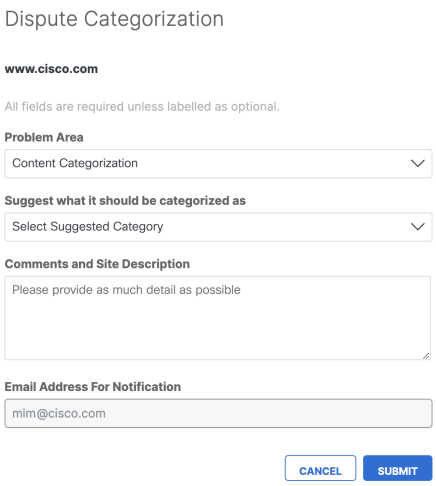


3. View the destination's content and threat categories.

   At the top of the report, under the domain for the destination you are viewing, are any categories associated with the destination. For category definitions, see Manage Content Categories and Manage Threat Categories.



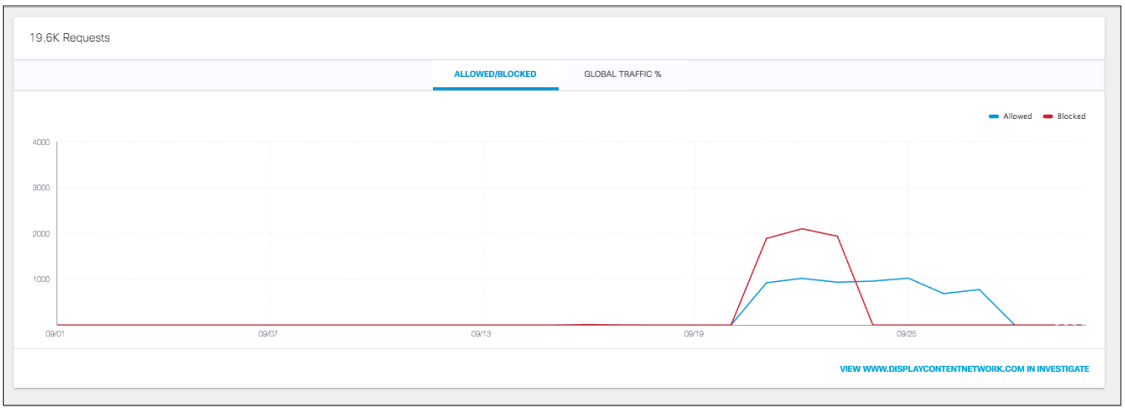
   If you believe this destination belongs in a security category, click **Suggest Security Categorization**, fill out the request form that creates an internal Secure Access ticket for a security researcher to review, and click **Submit**.



View the Request Traffic

Describes View the Request Traffic in Cisco Secure Access. The traffic graph displays the traffic for the type selected (blocked, allowed, or both) within the selected time period.

The traffic graph displays the traffic for the type selected (blocked, allowed, or both) within the selected time period. This enables you to visualize when there are more active requests for this destination and if these requests are allowed or blocked.



View Requests by Blocked or Allowed

Provides instructions for completing the View Requests by Blocked or Allowed workflow in Cisco Secure Access. Click on Allowed, Blocked, or both to view those requests in the traffic graph.

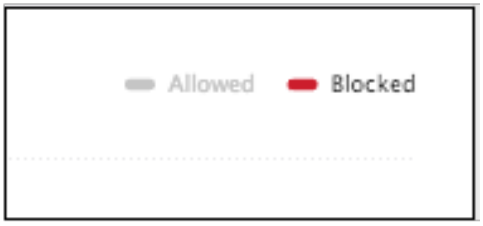
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

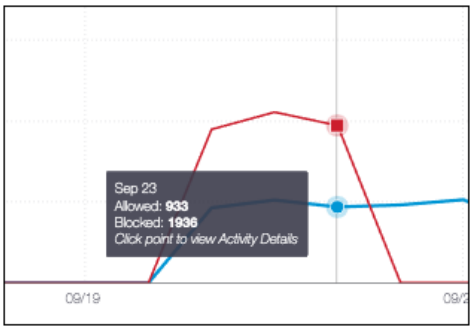
1. Click on **Allowed**, **Blocked**, or both to view those requests in the traffic graph.

   The graph displays the number of blocked and allowed requests for the destination that you are viewing within the selected time period. You can choose to see both Allowed and Blocked requests or one or the other individually. By default, only Allowed are shown initially.



2. Hover over a point on the graph to reveal the date and time and the number of Blocked and Allowed requests at that point.

   Clicking the point will redirect you to the Activity Search Report filtered by this domain and the Response (Blocked or Allowed) selected.



View Requests Through Global Traffic %

Provides instructions for completing the View Requests Through Global Traffic % workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

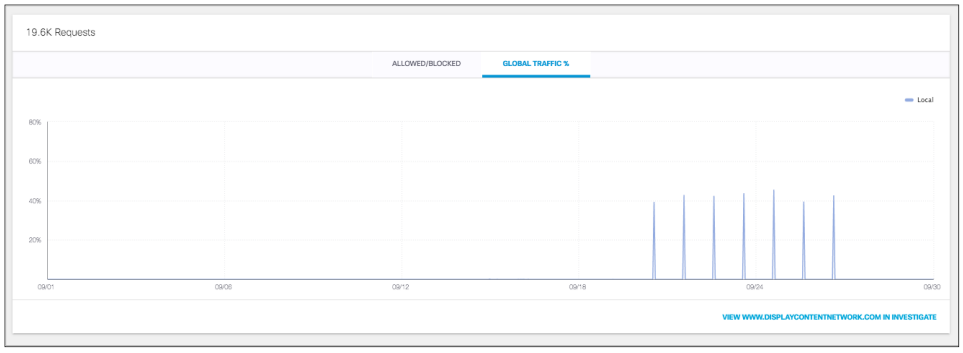
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

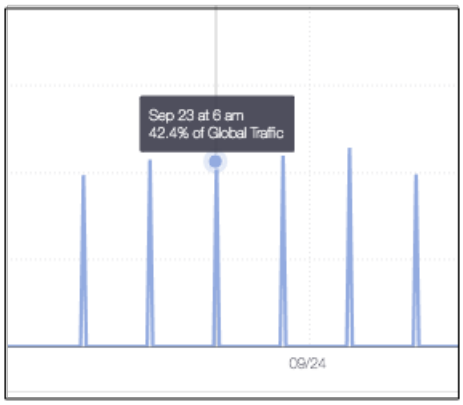
Procedure

1. Click **Global Traffic %** on the traffic graph.

   The Global Traffic % chart displays the percentage of global traffic to this specific destination that is comprised of local traffic from your organization's Identities.



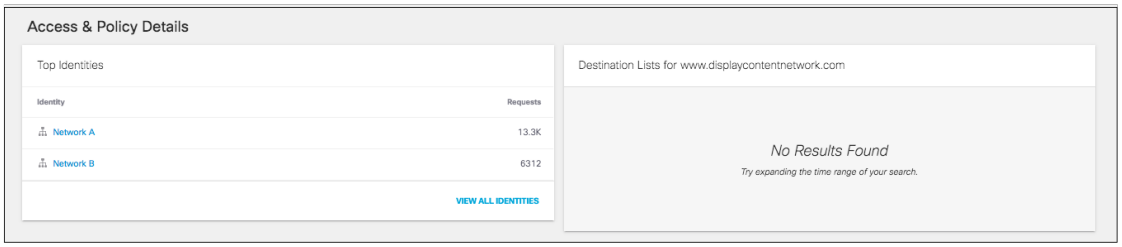
2. Hover on a point to view the date, time, and percentage of global traffic at that time.



View the Access and Policy Details

Provides instructions for completing the View the Access and Policy Details workflow in Cisco Secure Access. The Access and Policy Details presents information related to identities accessing the destination and if the destination belongs to any Destination List policies.

The Access and Policy Details presents information related to identities accessing the destination and if the destination belongs to any Destination List policies.



Before you begin
A minimum user role of Read-only. For more information, see Manage Accounts.

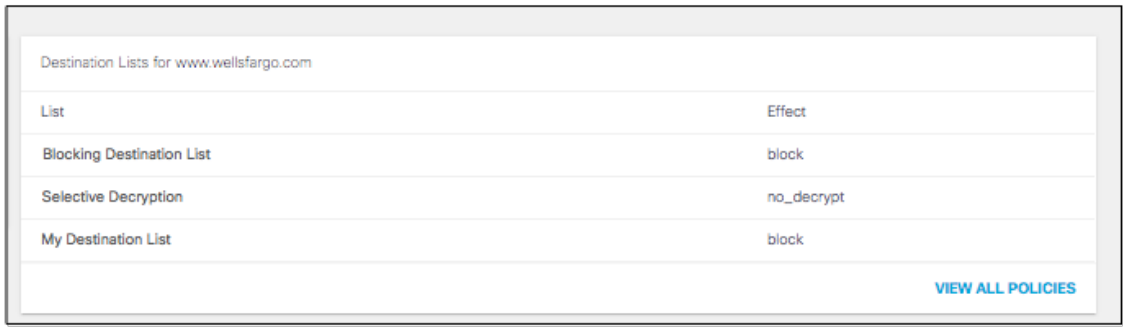
Procedure

1. Navigate to the **Access & Policy Details** > **Top Identities**.

   The Top Identities lists the sources that had the most requests for access to this destination.

2. Navigate to the **Access & Policy Details** > **Destination Lists**.

   The Destination Lists table shows if this domain belongs to any Destination Lists in your rules and what effect that list would have on the domain.



View Recent Activity

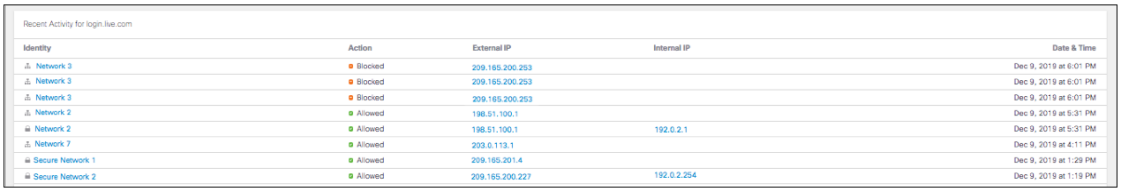
Provides instructions for completing the View Recent Activity workflow in Cisco Secure Access. The Recent Activity chart lets you investigate DNS activity for this destination.

Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

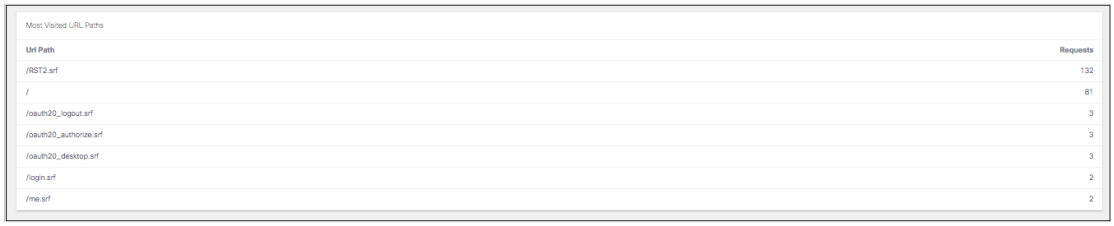
The Recent Activity chart lets you investigate DNS activity for this destination. You can view the identities that requested the destination, the action (response) to that request (Blocked or Allowed), the external and internal IP addresses, and the date and time of the request. Viewing this information enables you to make decisions about how to best maintain your destination lists. Click **View All Activity** to open the Activity Search Report filtered by this domain.



View the Most Visited URL Paths

Describes View the Most Visited URL Paths in Cisco Secure Access. This chart lists the most frequently visited URL paths for this domain and the number of requests for each path within the requested time period.

This chart lists the most frequently visited URL paths for this domain and the number of requests for each path within the requested time period.



84 Total Requests Report

Topics:

- Total Requests Report

Provides an overview of Total Requests Report in Cisco Secure Access, including Total Requests Report. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Total Requests Report

Describes Total Requests Report in Cisco Secure Access. The Total Requests Report provides a visualization of traffic over a given time period.

The Requests over time tab in Traffic Reports visualizes traffic over a selected time period. Filter by categories, traffic type, responses, and identities to review traffic trends in your environment.

View Trends in the Total Requests Report

Provides instructions for completing the View Trends in the Total Requests Report workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

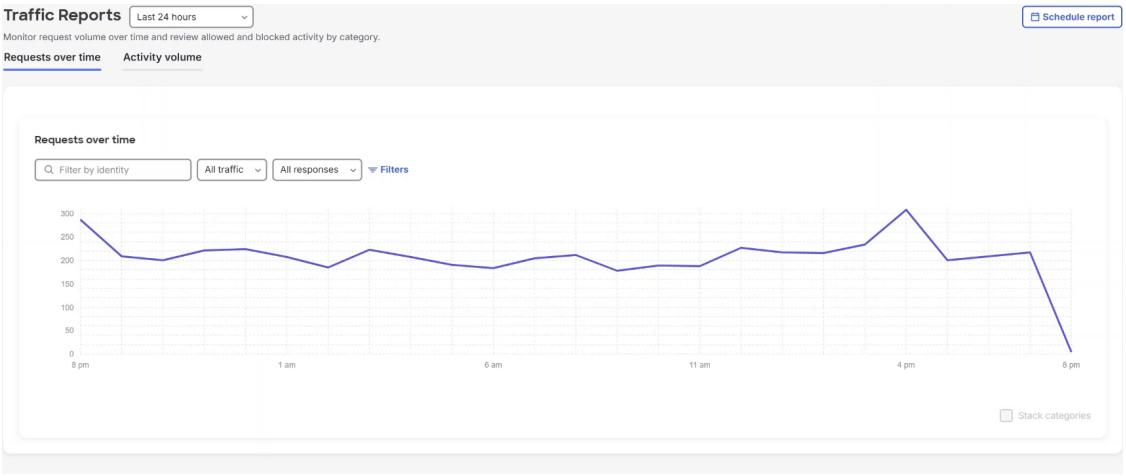
Before you begin

A minimum user role of Read-only. For more information, see Manage Accounts.

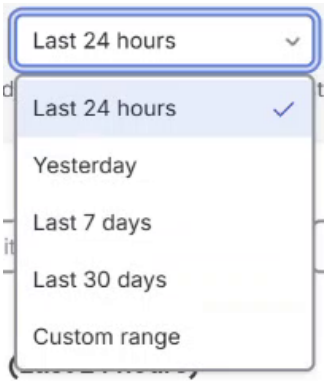
Procedure

1. Navigate to **Monitor** > **Reports** > **Total Reports**, and select **Requests over time**.

   Filters opens the drawer.



2. Choose a time frame above the report: Last 24 hours, Yesterday, Last 7 days, Last 30 days, or Custom range.

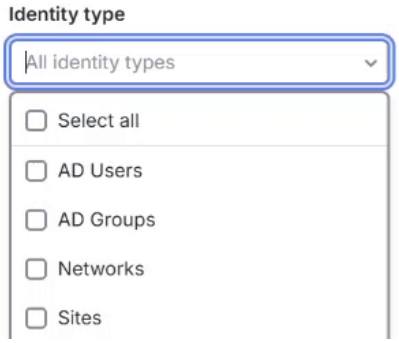


3. Use All responses above the graph, or Response in Filters, to choose **Allowed** or **Blocked**.

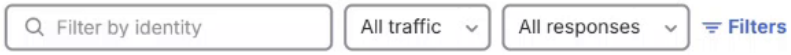
   All responses are shown by default.



4. In Filters, open Identity type and select the identity types to include.



Alternatively, enter a specific identity in Filter by identity above the graph.



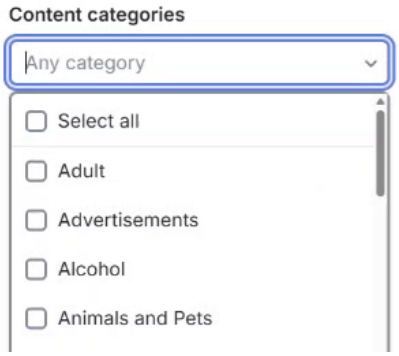
5. In Filters, choose **Security categories**.

For more information about threat categories, see Manage Threat Categories and Threat Category Descriptions.

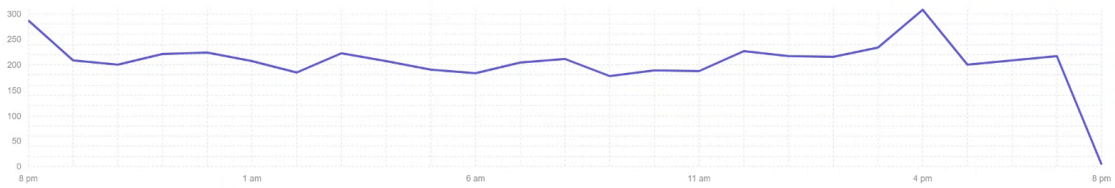


6. In Filters, choose **Content categories**, then select **Done**.

For a full list of content categories, see Available Content Categories.



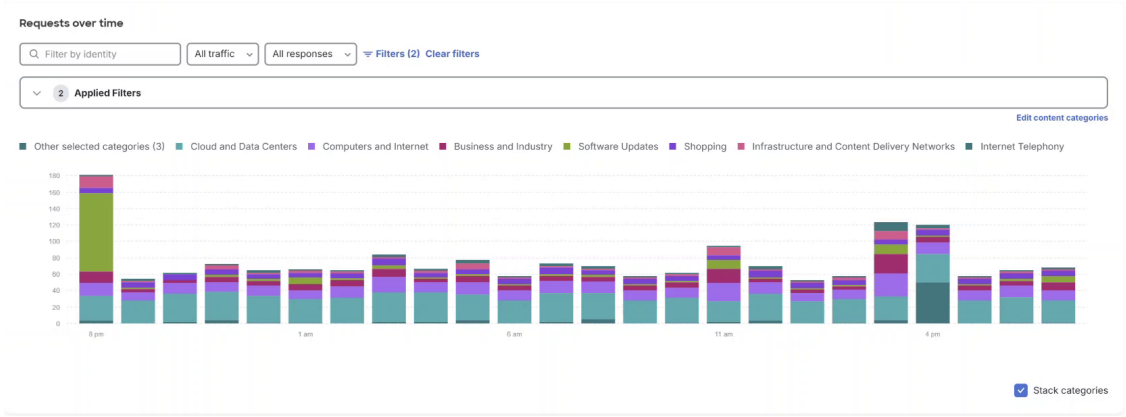
Select **Done** to close Filters. Applied filters appear above the updated graph. With no security or content categories selected, the graph remains a line for the selected time frame, responses, and identities.



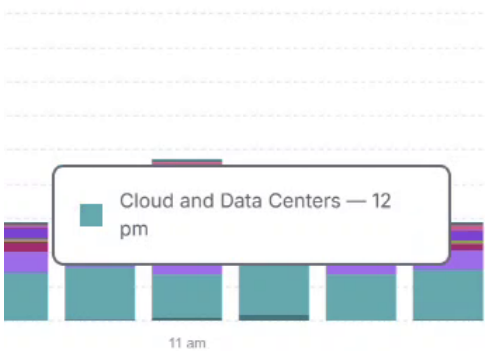
Hover over a point on the graph to see its total request count.



When security or content categories are selected, the graph shows those categories for the selected time frame and filters. Select **Stack categories** to show their values as stacked bars at each timestamp.



Hover over a category segment to identify the category and time represented by that segment.



You can also view the categories unstacked by clearing the **Stack categories** checkbox.

Hovering on a point on the graph will show the total requests for that category at that time.

Clicking a category on either graph type will redirect you to the Category Details for that category.

Part VII

Integrations

Topics:

- Secure Access Integrations
- Cisco Security for Chromebook Client

Integrating Secure Access with external devices and platforms.

85 Secure Access Integrations

Topics:

- Manage Third-Party Integrations
- Chrome Enterprise Browser
- Microsoft Intune Third-Party Integration
- Jamf Pro Third-Party Integration
- Push Security Events Third-Party Integration
- Microsoft Edge for Business Third-Party Integration
- Island Enterprise Browser Third Party Integration
- Threat Intelligence Feeds
- Manage Webhooks for Third-Party Integrations
- Integrate ISE (Identity Services Engine) with Secure Access
- Integrate Catalyst SD-WAN with Secure Access
- Integrate Cisco Identity Intelligence with Secure Access

Provides an overview of Secure Access Integrations, including Manage Third-Party Integrations, Chrome Enterprise Browser, and Microsoft Intune Third-Party Integration. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

Manage Third-Party Integrations

Understand the integrations available with Secure Access.

A Secure Access third-party integration enhances an organization's network management and security services with third-party applications or systems. Third-party integrations require the configuration of resources in Secure Access and third-party products.

For information about configuration requirements or procedures for third-party products, consult the third-party product documentation.

Secure Access supports third-party integrations with these products:

- Chrome Enterprise Premium Browser–The integration of Chrome Enterprise Premium Browser with Secure Access enables easy and secure onboarding of remote workers, contractors and third-party users to access private applications.
- Microsoft Intune –The integration of Microsoft Intune with Secure Access enhances device management and ensures secure access and compliance across your organization devices.
- Jamf Pro –The integration of Jamf Pro with Secure Access streamlines device management and enhances security, deployment and compliance across platforms.
- Microsoft Edge – The Microsoft Edge for Business integration provides a secure enterprise browser with built-in security, AI controls, and seamless management at no additional cost with Microsoft 365 licenses. This integration is designed to enable secure access to private applications, particularly in scenarios involving unmanaged devices.
- Island– The Island integration with Cisco Secure Access enables secure access to private applications, for unmanged devices, ensuring protected connectivity to sensitive resources.

Secure Access supports third-party integrations with a Webhook. A Webhook supports notifications for Secure Access Push Security Events and Secure Access Alert Rules. For more information, see:

- Manage Webhooks
- Push Security Events
- Monitor Secure Access with Alert Rules

Additional Secure Access Integration Guides

Lists the end-to-end integration guides that are available for certain Secure Access integrations.

The following additional documents are available to guide you through the end-to-end process of integrating with Secure Access:

- Secure Access SD-WAN Integration with Arista VeloCloud
- Secure Access SD-WAN Integration with HPE Aruba Networking EdgeConnect

Chrome Enterprise Browser

Integrate Chrome Enterprise Browser with Secure Access to enable conditional access policies and restrict access to private resources to authorized employees and contractors.

Cisco Secure Access integrates with Chrome Enterprise to provide secure access to corporate resources and applications, particularly within a managed environment. This combination offers a robust solution for secure remote access and data protection.

Enterprise browsers enable conditional access policies restricting private resource application access to authorized employees and contractors connecting through the browser using an endpoint with a healthy security posture. Enterprise browsers also alleviate the concerns over unmanaged devices, reducing the risk of data exfiltration and reducing the complexity of implementing security controls.

Chrome Enterprise builds upon the standard Chrome browser and is designed for businesses, offering enhanced deployment, management, and security features, while the consumer version is the standard Chrome browser for personal use.

The Google Admin console allows IT administrators to manage various Google products for their organization, including the Chrome and Chrome Enterprise browsers.

For administrators who manage Chrome browser or ChromeOS devices for a business or school, the Chrome Enterprise Connectors Framework offers a collection of connectors and APIs that simplify the steps needed to integrate Chrome Enterprise browser and ChromeOS with Secure Access.

Important

To integrate Chrome Enterprise browser with Secure Access you'll need to configure the Secure Access Enterprise Connector (i.e. IdP Agnostic Browser Trust) in the Chrome Enterprise dashboard. This provides the required URL patterns and service account name parameters for your Secure Access org. For more information, see Chrome Enterprise Connectors Framework.

Configure the Chrome Enterprise Browser Third-Party Integration

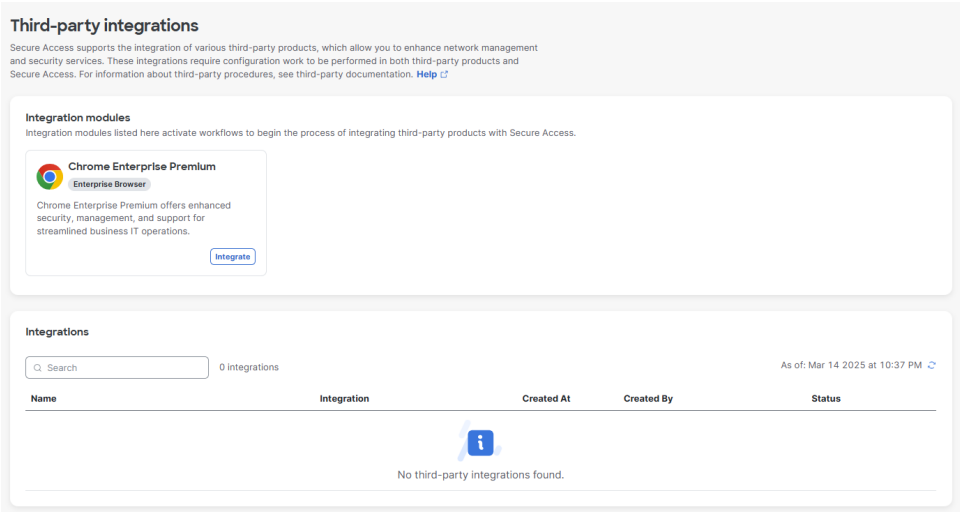
Provides instructions for completing the Configure the Chrome Enterprise Browser Third-Party Integration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

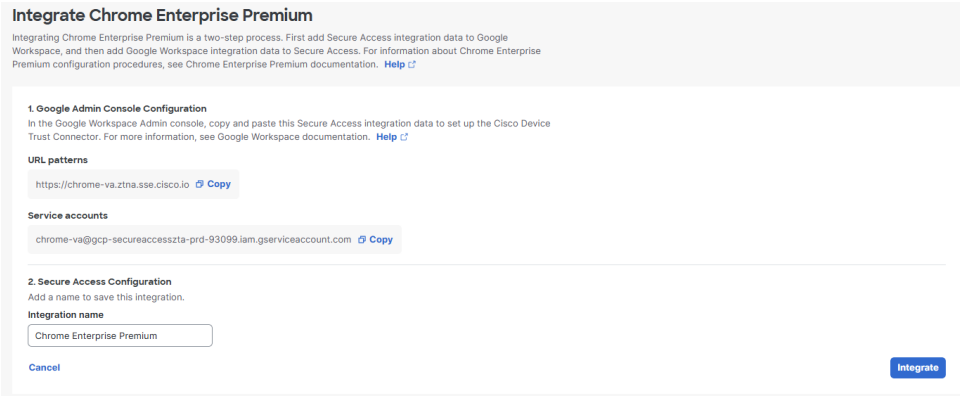
- Full Admin user role. For more information, see Manage Accounts.
- Access to the Google Admin Console. You'll need an administrator account for access the Admin console.
  - To get a Google Admin administrator account, you need to have a domain-verified Google Workspace or Cloud Identity account and then sign in to the Google Admin console at admin.google.com using your administrator credentials.
- A configured Chrome Enterprise connector for your Secure Access org.
  - To configure a Chrome Enterprise connector, you'll need to sign in to the Google Admin console, navigate to **Devices** > **Chrome browser** > **Connectors**, and then choose the provider and set up the configuration details, including testing the connection and adding the configuration. For more information, see Cloud-managed Chrome browser.

Procedure

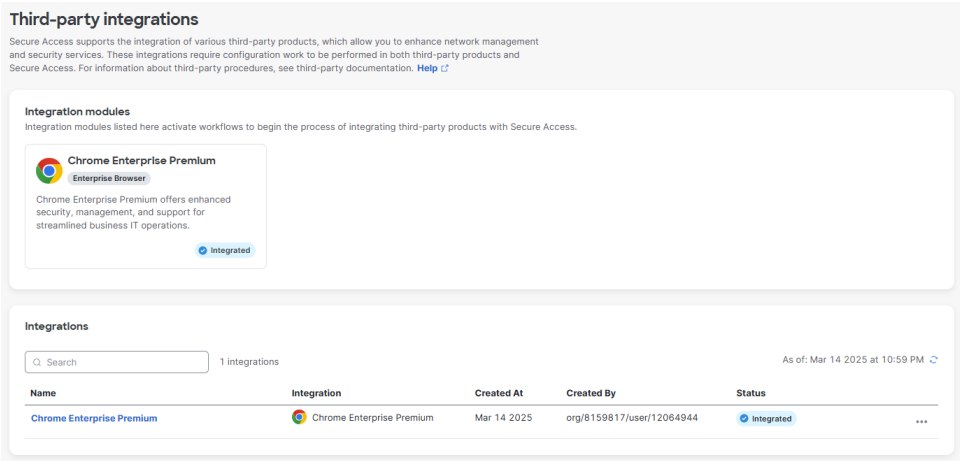
1. Navigate to **Admin** > **Third-party Integrations** and click **Integrate**.



2. In the Google Admin console, copy and paste this Secure Access integration data to set up the Google Chrome Enterprise Device Trust Connector for Secure Access.



3. Enter an **Integration name** for this configuration and click **Integrate** to complete the integration.



4. Click the ellipse menu (**...**) to view or modify the integration name.

   The **URL patterns** and **Service accounts** information is available in read-only format.

What to do next

Define a browser-based **Zero Trust Connection** endpoint posture profile for the Chrome Enterprise browser. For more information, see Manage Zero Trust Access Posture Profiles.

Microsoft Intune Third-Party Integration

Integrate Microsoft Intune with Secure Access to enhance device security enforcement, improve compliance, and centralize device management.

Cisco Secure Access integrates with Microsoft Intune to streamline device management and strengthen security compliance across your organization's devices.

What is Microsoft Intune?

Microsoft Intune is a cloud-based endpoint management solution that allows organizations to manage user access to corporate resources. It simplifies application and device management for a wide range of endpoints, including mobile devices, desktops, and virtual machines.

By integrating Microsoft Intune with Cisco Secure Access, you can:

- Enhance Security Enforcement: Cisco Secure Access uses device data from Intune to assess endpoint posture and enforce security policies.
- Improve Compliance: Ensure devices comply with organizational security standards before granting access to sensitive resources.
- Centralize Device Management: Manage and monitor device health and compliance from a single, unified platform.

When Microsoft Intune integration is configured, Cisco Secure Access receives device posture information from Intune. This data enables Cisco Secure Access to:

- Evaluate device compliance status.
- Apply appropriate security policies based on real-time device data.
- Restrict or allow access to organizational resources according to policy requirements.

Configure the Microsoft Intune Third-Party Integration

Provides instructions for configuring the Microsoft Intune Third-Party Integration workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts
- Administrator access to the Microsoft Intune admin center. For more information, see Tutorial: Walkthrough Microsoft Intune admin center.

Procedure

1. Navigate to **Admin** > **Third-party Integrations** > **Microsoft Intune** and click **Integrate**.
2. Enter integration details.
   a) **Integration name**: Enter a descriptive name that will help you identify the purpose of the integration in Secure Access.
   b) **Application (Client) ID**: The unique identifier of your application used by Microsoft Entra (formerly known as Microsoft Azure) to validate security tokens received from the Microsoft identity platform. Find the **Application**

(Client) ID in the Overview page of your registered app in the Microsoft Entra admin center. For more information, see Register an application in Microsoft Entra ID.

c) **Client Secret**: The application password used by the registered app to identify itself. For more information, see Add and manage application credentials in Microsoft Entra ID.

d) **Token Endpoint URL**

3. Click **Save**.
4. Click the **ellipse menu** to view or modify integration details.

After creating an MDM integration, it can take up to 24 hours before the integration will take effect in a posture profile used in an access rule. During that time, devices will not be granted access to private or internet resources that are protected by the access rule.

What to do next

Define a client-based Zero Trust Connection endpoint posture profile for Microsoft Intune. For more information, see Add a Client-Based Zero Trust Access Posture Profile.

Jamf Pro Third-Party Integration

Integrate Jamf Pro with Secure Access to streamline device management and for better security enforcement in endpoint posture.

Cisco Secure Access integrates with Jamf Pro to streamline device management and enhance security, deployment, and compliance across platforms. Jamf Pro is a leader for management of Apple macOS, iOS, and tvOS devices. When you integrate Jamf Pro with Secure Access, data about your devices will be available to Secure Access. This information is used for better security enforcement in endpoint posture.

Configure the Jamf Pro Third-Party Integration

Provides instructions for configuring the Jamf Pro Third-Party Integration in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Full Admin user role. For more information, see Manage Accounts
- Administrator privileges in Jamf Pro. For more information, see Jamf Pro User Accounts and Groups.

Procedure

1. Navigate to **Admin** > **Third-party Integrations** > **Jamf Pro** and click **Integrate**.
2. Enter integration details.
   a) **Integration name**: Enter a descriptive name that will help you identify the purpose of the integration in Secure Access.
   b) **Client ID**: The unique identifier of the application.
   c) **Client Secret**: The application password used by the registered app to identify itself.
   d) **Base URL**
3. Click **Save**.
4. Click the **ellipse menu** to view or modify integration details.

After creating an MDM integration, it can take up to 24 hours before the integration will take effect in a posture profile used in an access rule. During that time, devices will not be granted access to private or internet resources that are protected by the access rule.

What to do next

Define a client-based Zero Trust Connection endpoint posture profile for Microsoft Intune. For more information, see Add a Client-Based Zero Trust Access Posture Profile.

Push Security Events Third-Party Integration

Add a third-party integration, such as ServiceNow or Splunk, for Secure Access push security events.

You can add a Third-party Integration in Secure Access to enable Push Security Events for a third-party product or service.

Push Security Events are logged by Secure Access when end users request destinations that are associated with Security categories or other security criteria. Security categories that trigger security events are **Command and Control**, **Malware**, and **Phishing**.

A Secure Access Third-party Integration for Push Security Events requires a Secure Access Webhook configured with the URL of the third-party HTTP listener and authentication credentials.

To get started, set up your Third-party Integration for Push Security Events with a Secure Access Webhook. Configure the Secure Access Webhook to send the security events to a destination URL for an HTTP target service. Select the type of security events that the Webhook will send to the HTTP listener.

Administrators of the third-party product or service are responsible for deploying the HTTP listener in the organization's on-premises or cloud environment.

Push Security Events are available for various types of network and security activities:

- DNS activity
- HTTP activity
- Other types of activity:
  - Firewall
  - Intrusion Prevention System (IPS)
  - Data Loss Prevention (DLP)
  - Zero Trust Network Access (ZTNA) with a blocked reason
  - Remote Access Virtual Private Network (RAVPN) with a failed reason

Benefits of Integrating Secure Access Push Security Events with Third-Party Security and Information Systems

- Administrators can configure Secure Access to send Push Security Events to an XDR or Security Information and Event Management (SIEM) system.
- Third-party integrations enable an organization's Security Operations Centers (SOCs) to have visibility into risky activity.
- Third-party integrations provide administrators with the capability to trigger automation and incident response and correlation workflows.
- Assist organizations to identify potential security threats.

Guidelines and Limitations

- Secure Access supports three (3) third-party integrations of Push Security Events in an organization.
- Secure Access sends all Push Security Events in batches formatted with the Cloud events schema or Splunk schema.
- Secure Access sends up to ten security events in each Webhook message.
- Secure Access does not convert numeric or UUID values in the events into names or labels. You can use the Secure Access API to resolve these identifiers.

How to Set Up a Third-Party Integration for Push Security Events

1. Deploy an HTTP listener in your on-premises or cloud environment. Ensure that the target system can receive HTTP POST messages from Secure Access. The target system must support Basic authentication with a username and password.
2. Add a Webhook in Secure Access as a Third-party integration. Configure the Webhook with the URL and Basic authentication credentials of the HTTP listener.
3. Add a Third-party integration for Push Security Events in Secure Access.
4. Validate that your target system receives Secure Access Push Security Events.

Add Third-Party Integrations for Push Security Events

Provides instructions for completing the Add Third-Party Integrations for Push Security Events workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Organizations can add a Third-party Integration for Push Security Events in Secure Access. To integrate the Secure Access Push Security Events with a third-party product or service, deploy an HTTP listener in the organization's on-premises or cloud environment.

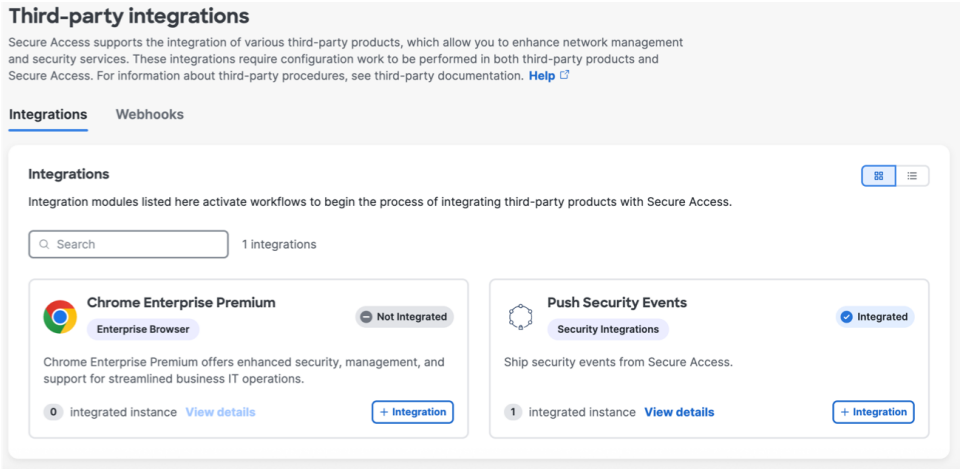
> **Note**
>
> Secure Access supports three Third-party Integrations for Push Security Events.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- Configure a Secure Access Webhook for the Third-party Integration of Push Security Events.

Procedure

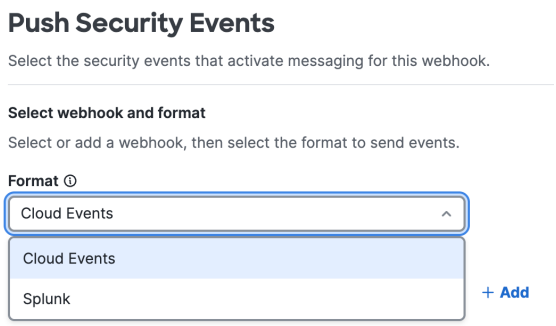
1. Navigate to **Admin** > **Third-party Integrations**.



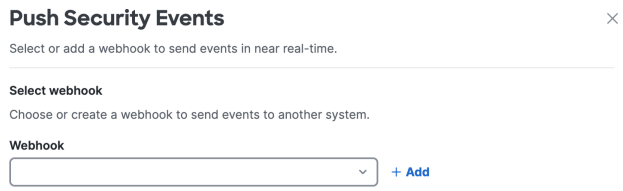
2. Navigate to **Push Security Events**, and then click **+ Integrate** to enter the details for the Third-party Integration.
3. Navigate to **Select webhook and format**.
4. For **Format**, choose the format of the Push Security Events that Secure Access will publish to the Webhook.

   The formats that are available to select for Push Security Events are:

   - **Cloud Events**-The Push Security Events formatted in the Cloud Events schema.
   - **Splunk**-The Push Security Events formatted in the Splunk events schema.



5. For **Webhook** choose a Webhook from the list of configured Webhooks, or navigate to **Webhook**, click **+ Add** and then configure a new Webhook.



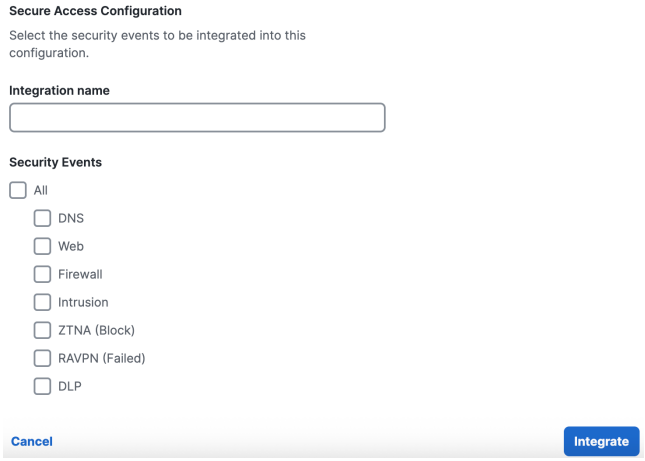
   a) For **Webhook name**, enter 2-250 alphanumeric, underscore, or hyphen characters. Choose a meaningful name for the Webhook that is unique for all Webhooks in the organization.
   b) For **Address/Destination URL**, enter the URL for the HTTP listener that you deployed in your environment.
   c) For **Authentication method**, Secure Access supports **Basic** authentication.
   d) For **Username**, enter the name for the user account that Secure Access will use to authenticate the API request to the target service.
   e) For **Password**, enter the password for the user account that Secure Access will use to authenticate the API request to the target service.
   f) Click **Save**.

6. Navigate to **Secure Access Configuration**.

a) For **Integration name**, enter 2-250 alphanumeric, underscore, or hyphen characters.

Choose a meaningful name for the integration that is unique for all Third-party Integrations in the organization.

b) For **Security Events**, click **All** to select all types of security events, or click the individual types of security events that Secure Access will push to the third-party service.



7. Click **Integrate**.

View Third-Party Integrations for Push Security Events

View the Third-party Integrations for Push Security Events in Secure Access.

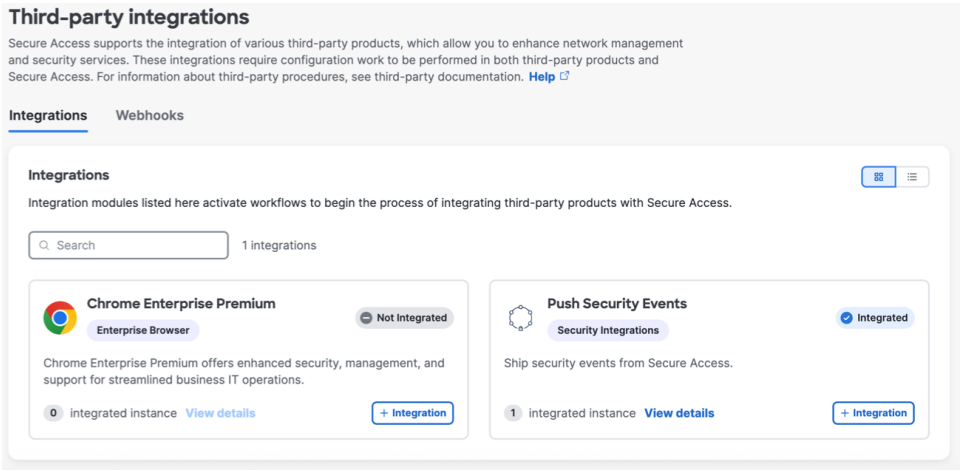
In your Secure Access organization, view the Third-party Integrations configured for Push Security Events.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

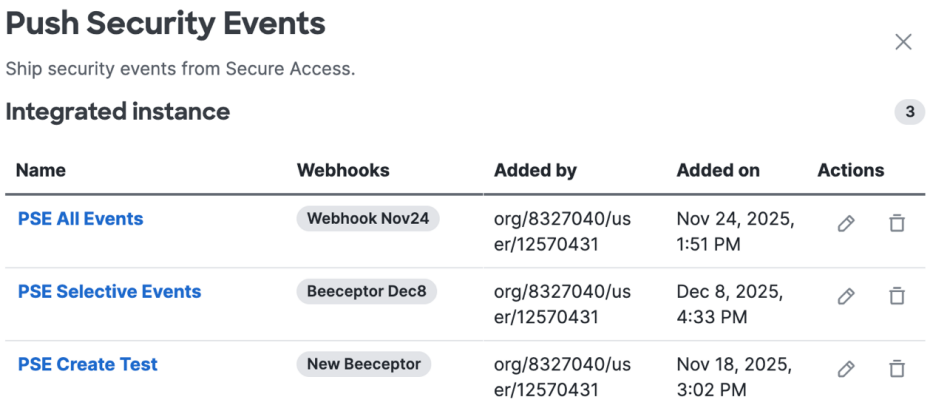
1. Navigate to **Admin** > **Third-party Integrations**.



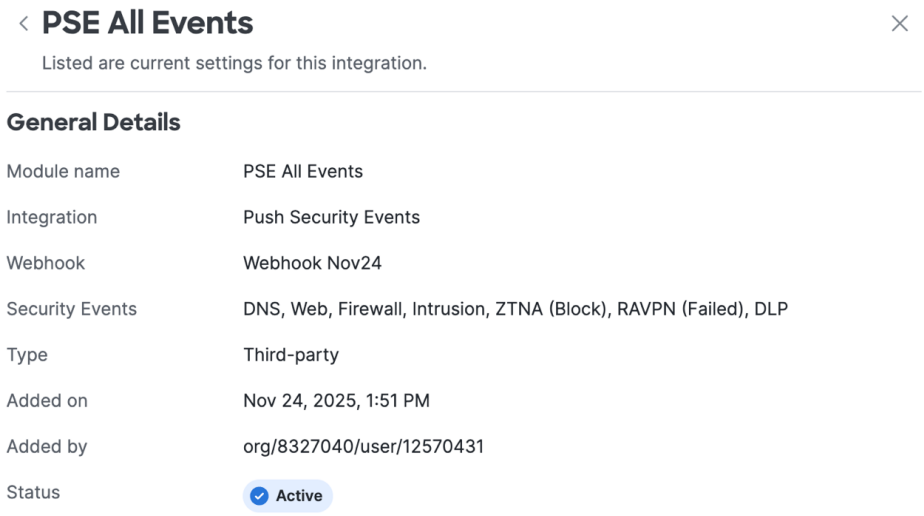
2. On the **Integrations** tab, navigate to **Push Security Events**.
3. Click **View details**.

Secure Access displays the list of Third-party Integrations that are set up to receive push notifications.

- **Name**–The name of the Third-party Integration for Push Security Events.
- **Webhooks**–The name of the Webhooks associated with the integration.
- **Added by**–The organization ID and user account that added the Third-party Integratio.
- **Added on**–The date and time when the organization added the Third-party Integration.



4. Navigate to the Push Security Events table and click on the name of a Third-party Integration to view the details about the integration.
   - **Module name**–The name of the Third-party Integration for Push Security Events.
   - **Integration**–The type of the Third-party Integration.
   - **Webhook**–The name of the Webhook associated with the Third-party Integration.
   - **Security Events**–The list of security events selected for the Third-party Integration.
   - **Type**–The type of the Secure Access integration.
   - **Added on**–The date and time when the organization added the Third-party Integration.
   - **Added by**–The organization ID and user account that added the Third-party Integration.
   - **Status**–The status of the Third-party Integration, either **Active** or **Inactive**.



5. Click **Close**.

Edit a Third-Party Integration for Push Security Events

Provides instructions for completing the Edit a Third-Party Integration for Push Security Events workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Organizations can edit a Third-party Integration for Push Security Events in Secure Access. To integrate the Secure Access Push Security Events with a third-party product or service, deploy an HTTP listener in the organization's on-premises or cloud environment.

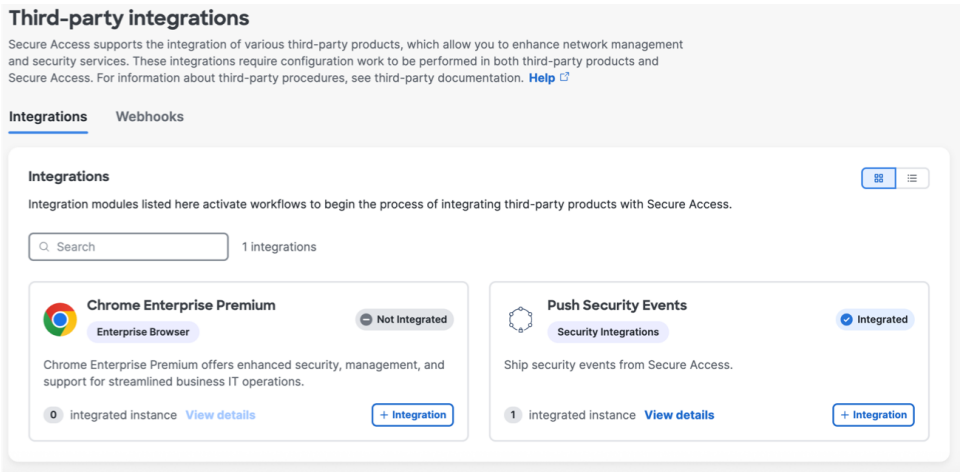
> **Note**
>
> Secure Access supports three Third-party Integrations for Push Security Events.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

Procedure

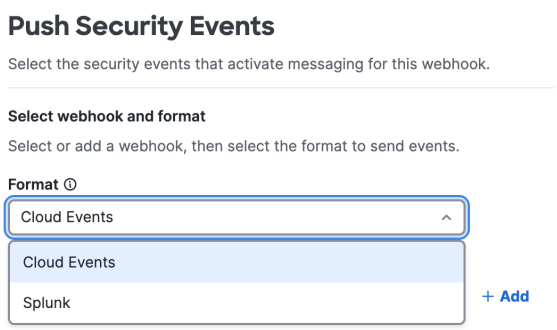
1. Navigate to **Admin** > **Third-party Integrations**.



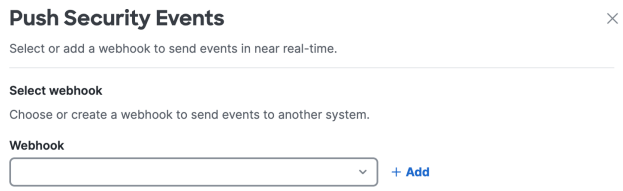
2. Navigate to **Push Security Events**, and then click **View details**.
   a) Navigate to a row in the Third-party Integrations table.
   b) Click on the pencil icon for an entry in the table or click the name of a Third-party Integration and then click **Edit**.
3. Navigate to **Select webhook and format**.
4. For **Format**, choose the format of the Push Security Events that Secure Access will publish to the Webhook.

   The formats that are available to select for Push Security Events are:

   - **Cloud Events**-The Push Security Events formatted in the Cloud Events schema.
   - **Splunk**-The Push Security Events formatted in the Splunk events schema.



5. For **Webhook** choose a Webhook from the list of configured Webhooks, or navigate to **Webhook**, click **+ Add** and then configure a new Webhook.

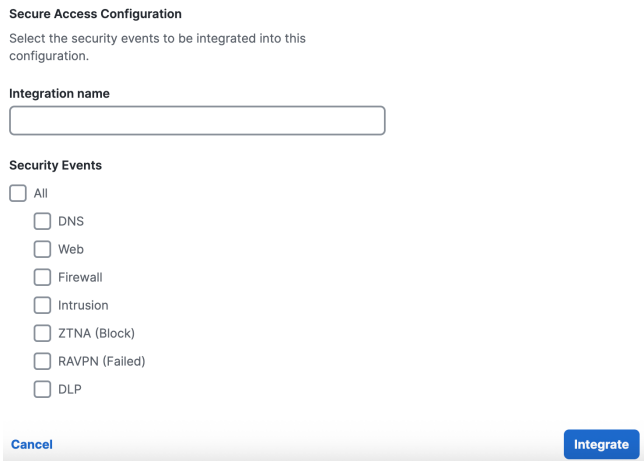


   a) For **Webhook name**, enter 2-250 alphanumeric, underscore, or hyphen characters. Choose a meaningful name for the Webhook that is unique for all Webhooks in the organization.
   b) For **Address/Destination URL**, enter the URL for the HTTP listener that you deployed in your environment.
   c) For **Authentication method**, Secure Access supports **Basic** authentication.
   d) For **Username**, enter the name for the user account that Secure Access will use to authenticate the API request to the target service.
   e) For **Password**, enter the password for the user account that Secure Access will use to authenticate the API request to the target service.
   f) Click **Save**.

6. Navigate to **Secure Access Configuration**.
   a) For **Integration name**, enter 2-250 alphanumeric, underscore, or hyphen characters.

      Choose a meaningful name for the integration that is unique for all Third-party Integrations in the organization.

   b) For **Security Events**, click **All** to select all types of security events, or click the individual types of security events that Secure Access will push to the third-party service.



7. Click **Integrate**.

Delete a Third-Party Integration for Push Security Events

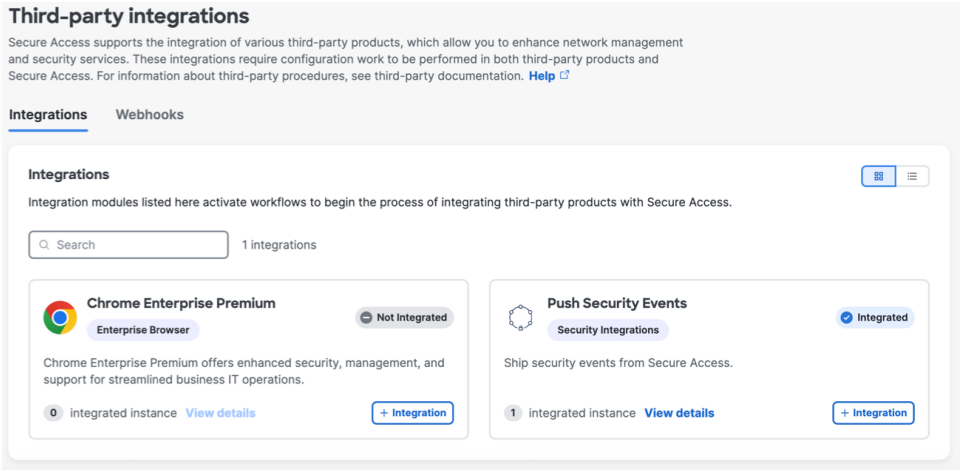
Provides instructions for completing the Delete a Third-Party Integration for Push Security Events workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

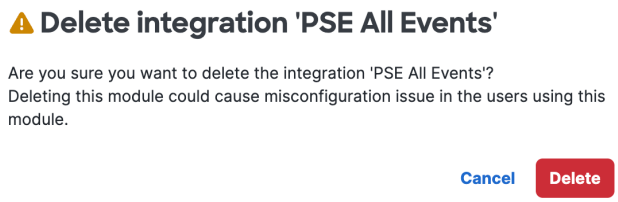
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.



2. Navigate to **Push Security Events**, and then click **View details**.
   a) Navigate to a row in the Third-party Integrations table for Push Security Events.
   b) Click on the trash can icon for an entry in the table or click the name of a Third-party Integration and then click **Delete**.
3. In the dialog window, click **Delete** to confirm the removal of the Third-party Integration.



Splunk Integration: Configure Push Security Events

Describes how to configure Push Security Events for Splunk in Cisco Secure Access.

To receive Push Security Events in Splunk, set up a Webhook for Splunk in Secure Access. Then, configure a Third-party Integration and add the Webhook for Splunk to the Third-party Integration.

Secure Access logs security events when end users send requests to destinations associated with Security categories. The Security categories are **Command and Control**, **Malware**, **Phishing** or other security criteria. Secure Access publishes the Push Security Events for Splunk in JSON using the Splunk events schema. For more information, see Push Security Events Third-Party Integration.

Set Up Push Security Events in Secure Access for Splunk

Configure a Secure Access Webhook for Splunk and then set up the Secure Access Third-party Integration for Push Security Events.

1. Add a Webhook in Secure Access. Configure the Webhook with the URL for the Splunk HTTP listener and the Basic authentication credentials for your Splunk account. For more information, see Manage Webhooks for Third-Party Integrations.
2. Add a Secure Access Third-party Integration for Splunk. For the Third-party Integration, select the Push Security Events. For more information, see Add Third-Party Integrations for Push Security Events.
3. Validate that your instance of Splunk receives the Secure Access Push Security Events.

ServiceNow Integration: Configure Push Security Events

Describes how to configure Push Security Events for ServiceNow.

Configure the integration of a Third-party Integration with ServiceNow to publish Data Loss Prevention (DLP) Push Security Events. Secure Access publishes the DLP Push Security Events for ServiceNow formatted in the cloud events schema.

ServiceNow creates incidents when the ServiceNow HTTP listener receives the DLP push security events from Secure Access and identifies that certain security conditions are present in the events.

Set up a Webhook for ServiceNow in Secure Access and add the Webhook to the Third-party Integration for ServiceNow. For more information, see Push Security Events Third-Party Integration.

Step1: Set Up ServiceNow to Receive Secure Access Push Security Events

Before you begin, obtain a ServiceNow account with administrative privileges.

1. In the ServiceNow app, create a Group for your Cisco Secure Access organization.
2. Set up filters in ServiceNow. The filters enable ServiceNow to read specific fields in the Secure Access DLP push security events. Optionally add boolean logic with the ServiceNow filters.
   - **cisco_origin**: The name of the Cisco Secure Access origin.
   - **metadata.correlation_id**: The correlation IDs for the Secure Access services.
   - **policy.name**: The name of the DLP policy that triggered the DLP security event.
   - **cisco_dlp_metadata.severity**: The severity of the security event.
   - **cisco_dlp_metadata.event_type**: Type of the security event.
   - **cisco_organization_id**: The ID of the Secure Access organization.
3. Configure authentication for the ServiceNow HTTP listener. Allow end users to manage Basic authentication for the Cisco Secure Access Group.
4. Submit the configuration of the Group for Cisco Secure Access.
5. ServiceNow exposes a single Scripted REST API endpoint URL for all groups.

Step 2: Set Up Push Security Events in Secure Access for ServiceNow

1. Add a Webhook in Secure Access. Configure the Webhook with the URL for the ServiceNow HTTP listener and the Basic authentication credentials for your ServiceNow account. For more information, see Manage Webhooks for Third-Party Integrations.
2. Add a Secure Access Third-party Integration for ServiceNow. For more information, see Push Security Events Third-Party Integration.

For the Third-party Integration, select the DLP Push Security Events only.

For the format of the Push Security Events, select **Cloud Events**.

3. Validate that your target system receives the Secure Access DLP Push Security Events.

Microsoft Edge for Business Third-Party Integration

Integrate Microsoft Edge for Business with Cisco Secure Access to enable secure access to private applications, enhance security and compliance for unmanaged devices, and provide advanced management and monitoring features for enterprise environments.

This integration allows Cisco Secure Access security policies, and posture checking to be applied within the Microsoft Edge for Business browser, focusing on scenarios involving unmanaged devices.

What is Microsoft's Edge for Business?

Microsoft Edge for Business is a secure enterprise browser built into Windows. It separates work and personal browsing into dedicated windows, helping users maintain focus and security.

By integrating Microsoft's Edge for Business with Cisco Secure Access, you can:

- Increase adoption of Cisco Secure Access for third-party and bring your own device (BYOD) environment.
- Ensure secure access to unmanaged devices.
- Enhance data protection through browser-based controls.
- Simplify deployment and management for contractor access.
- Support Zero Trust Network Access (ZTNA) requirements through Microsoft integration.

When Microsoft's Edge for Business is configured, Cisco Secure Access receives device posture information from Edge. This data enables Cisco Secure Access to:

- Securely manage access to private applications for third-party contractors and users on unmanaged devices.
- Configure clientless posture profiles specific to Microsoft Edge for Business.
- Display an "access denied" page and block access to the private resource when a trusted browser attempts to access a private resource.
- Define a trusted browser as Microsoft Edge for Business operated by a user authenticated with an Entra ID account.
- Monitor and audit all private application access through Microsoft Edge for Business.

Add Third-Party Integration for Microsoft Edge for Business

Learn how to configure Microsoft Edge for Business integration with Cisco Secure Access, enabling secure access management for third-party applications and unmanaged devices. Follow these steps to enter integration details, define a Zero Trust Connection endpoint posture profile, and manage credentials in Microsoft Entra ID.

Organizations can integrate Microsoft Edge for Business with third-party products or services in Cisco Secure Access by deploying an HTTP listener within their on-premises or cloud environment.

Important

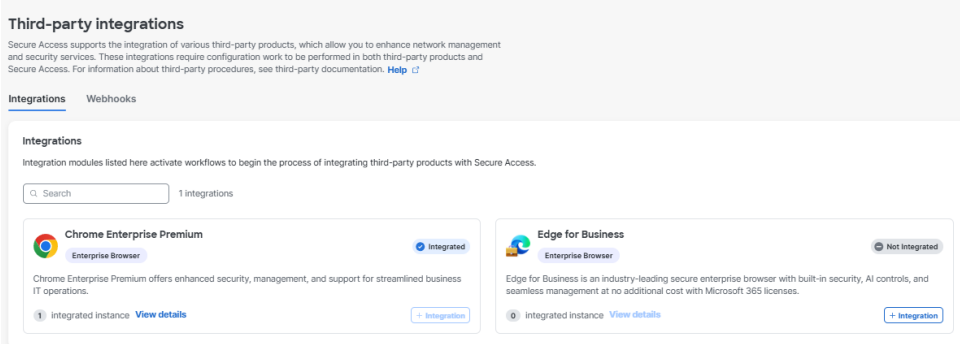
You can add upto three third-party Integrations for Microsoft Edge for Business.

Before you begin

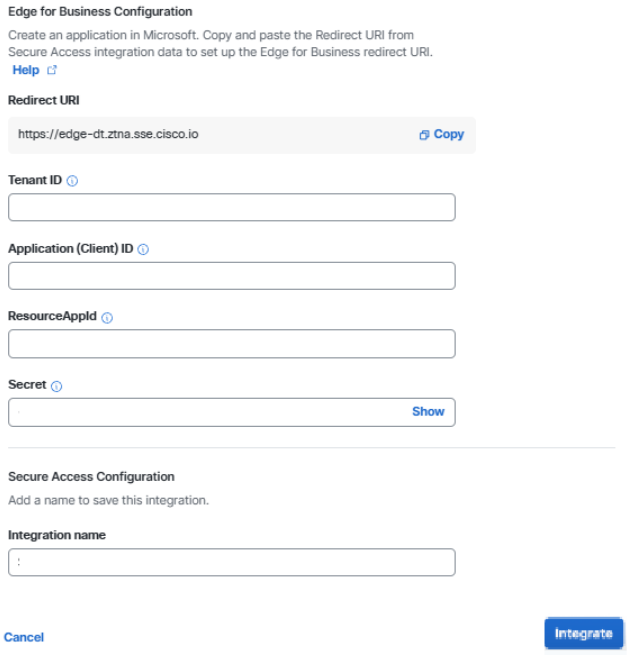
- Full Admin user role. For more information, see Manage Accounts
- Administrator access to the Microsoft Edge for Business admin center. For more information, see Tutorial: Walkthrough Microsoft Edge for Business admin center.

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to **Edge for Business**, then click **+ Integrate**.



3. For **Edge for Business**, enter the details for third-party integration:
   a) Navigate to **Edge for Business Configuration**.
   b) **Tenant ID**: It is the Microsoft Entra ID. Find the **Tenant ID** on the Properties page of your registered app in the Microsoft Entra admin center. For more information, see Find tenant ID through the Microsoft Entra admin center or Set up a new Microsoft Entra tenant.
   c) **Application (Client) ID**: The unique identifier of your application used by Microsoft Edge for Business to validate security tokens received from the Microsoft identity platform. Find the **Application (Client) ID** in the **Overview** page of your registered app in the Microsoft Entra admin center. For more information, see Register an application in Microsoft Entra ID.
   d) **ResourceApp ID**: This ID is from the Microsoft Entra ID portal. This identifier associates with the resource application registered in the Microsoft Entra ID portal.
   e) **Secret**: The application password used by the registered app to identify itself. For more information, see Add and manage application credentials in Microsoft Entra ID.
   f) **Integration name**: Enter a descriptive name to help you identify the purpose of the integration in Secure Access.



4. Click **Integrate**.

After creating an MDM integration, it may take up to 24 hours for the integration to take effect in a posture profile used in an access rule. During this time, devices will not be granted access to private or internet resources protected by the access rule.

What to do next

Define a client-based Zero Trust Connection endpoint posture profile for Microsoft Edge for Business. For more information, see Add a Browser-Based Zero Trust Access Posture Profile.

View Third-Party Integration for Microsoft Edge for Business

View the Third-party Integrations for Microsoft Edge for Business in Secure Access.

In your Secure Access organization, view the third-party integrations configured for Microsoft Edge for Business.

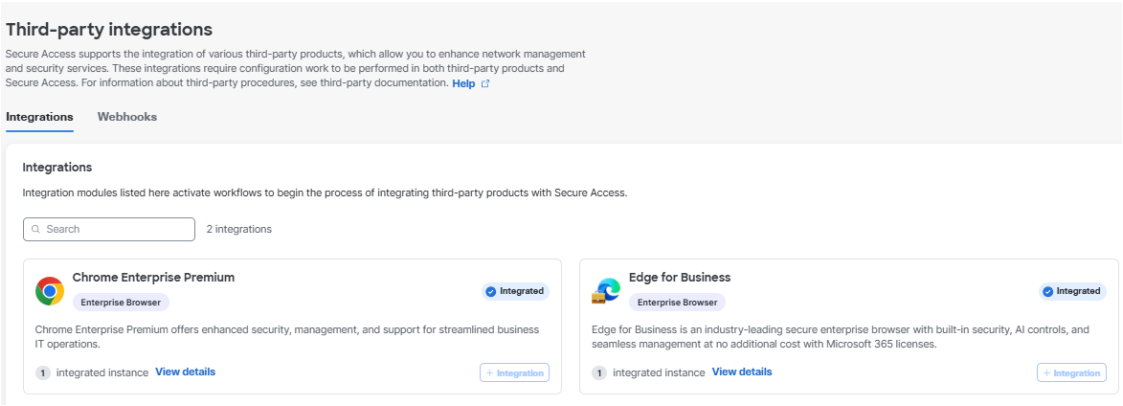
Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

---

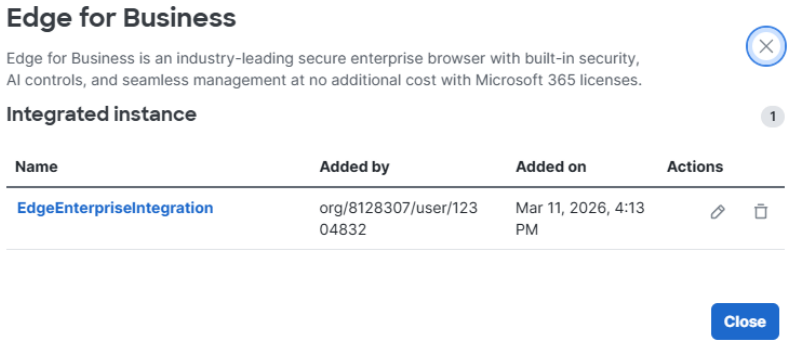
1. Navigate to **Admin** > **Third-party Integrations**.
2. On the **Integrations** tab, navigate to **Edge for Business**.



3. Click **View details**.

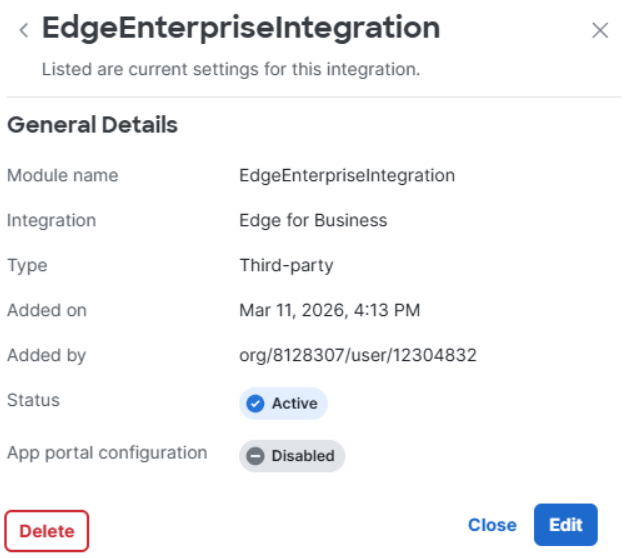
   Secure Access displays the list of Third-party Integrations that are set up to receive push notifications.

   - **Name**–The name of the Third-party Integration for Microsoft Edge for Business.
   - **Added by**–The organization ID and user account that added the Third-party Integration.
   - **Added on**–The date and time when the organization added the Third-party Integration.



4. Navigate to the Microsoft Edge for Business table and click on the name of a **Third-party Integration** to view the details about the integration.

   - **Module name**–The name of the **Third-party Integration** for Microsoft Edge for Business.
   - **Integration**–The type of the **Third-party Integration**.
   - **Type**–The type of the Secure Access integration.
   - **Added on**–The date and time when the organization added the **Third-party Integration**.
   - **Added by**–The organization ID and user account that added the **Third-party Integration**.
   - **Status**–The status of the **Third-party Integration**, either **Active** or **Inactive**.
   - **App portal configuration**–The status of the App portal configuration, either **Enabled** or **Disabled**.



5. Click **Close**.

Edit a Third-Party Integration for Microsoft Edge for Business

Learn how to edit the Third-party Integrations for Microsoft Edge for Business in Secure Access.

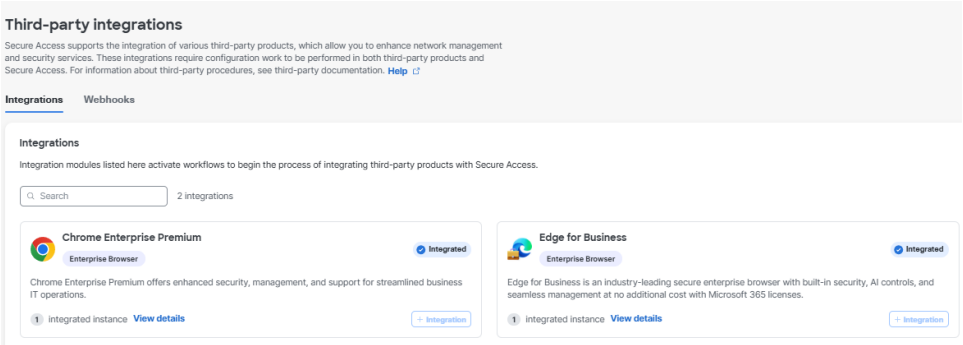
Organizations can edit a Third-party Integration for Microsoft Edge for Business in Secure Access. The integration requires the deployment of an HTTP target service in the organization's on-premises or cloud environment.

Before you begin

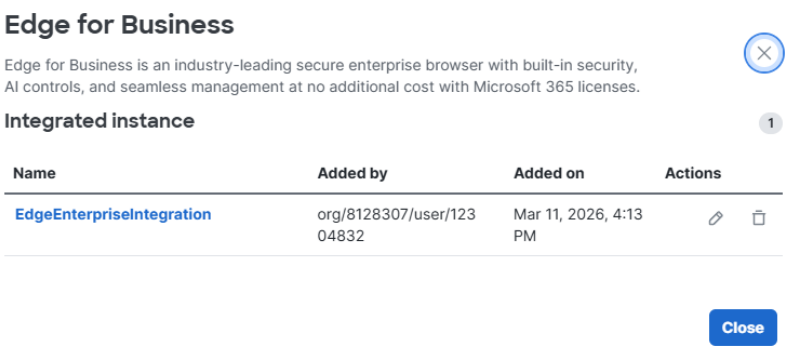
- Full Admin user role. For more information, see Manage Accounts

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to **Edge for Business**, and then click **View details**.

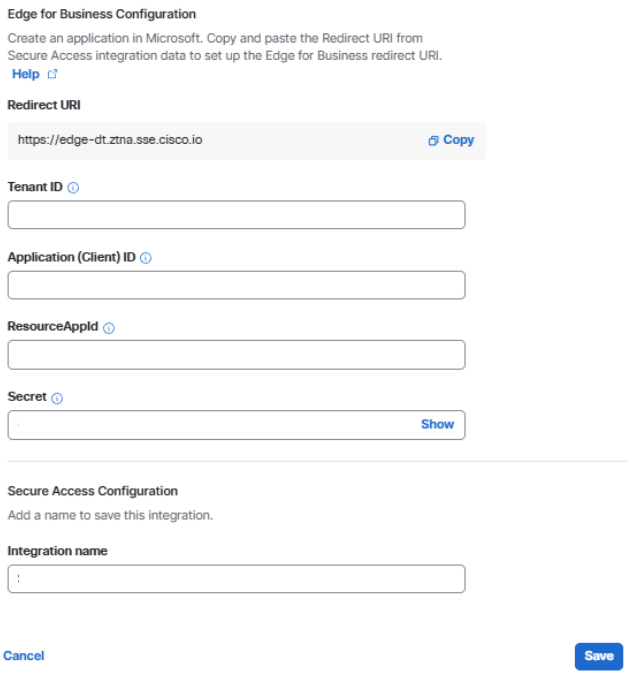


a) To edit the integration settings, in the Integrated instance table, click the **Edit** (pencil) icon next to the respective instance name.



3. Navigate to **Edge for Business Configuration**.
   a) **Tenant ID**: It is the Microsoft Entra ID. Find the **Tenant ID** on the **Properties** page of your registered app in the Microsoft Entra admin center. For more information, see Find tenant ID through the Microsoft Entra admin center or Set up a new Microsoft Entra tenant.
   b) **Application (Client) ID**: This ID is from the Microsoft Entra ID portal. This unique identifier refers to the application registered in the Microsoft Entra ID portal. For more information, see Register an application in Microsoft Entra ID.
   c) **ResourceApp ID**: This ID is from the Microsoft Entra ID portal. This identifier associates with the resource application registered in the Microsoft Entra ID portal.
   d) **Secret**: This ID is from the Microsoft Entra ID portal. This value associates with the application registered in the Microsoft Entra ID portal. For more information, see Add and manage application credentials in Microsoft Entra ID.
   e) **Integration name**: The name must be alphanumeric with characters length between 2 and 250. Choose a meaningful name that begins with an alphabetic character.

      The name of the integration must be unique for all Third-party Integrations in the organization.



4. Click **Save**.

Island Enterprise Browser Third Party Integration

Integrate an island enterprise browser with Secure Access to provide secure and managed access to corporate resources without requiring full device management.

The integration allows Cisco Secure Access security policies, and posture checking to be applied within the Island Enterprise Browser.

What is an Island Enterprise Browser?

An Island Enterprise Browser is designed for secure and managed access to corporate resources and offer support for managed and unmanaged devices, enabling secure access for contractors, partners, and bring-your-own-device users without requiring full device management with the intention of extending zero trust controls to the browser level, providing a comprehensive security posture from the network to the endpoint.

Add a Third-Party Integration for Island Enterprise Browser

Provides instructions for completing the Add a Third-Party Integration for Island Enterprise Browser workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the following procedure to add a new, validated third party integration for your Island Enterprise Browser. Note that you can only have one Island Enterprise Browser configured at a time.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.
- You must have an API key generated from your enterprise browser.

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to **Island Enterprise Browser**, then click **+ Integrate**.
3. Enter the **API Key** from your Island Enterprise browser.
4. Enter a unique **Integration name**. This title is displayed in the Island Enterprise Browser window.
5. Click **Integrate**.

What to do next

Define a browser-based **Zero Trust Connection** endpoint posture profile for the Island Enterprise browser. For more information, see Manage Zero Trust Access Posture Profiles.

Edit a Third-Party Integration for Island Enterprise Browser

Provides instructions for completing the Edit a Third-Party Integration for Island Enterprise Browser workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the following procedure to change the integration credentials that securely connects your Secure Access organization to the island enterprise browser:

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.

2. Navigate to **Island Enterprise Browser**, then click **View details**.
3. To edit the integration settings, in the Integrated instance table, click the **Edit** (pencil) icon next to the respective instance name.
4. Modify one of the two options:
   - **API Key**
   - **Integration name** - this is the name that appears in the dashboard.
5. Click **Save**. Alternatively, you can cancel out of these changes at any time.

Delete a Third-Party Integration for Island Enterprise Browser

Provides instructions for completing the Delete a Third-Party Integration for Island Enterprise Browser workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Use the following procedure to permanently delete the Island Enterprise Browser configuration from your organization as a third party integration:

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to **Island Enterprise Browser**, then click **View details**.
3. Click the **Delete** icon.
4. Confirm the **Delete** action. Alternatively, click **Cancel** to keep the integration.

Threat Intelligence Feeds

Integrate supported threat intelligence feeds in Secure Access to share collections of information about security threats and indicators of compromise.

Secure Access supports the integration of threat intelligence feeds in a Secure Access organization. Threat intelligence feeds are services that provide collections of information about security threats and indicators of compromise (IOCs).

In Secure Access, you can add a Third-party Integration and configure the integration of a threat intelligence feed.

- The threat intelligence feed must provide the collections of data in the Structured Threat Information eXpression (STIX) JSON schema.
- The threat intelligence feed must deliver the data using the Trusted Automated eXchange of Intelligence Information (TAXII) protocol.
- Integrated threat intelligence feeds must support a collection of IOCs that include: IPv4 or IPv6 addresses, fully-qualified domain names (FQDNs), and URLs.

When you integrate a threat intelligence feed in your organization, Secure Access creates and manages a dedicated destination list in the organization.

After Secure Access begins to collect data from the integrated threat intelligence feed, you can view the destinations in the destination list. The new destination list is available to add on the internet access rules in the organization's Access policy.

Requirements for Integrating a Threat Intelligence Feed

To integrate with Secure Access, a threat intelligence feed must meet the following requirements:

- Support for the STIX 2.0/2.1 JSON schema over the TAXII 2.0/2.1 protocol.
- Support at a minimum for basic authentication with a username and password.
- Have a publicly accessible URL.
- Provide a unique identifier for the STIX collection.
- Provide a collection of IOCs with IPv4 or IPv6 addresses, fully qualifed domain names (FQDNs), and URLs.

How to Integrate a Threat Intelligence Feed in Secure Access

1. Subscribe to a threat intelligence feed.
2. Add a third-party integration in Secure Access with the configuration details for the threat intelligence feed.
3. Add the destination list associated with the threat intelligence feed in the internet access rules in the organization's access policy.
4. View the details about the impacted internet destinations in the Secure Access Activity Search report or with the Cisco Secure Access Reporting API.

Add a Third-Party Integration for a Threat Intelligence Feed

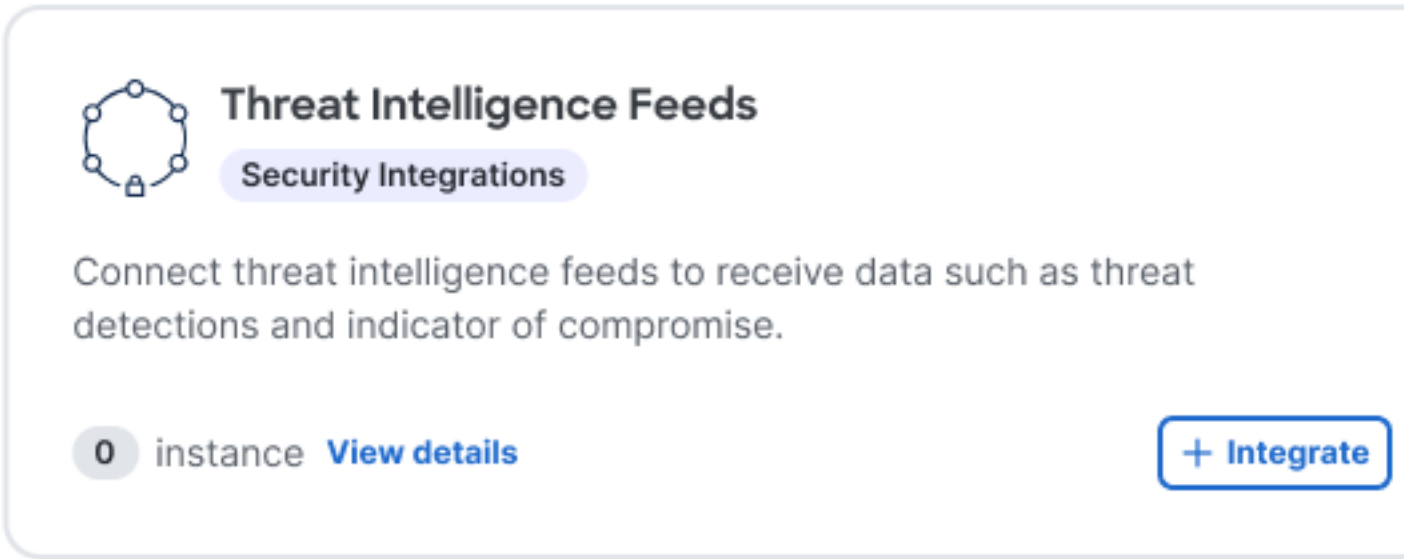
For more information, see Add Third-Party Integrations for Threat Intelligence Feeds.

View Integrated Threat Intelligence Feeds

For more information, see View Integrated Threat Intelligence Feeds.

Manage a Threat Intelligence Feed in Secure Access

For more information, see Edit or Delete a Threat Intelligence Feed.



Add Third-Party Integrations for Threat Intelligence Feeds

Provides instructions for adding Third-Party Integrations for Threat Intelligence Feeds workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Add a Third-party Integration for a threat intelligence feed.

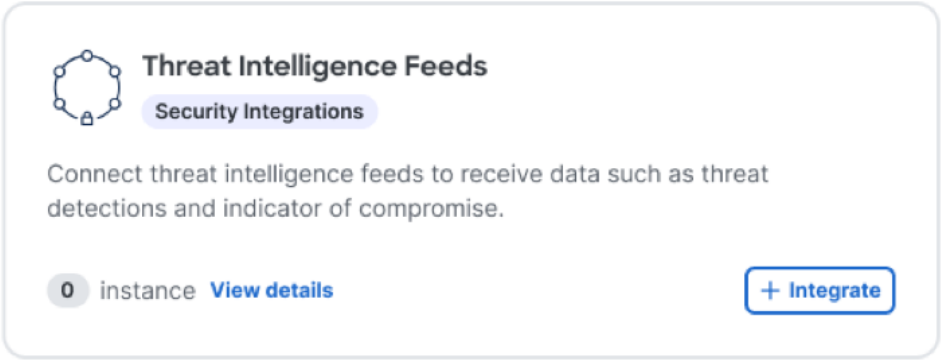
- Configure the settings for the threat intelligence feed in Secure Access and enable the integration. Secure Access supports Basic authentication and a username and password in all communications with the threat intelligence feed service.
- Configure the settings for the collection that Secure Access will ingest from the threat intelligence feed.

Before you begin

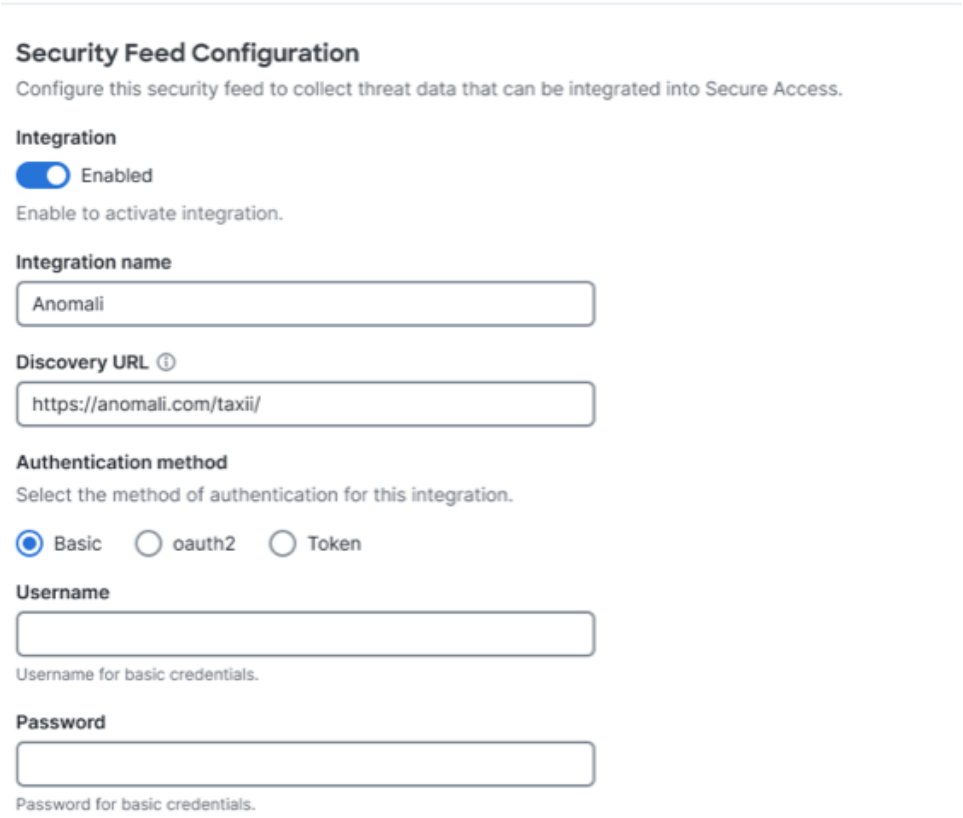
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Click + **Integrate**.



3. Expand **Security Feed Configuration**.
4. Toggle on **Integration** to enable the threat intelligence feed.
5. For **Integration Name**, enter a name that distinguishes the threat intelligence feed in the organization.
6. For **Discovery URL**, enter the URL for the threat intelligence feed.
7. For **Authentication method**, choose Basic.
8. For **Username**, enter the username for the account that Secure Access will use to authenticate with the threat intelligence feed.
9. For **Password**, enter the password for the user account that Secure Access will use to authenticate with the threat intelligence feed.
10. Click **Next**.



11. Expand **Security Feed Collections**.
12. For **Root URL**, enter a root URL for the threat intelligence feed.
13. For **Collections**, enter an identifier for a collection in the threat intelligence feed.
14. Click **Integrate**.



View Integrated Threat Intelligence Feeds

Provides instructions for completing the View Integrated Threat Intelligence Feeds workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

After you add a third-party integration for a threat intelligence feed, you can view the details about the settings configured in Secure Access and the destinations in the destination list for the integration.

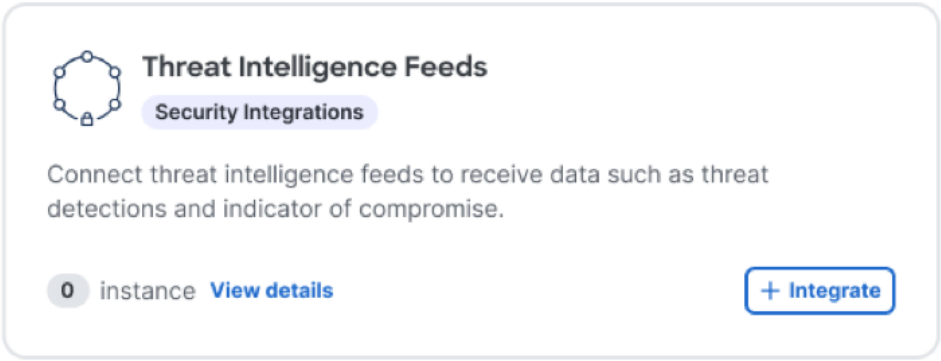
You can view the status and details about the threat intelligence feeds integrated in Secure Access.

Before you begin

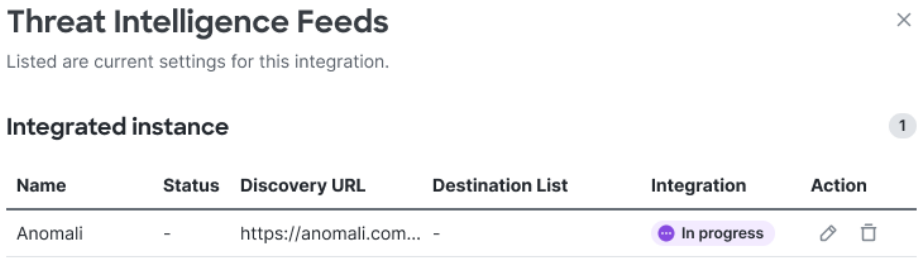
- A user role of Read Only. For more information, see Manage Accounts.

Procedure

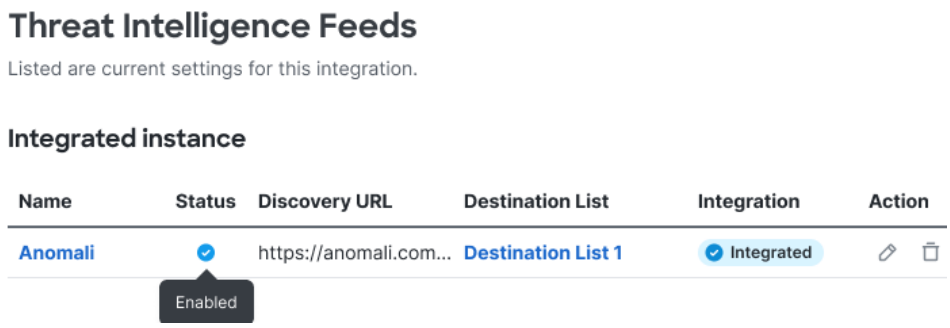
1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to Threat Intelligence Feeds.



3. Click View details.
4. Navigate to Integrated instances.



5. You can view the details about a threat intelligence feed, and edit or remove the integration of the threat intelligence feed.



6. Navigate to a row in the table.
7. Click **Close**.

Edit or Delete a Threat Intelligence Feed

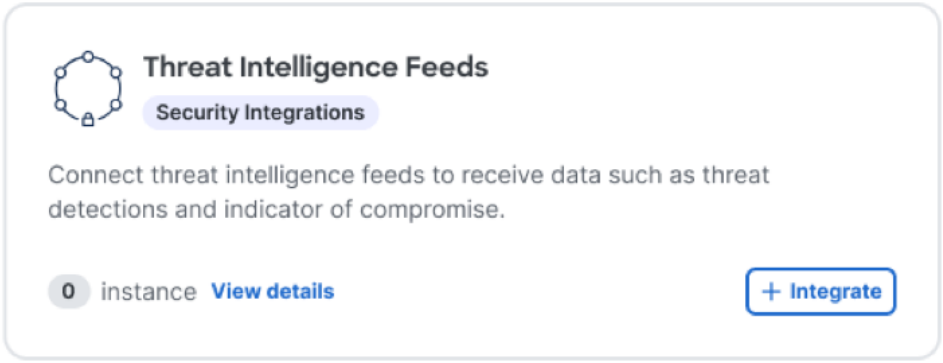
Provides instructions for editing or deleting a Threat Intelligence Feed in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

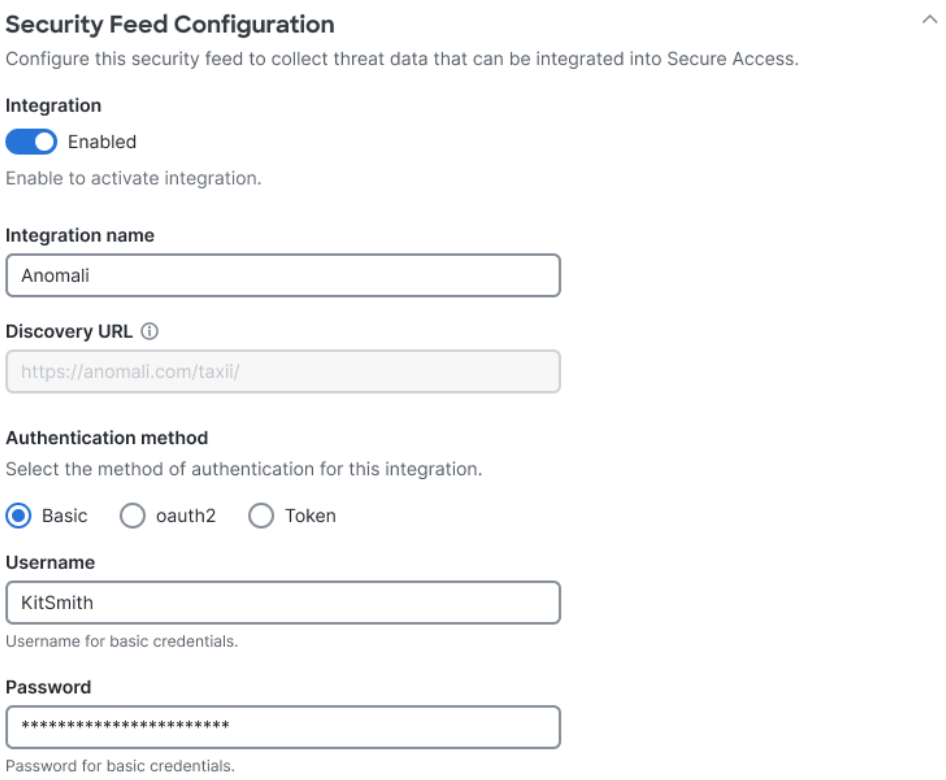
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations**.
2. Navigate to **Threat Intelligence Feeds**.
3. Click **View Details.**



4. Navigate to **Integrated instances**.
5. To edit an integrated threat intelligence feed, navigate to the **Action** column in a row in the table and then click the pencil icon.
   a) Expand **Security Feed Configuration**.



b) Toggle on **Integration** to enable the threat intelligence feed.
c) For **Integration Name**, enter a name that distinguishes the threat intelligence feed in the organization.
d) For **Authentication method**, choose Basic.
e) For **Username**, enter the username for the account that Secure Access will use to authenticate with the threat intelligence feed.
f) For **Password**, enter the password for the user account that Secure Access will use to authenticate with the threat intelligence feed.
g) Click Save.

6. To delete an integrated threat intelligence feed, navigate to the **Action** column in a row in the table and then click the trash can icon.
   a) Click **Delete** and then click **Delete** again to confirm the removal of the threat intelligence feed.

Manage Webhooks for Third-Party Integrations

Manage Webhooks to support notifications for alert rules and third-party integrations in Secure Access.

Organizations can add Webhooks in Secure Access that support notifications for alert rules or third-party integrations. A Secure Access Webhook sends notifications or messages to a configured destination URL for an integrated third-party product or service.

For example, set up a Webhook to send notifications about certain conditions on a specific type of Secure Access resource to a third-party Security Information and Event Management (SIEM) system. The organization is responsible for configuring any third-party products or services to receive the notifications.

> **Note**
>
> You can add a maximum of ten Webhooks in your Secure Access organization.

Guidelines for Configuring an HTTP Listener

- Configure an HTTP listener (target service of the Webhook) in the organization's on-premises or cloud environment.
- Ensure that the target service accepts Basic authentication for HTTP POST API requests. You will set up the Secure Access Webhook with the **username** and **password** for an account on the target service.

Add a Webhook for a Third-Party Integration

Add a Webhook in Secure Access. A Webhook is configured to send notifications to a third-party product or service.

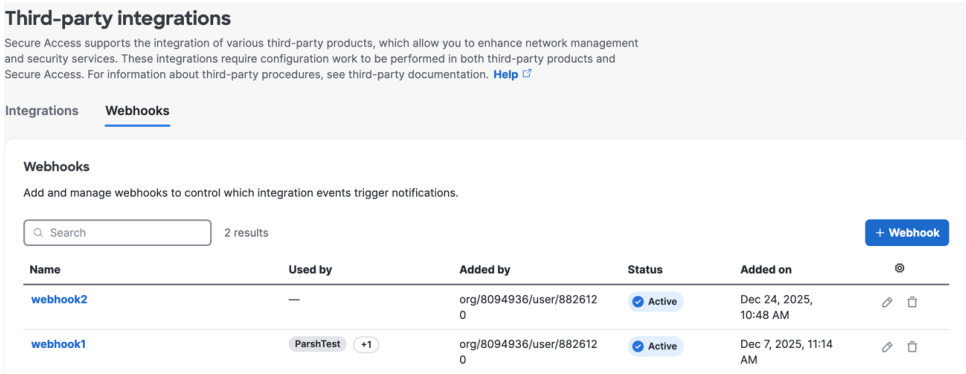
Add a Webhook in Secure Access. A configured Webhook sends notifications to an integrated third-party product or service.

Before you begin

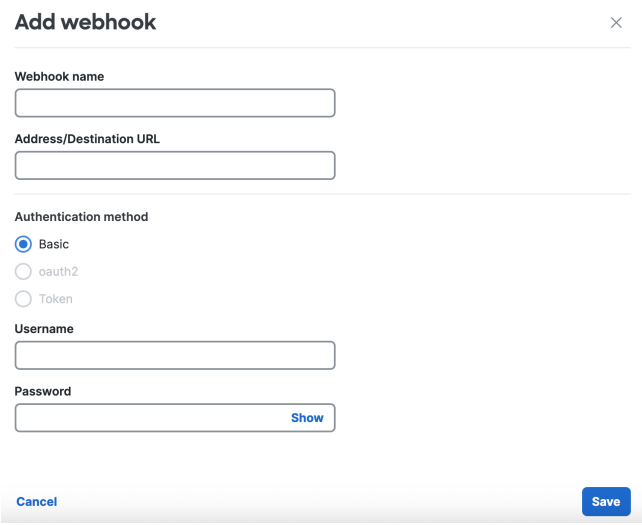
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations** and then click **Webhooks**.



2. Click **+ Webhook**.



a) For **Webhook name**, enter 2-250 alphanumeric, underscore, or hyphen characters. Choose a meaningful name that describes the Webhook.
b) For **Address/Destination URL**, enter the URL for the HTTP listener that you deployed in your environment.
c) For **Authentication method**, Secure Access supports **Basic** authentication.
d) For **Username**, enter the name for the user account that Secure Access will use to authenticate the API request to the target service.
e) For **Password**, enter the password for the user account that Secure Access will use to authenticate the API request to the target service.

3. Click **Save**.

View Details for Webhooks

View the Webhooks in Secure Access and the details for a Webhook.

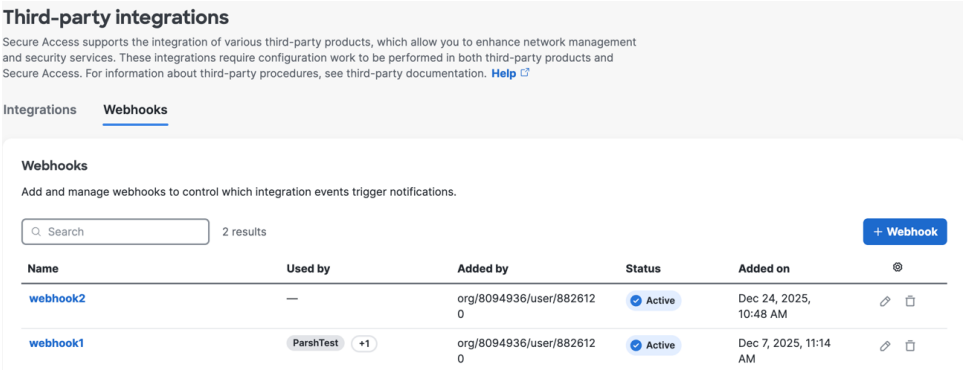
View the Webhooks in Secure Access and the details for each configured Webhook.

Before you begin

- A minimum user role of Read-only. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations** and then click **Webhooks**.

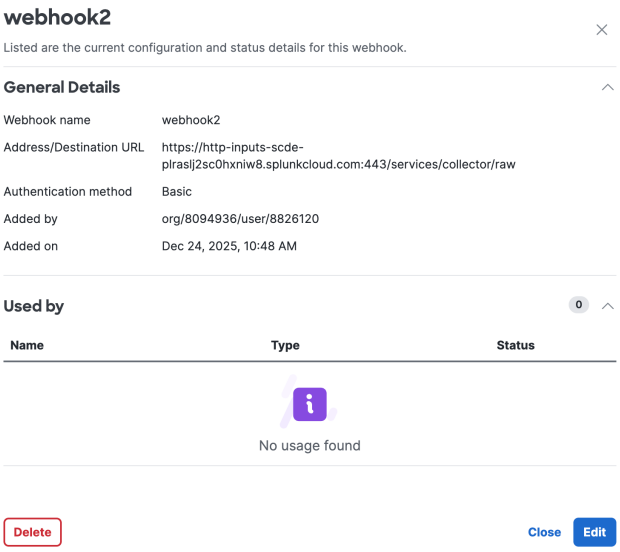


Secure Access displays the list of configured Webhooks and the details for each Webhook added in the organization.

- **Name**–The name of the Webhook.
- **Used by**–The name of the Third-party Integration that is associated with the Webhook.
- **Added by**–The organization ID and user account that added the Webhook.
- **Status**–The state of the Webhook, either active or inactive.
- **Added on**–The date and time when the organization added the Webhook.

2. To view the details for a Webhook, navigate to the Webhooks table, and then click on the name of a Webhook.

   Secure Access displays the details about the Webhook and the Third-party integration associated with the Webhook.



   a) Navigate to **General Details**.
      - **Webhook name**–The name of the Webhook.
      - **Address/Destination URL**–The address of the HTTP listener assigned to the Webhook.
      - **Authentication method**–The method of authentication used in the API request by the Webhook.
      - **Added by**–The organization ID and user account that added the Webhook.
      - **Added on**–The date and time when the organization added the Webhook.

   b) Navigate to **Used by**.
      - **Name**–The name of the Third-party Integration.
      - **Type**–The type of the Third-party Integration.
      - **Status**–The state of the Third-party Integration, either active or inactive.

3. Click **Close**.

Edit a Webhook for a Third-Party Integration

Edit a Webhook in Secure Access. A Webhook is configured to send notifications to a third-party product or service.

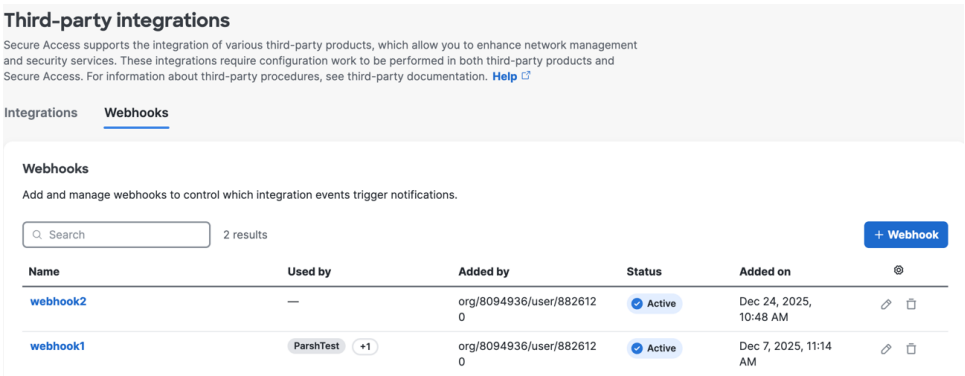
In Secure Access, edit a Webhook that is configured to send notifications to an integrated third-party product or service.

Before you begin

- Full Admin user role. For more information, see Manage Accounts.

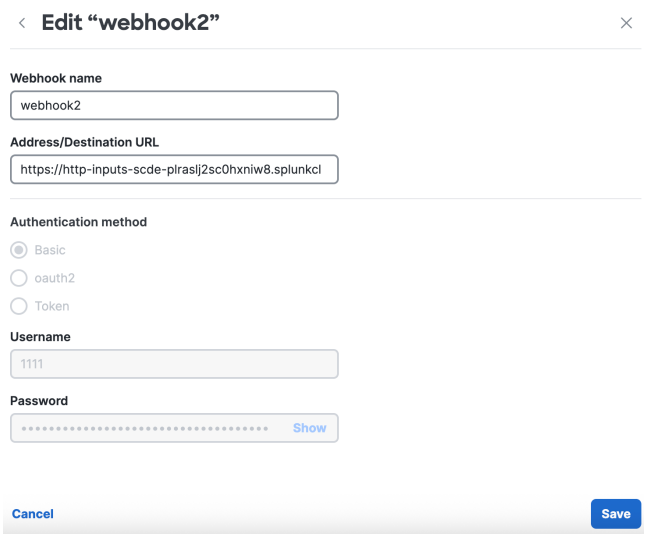
Procedure

1. Navigate to **Admin** > **Third-party Integrations** and then click **Webhooks**.



2. Navigate to the Webhooks table, and then click on the name of a Webhook or the pencil icon at the end of a row.

> **Note**
>
> You can modify the Webhook name and destination URL only.



   a) For **Webhook name**, enter 2-250 alphanumeric, underscore, or hyphen characters. Choose a meaningful name that begins with an alphanumeric character.
   b) For **Address/Destination URL**, enter the URL for the HTTP listener that you deployed in your on-premises or cloud environment.

3. Click **Save**.

Delete a Webhook for a Third-Party Integration

Delete a Webhook in Secure Access. A Webhook is configured to send notifications to a third-party product or service.

In Secure Access, delete a Webhook that is configured to send notifications to an integrated third-party product or service.

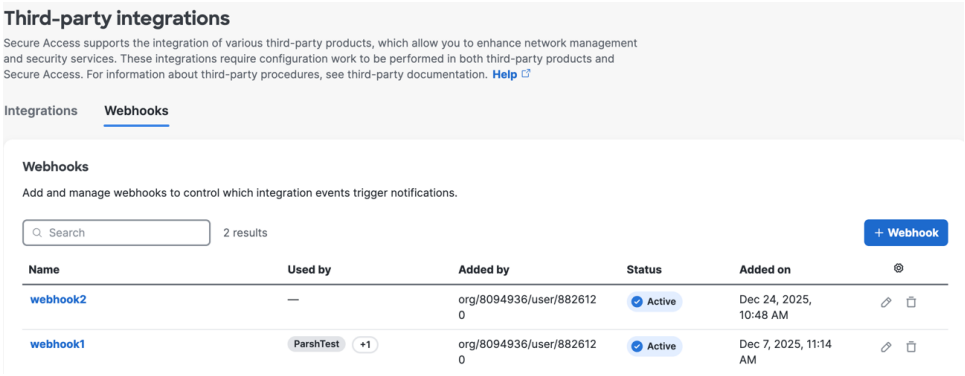
> **Note**
>
> You can delete a Webhook that is associated with an integration.

Before you begin

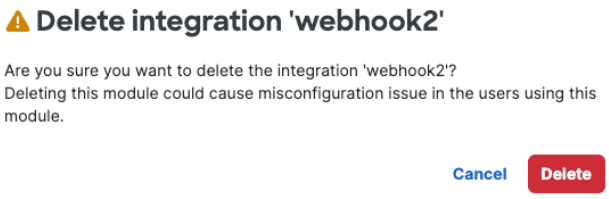
- Full Admin user role. For more information, see Manage Accounts.

Procedure

1. Navigate to **Admin** > **Third-party Integrations** and then click **Webhooks**.



2. Navigate to the Webhooks table, and then click on the name of a Webhook or the trash can icon at the end of a row.
3. In the dialog window, click **Delete** to confirm the removal of the Webhook.



Integrate ISE (Identity Services Engine) with Secure Access

Integration Identity Services Engine with Secure Access to share network context and apply consistent security enforcement for users, devices, and workloads.

Cisco Identity Services Engine (ISE) integrates with Cisco Secure Access to share network context between the platforms for the purpose of applying consistent security enforcement for users, devices and workloads across the enterprise. This integration allows IT teams to:

- Verify user identity: ISE verifies user identity, providing visibility into every device.
- Enforce adaptive policies: ISE enforces adaptive policies to secure access to applications.
- Employ zero-trust security: ISE enables zero-trust security functions for traffic that goes through the SD-WAN fabric.
- Use anti-malware protection: ISE can use an anti-malware protection (AMP) agent to identify malicious files on endpoints.
- Prevent USB device insertion: ISE can prevent the insertion of USB devices into endpoints.

This section describes how to enable context sharing between Cisco ISE and Cisco Secure Access.

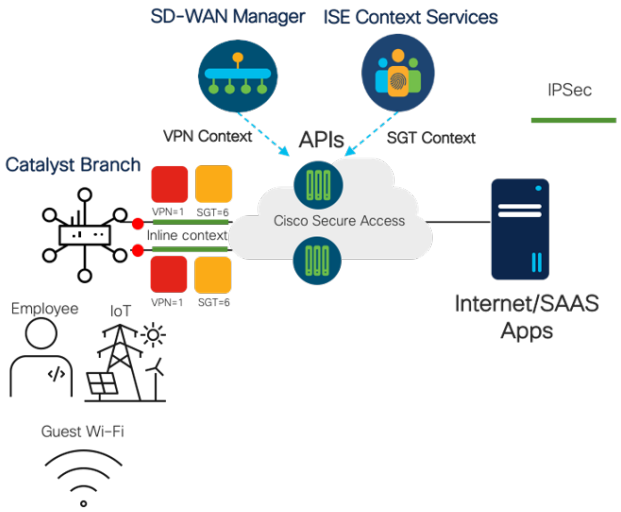
Solution Overview

Describes Solution Overview in Cisco Secure Access. You can use Cisco Identity Services Engine (ISE) to define and use security group tags (SGTs) for classifying traffic in a Cisco TrustSec network.

You can use Cisco Identity Services Engine (ISE) to define and use security group tags (SGTs) for classifying traffic in a Cisco TrustSec network. SGTs specify the privileges of a traffic source within a trusted network. Cisco ISE and Cisco TrustSec use a feature called Security Group Access (SGA) to apply SGT attributes to packets as they enter the network. These SGTs correspond to a user's assigned security group within ISE or TrustSec. If you configure ISE as an identity source, Secure Access can use these SGTs to filter traffic.

With this integration, Cisco Secure Access administrators can use the rich enterprise context shared from Cisco ISE to configure simpler but granular policy control towards internet/SaaS for branch users. Cisco ISE, in conjunction with Catalyst SD-WAN, shares the network context (ISE SGTs and SD-WAN VPN IDs) with Cisco Secure Access.

Use cases for context-aware security enforcement can revolve around employees, guests, or IoT networks behind a Catalyst SD-WAN branch that need to securely access internet/SaaS applications, with Cisco Secure Access providing cloud-based security enforcement.



Note

For information about context sharing with Cisco Catalyst SD-WAN, see Integrate Catalyst SD-WAN with Secure Access.

Security Group Tags

Describes Security Group Tags in Cisco Secure Access. A Securitygroup tag (SGT) is a label used to facilitate classification, propagation and enforcement by associating the SGT with an IP, VLAN, or port-profile as a source or destination.

A Securitygroup tag (SGT) is a label used to facilitate classification, propagation and enforcement by associating the SGT with an IP, VLAN, or port-profile as a source or destination. Matching on SGT tags provides the following benefits:

- The management center can subscribe to Security Group Tag eXchange Protocol (SXP) mappings from ISE.
- ISE uses SXP to propagate the IP-to-SGT mapping database to managed devices. When you configure management center to use an ISE server, you enable the option to listen to the SXP topic from ISE. This causes the management center to learn about the security group tags and mappings directly from ISE. The management center then publishes SGTs and mappings to managed devices.

  For the SGT tag to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
- The SGT assigned to the user session, as downloaded from the ISE session directory. The SGT can be matched to source or destination.
- You can create security group tags in ISE and assign host or network IP addresses to each tag. You can also assign SGTs to user accounts, and the SGT is assigned to the user's traffic. If the switches and routers in the network are configured to do so, these tags then get assigned to packets as they enter the network controlled by ISE, the Cisco TrustSec cloud.
- Supports Cisco TrustSec, which enables you to segment your network to protect critical business assets.

SGT Matching

If you use ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as a source matching criteria. This enables you to block or allow access based on security group membership rather than IP addresses or network objects.

SGT Limitations

Before you start using SGTs in your Access policy, consider the following limitations:

- Security Group Tags can only be used as source and **not** destination matching criteria in access control rules.
- RA-VPNs do not receive SGT mappings directly through RADIUS.

Components and Prerequisites

Describes Components and Prerequisites in Cisco Secure Access. This topic describes the components and prerequisites required for integrating Catalyst SD-WAN with Secure Access.

This topic describes the components and prerequisites required for integrating Catalyst SD-WAN with Secure Access.

Components Used

The information in this integration section is based on the following components:

- Cisco Secure Access–A cloud-based security service edge (SSE) solution that provides zero-trust network access to allow users to easily connect to the internet and private applications from any device
- Cisco Identity Service Engine (ISE) Version 3.3 Patch 1 (or newer)
- Cisco pxGrid Cloud–A cloud-based solution that enables administrators to share contextual information between on-prem applications (such as Cisco ISE) and cloud-based solutions (such as Secure Access) without compromising the security of your network. See the Cisco pxGrid Cloud Solution Guide for complete information.
- Cisco DNA Portal–Activate Cisco Network Experience Applications for your Cisco products. Onboard new capabilities and get more out of your network.

- Cisco Security Cloud Control—A unified management solution for your Security Cloud products and identity. Security Cloud Control is included with Secure Access.

Prerequisites

The information in this integration section assumes the following prerequisites:

- A Cisco account.
- A working knowledge of Cisco Secure Access (with full Administrator access).
- A working knowledge of Cisco Identity Services Engine (ISE) (v3.3 patch 1 or newer with full Administrator access).
- Access to and credentials for:
  - Cisco pxGrid Cloud.
  - Cisco DNA Portal.
  - Cisco Security Cloud.
- (Optional) A working knowledge of Cisco Catalyst SD-WAN configuration and features; see Integrate Catalyst SD-WAN with Secure Access.

Solution Workflow

Describes the workflow to set up context sharing between Cisco Identity Services Engine (ISE) and Cisco Secure Access works for Security Group Tags (SGTs).

This topic describes the workflow to set up context sharing between Cisco Identity Services Engine (ISE) and Cisco Secure Access works for Security Group Tags (SGTs).

This section breaks up the overall configuration into the following main steps:

1. Connect Cisco ISE and Cisco pxGrid Cloud.
2. Enable the Cisco Security Cloud Exchange.
3. Integrate Cisco ISE with Cisco Secure Access.
4. Verify Security Group Tags in Cisco Secure Access.

Connect Cisco ISE and Cisco pxGrid Cloud

Describes how to set up and complete the integration between Cisco Identity Services Engine (Cisco ISE) and Cisco pxGrid Cloud.

This section describes how to set up and complete the integration between Cisco Identity Services Engine (Cisco ISE) and Cisco pxGrid Cloud.

About Cisco pxGrid Cloud

Cisco pxGrid Cloud is a cloud-based solution that enables you to share contextual information between on-premises applications such as Cisco ISE and cloud-based solutions such as Cisco Secure Access without compromising the security of your network. It is secure and customizable, enabling you to share only the data that you want and consume only the contextual data that is relevant to your application.

Cisco pxGrid Cloud offers the following benefits:

- Plug-and-play deployment without requiring infrastructure changes to your network.

- Cisco ISE as a single source of truth for endpoint identity by delivering consistent context exchange with on-premise and cloud partners.
- Enrichment of Software as a Service-based (SaaS-based) security analysis with real-time endpoint context from Cisco ISE.
- Threat containment by isolating endpoints from the network through actions initiated from the security SaaS solutions.

Cisco pxGrid Cloud Terminology

Describes Cisco pxGrid Cloud Terminology in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

The following are some of the common terms that are used in the Cisco pxGrid Cloud solution and their meaning in the Cisco pxGrid Cloud environment:

- Offer—A set of capabilities packaged together and offered as a solution.
- Subscription—An instance of an offer being consumed by a tenant is a subscription.
- App—You can create and register applications for your product based on your requirements. For example, you can create an app that can retrieve the session and endpoint data from Cisco ISE.

  Applications with a cloud offering can be onboarded to Cisco pxGrid Cloud. After an application is onboarded, you can share data between your Cisco ISE deployment and the application.

Cisco pxGrid Cloud and Cisco ISE Integration Workflows

Describes Cisco pxGrid Cloud and Cisco ISE Integration Workflows in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Secure Access has two workflows that address the Cisco pxGrid Cloud and Cisco ISE integration. Confirm the version your environment is running and review the appropriate workflow documentation:

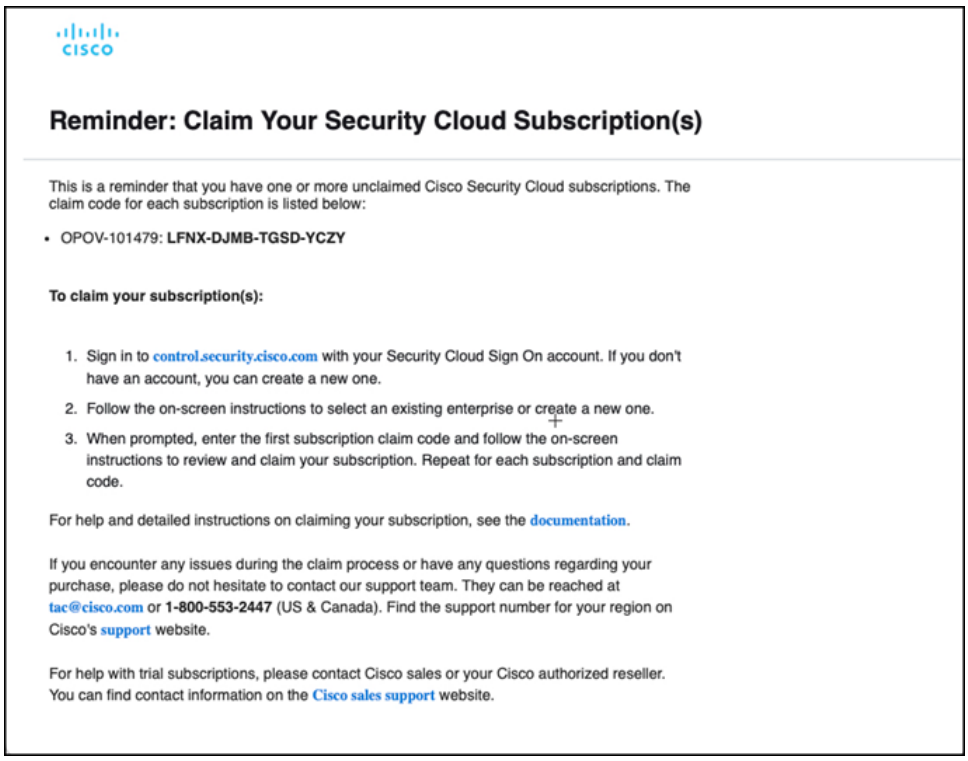
- Cisco pxGrid Cloud and Cisco ISE Integration Workflow for Cisco ISE Release 3.4 Patch 1 and Cisco ISE Release 3.3 Patch 5.
- Cisco pxGrid Cloud and Cisco ISE Integration Workflow for Other Cisco ISE Releases

Enable Cisco Security Cloud Exchange

Describes how to onboard Cisco Secure Access to Cisco Security Cloud.

Procedure

1. Claim your security cloud subscription. The claim link would be sent to the cloud account administrator via email. See the sample message below:



Reminder: Claim Your Security Cloud Subscription(s)

This is a reminder that you have one or more unclaimed Cisco Security Cloud subscriptions. The claim code for each subscription is listed below:

- OPOV-101479: **LFNX-DJMB-TGSD-YCZY**

To claim your subscription(s):

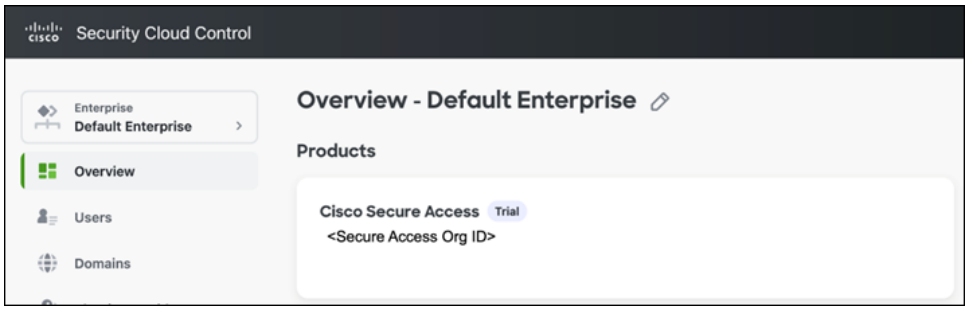
1. Sign in to control.security.cisco.com with your Security Cloud Sign On account. If you don't have an account, you can create a new one.
2. Follow the on-screen instructions to select an existing enterprise or create a new one.
3. When prompted, enter the first subscription claim code and follow the on-screen instructions to review and claim your subscription. Repeat for each subscription and claim code.

For help and detailed instructions on claiming your subscription, see the documentation.

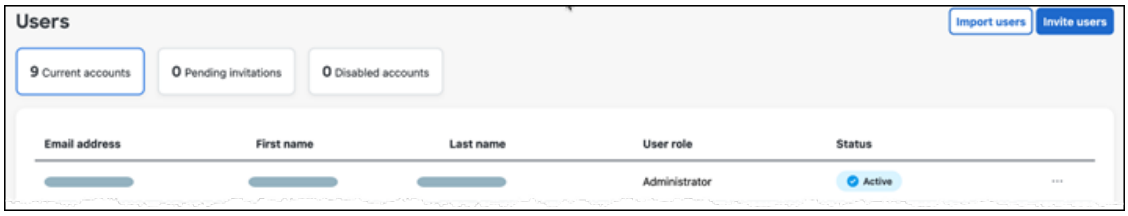
If you encounter any issues during the claim process or have any questions regarding your purchase, please do not hesitate to contact our support team. They can be reached at tac@cisco.com or **1-800-553-2447** (US & Canada). Find the support number for your region on Cisco's support website.

For help with trial subscriptions, please contact Cisco sales or your Cisco authorized reseller. You can find contact information on the Cisco sales support website.

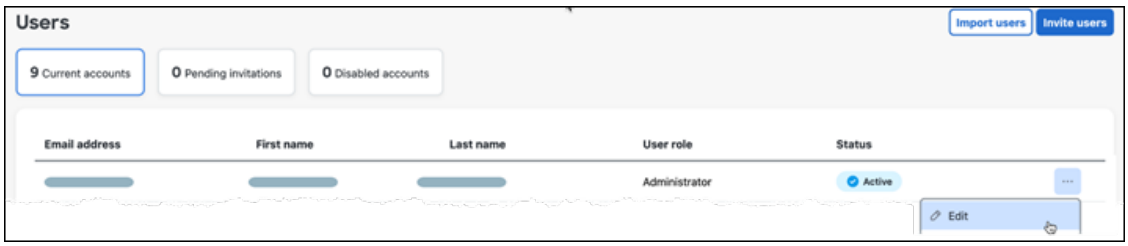
2. Log in and verify that your cloud account subscription is associated with your provisioned Secure Access organization. To do so, navigate to the **Overview** screen. You should see **Cisco Secure Access** listed under Products as shown in the following example view.



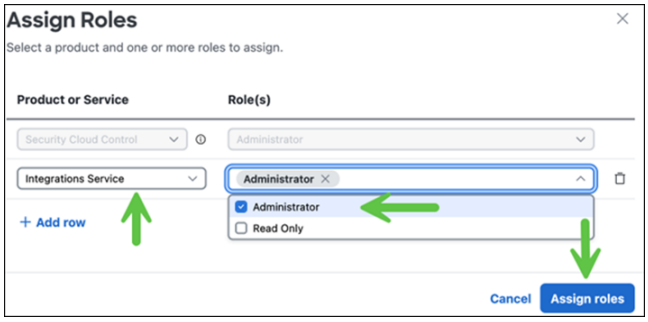
3. Next, navigate to **Users** to see a list of the user(s) that are members of your Cisco Security Cloud enterprise as shown in the following example view. You'll want to choose one user to be the administrator for integration services.



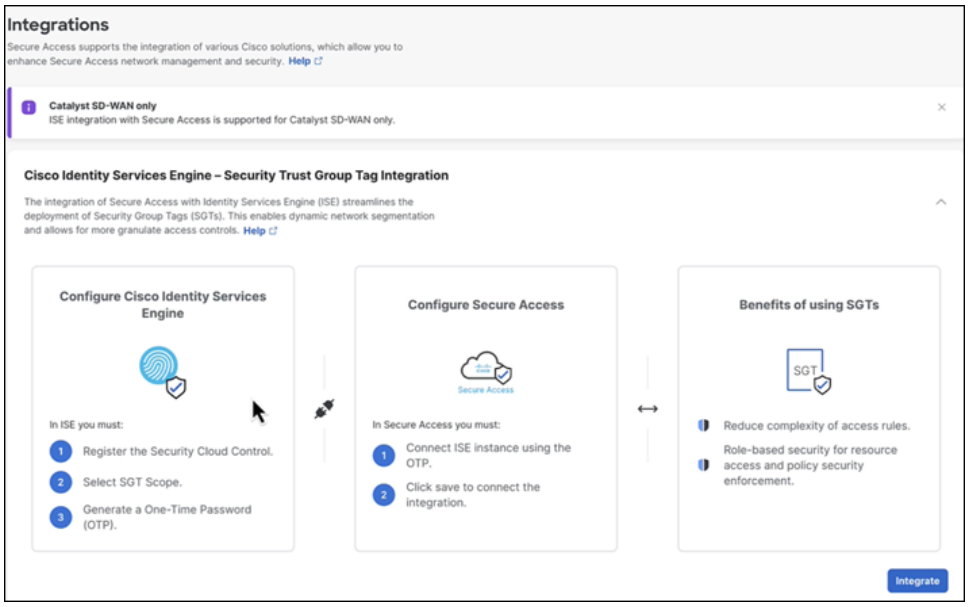
4. Click the ellipse icon (. . .) for the user you've chosen as the integrations administrator, then click **Edit**.



5. Click **Assign roles to user** and click **+ Add Row**.
6. Under **Product or Service**, choose **Integrations Service** and under **Role(s)** check **Administrator**, then click **Assign roles**.



7. Open a new browser tab to sign in to **Cisco Secure Access** using the Integrations Service admin account you just created. Your Secure Access login link will be in this format: (https://dashboard.sse.cisco.com<SecureAccessOrgID/overview>)
8. Navigate to **Admin** > **Management** > **Integrations**. You should see the resulting Integrations page similar to the following example.



> **Note**
>
> If your integrations page does not load or displays an error, reach out to your Cisco representative or Cisco Support for assistance.

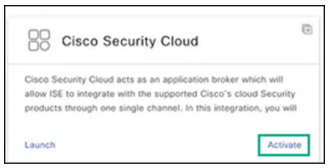
Integrate Cisco ISE with Secure Access

Provides instructions for completing the Integrate Cisco ISE with Secure Access workflow in Cisco Secure Access. This topic describes how to complete the integration between Cisco ISE and Cisco Secure Access.

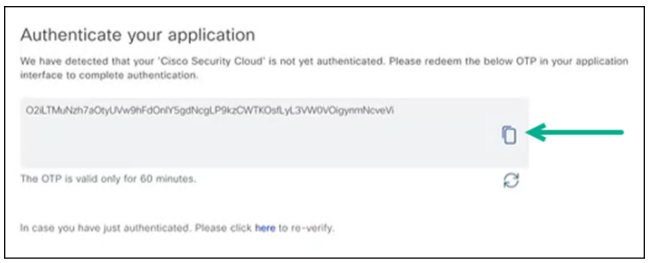
This topic describes how to complete the integration between Cisco ISE and Cisco Secure Access.

Procedure

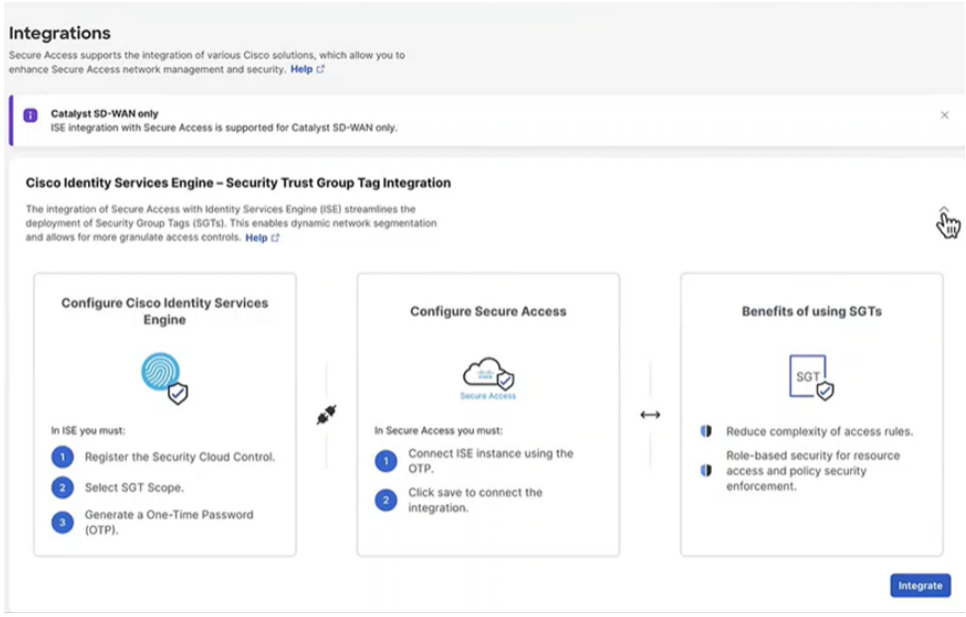
1. Return to the **Cisco DNA Portal** tab, search for the **Cisco Security Cloud** application, and click **Activate**.



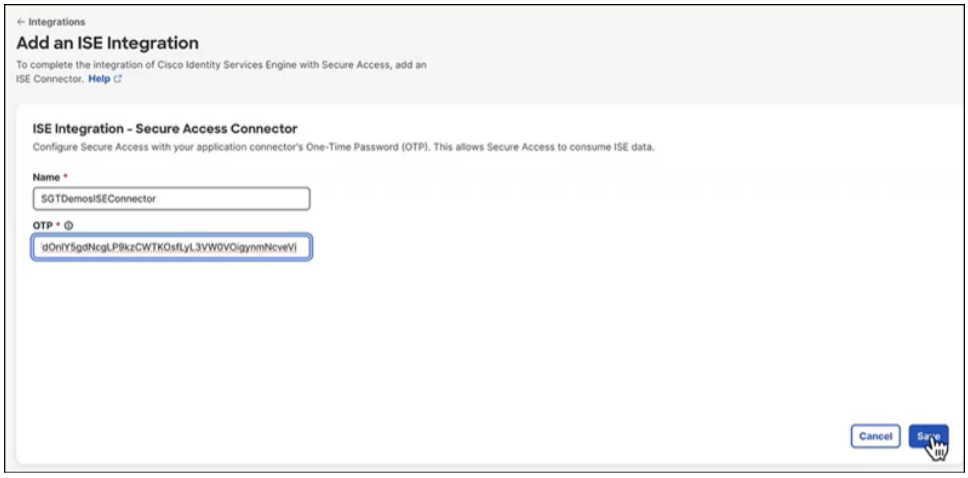
2. Choose **Authenticate your application** and copy the resulting token to your clipboard by clicking the copy icon.



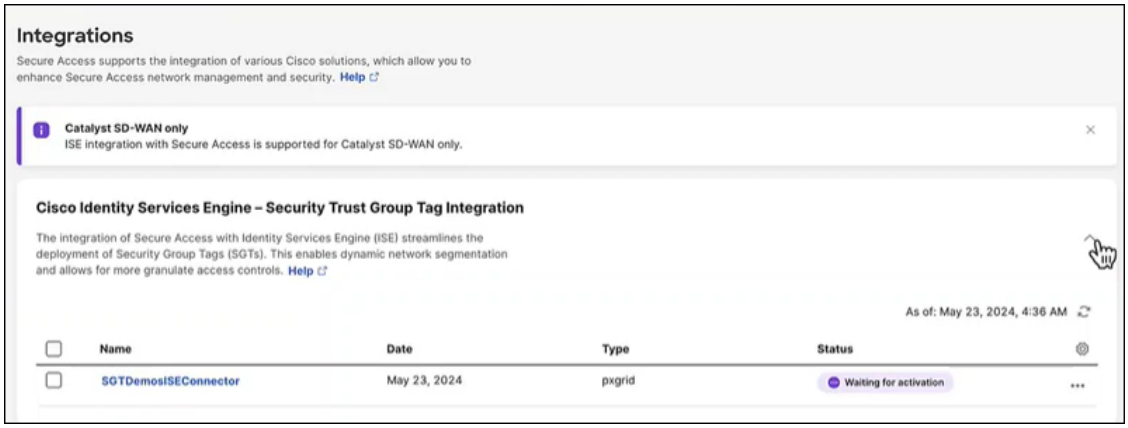
3. Click **Exit**.
4. Return to the Secure Access tab.
5. Navigate to **Admin** > **Management** > **Integrations**.



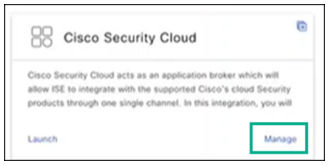
6. Click **Integrate** to add the ISE integration.
7. Enter a **Name** for the ISE integration, paste in the copied token, and then click **Save**.



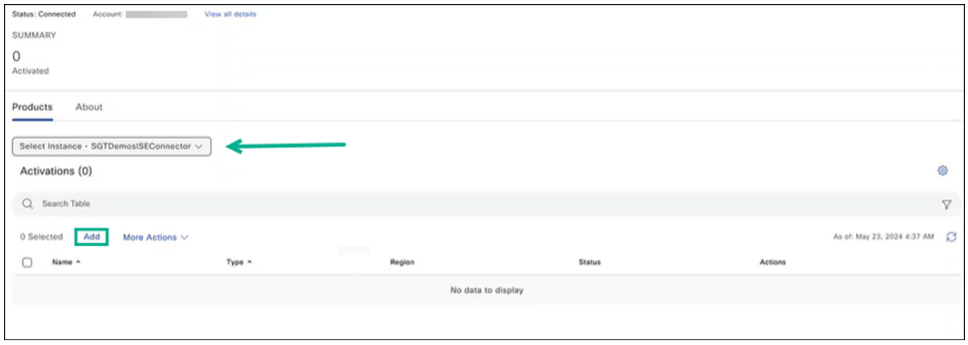
8. The system returns a confirmation banner indicating a **New ISE Cluster added**.
9. Expand the integration pane to view the status of the ISE cluster (waiting for activation).



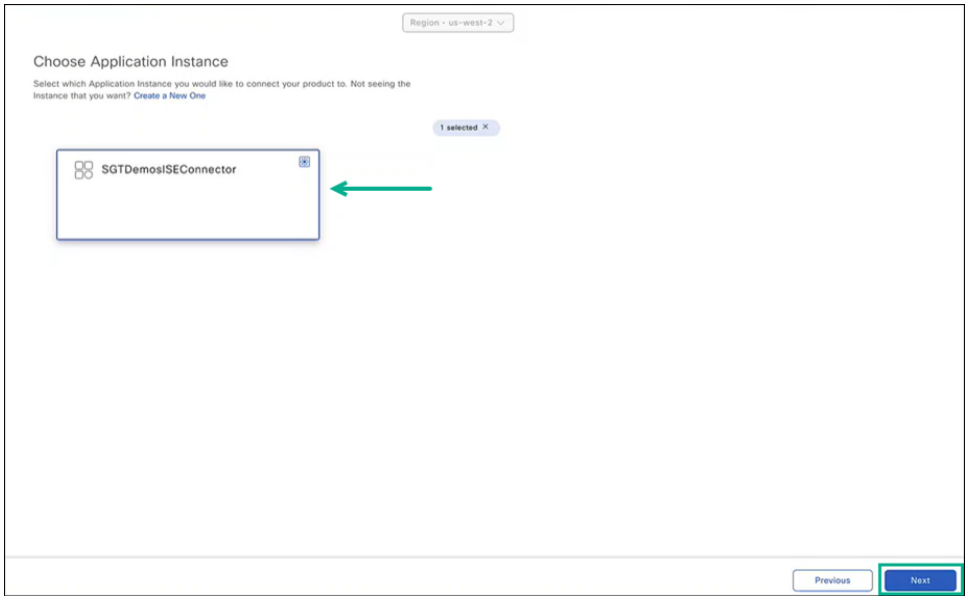
10. Return to the **Cisco DNA Portal** tab and the **Cisco Security Cloud** application.
11. On the **Cisco Security Cloud** tile, click **Manage**.



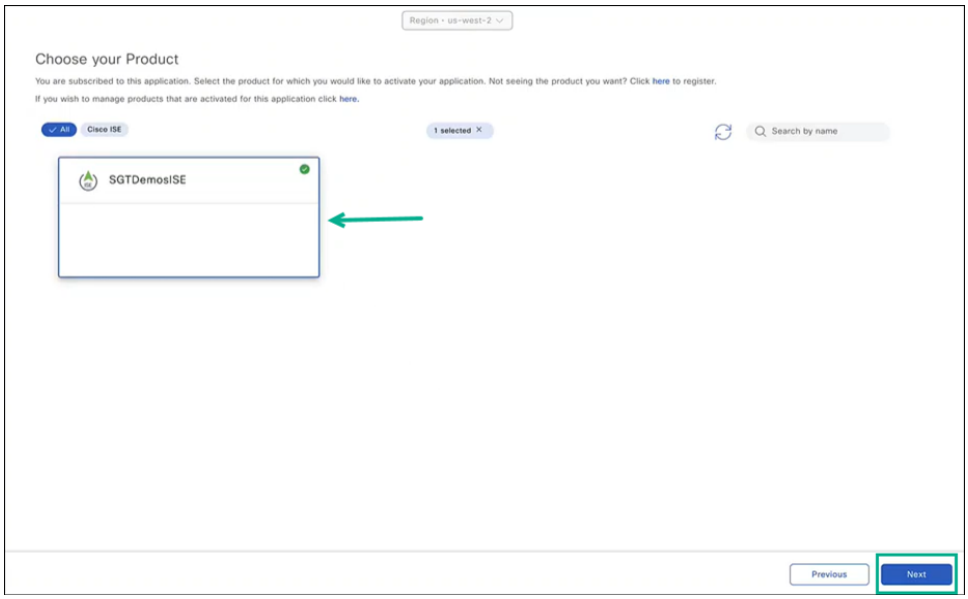
12. Choose **Add** and select the ISE application instance.



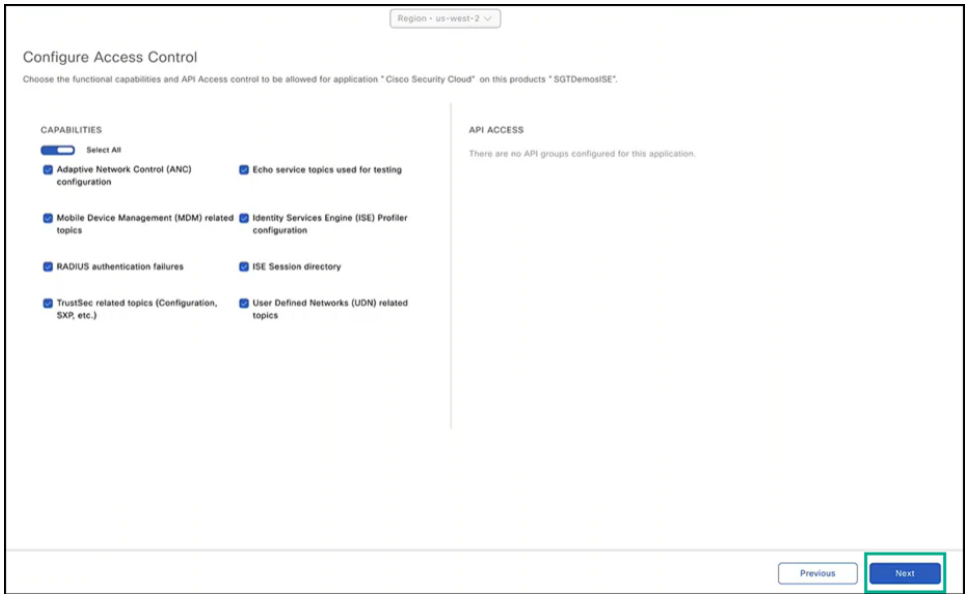
13. Choose the application instance that will be associated with your subscription, then click **Next**.



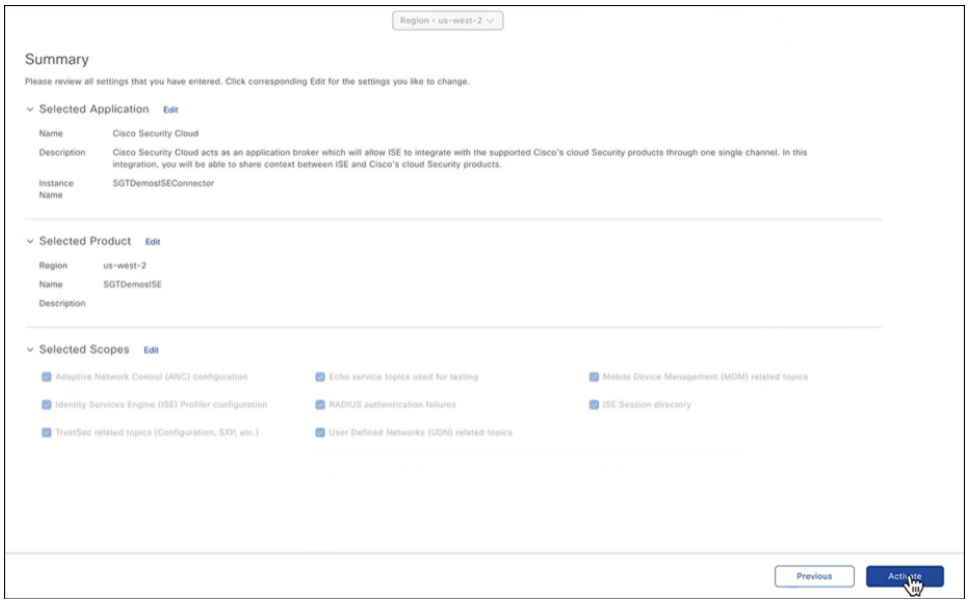
14. Choose the product for which you want to associate the application. In this example choose Cisco ISE, then click **Next**.

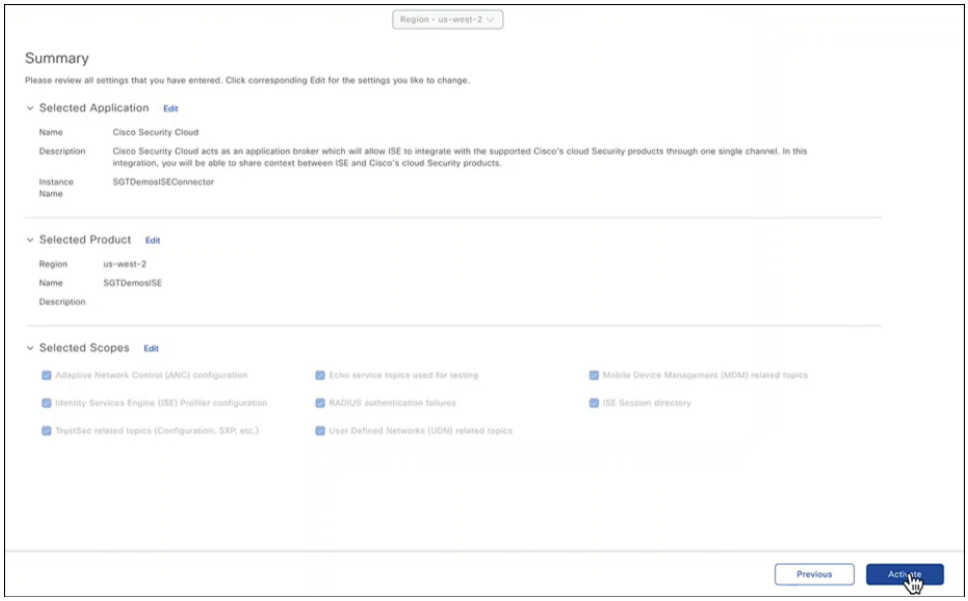


15. Choose capabilities and API access for the application and click **Next**.

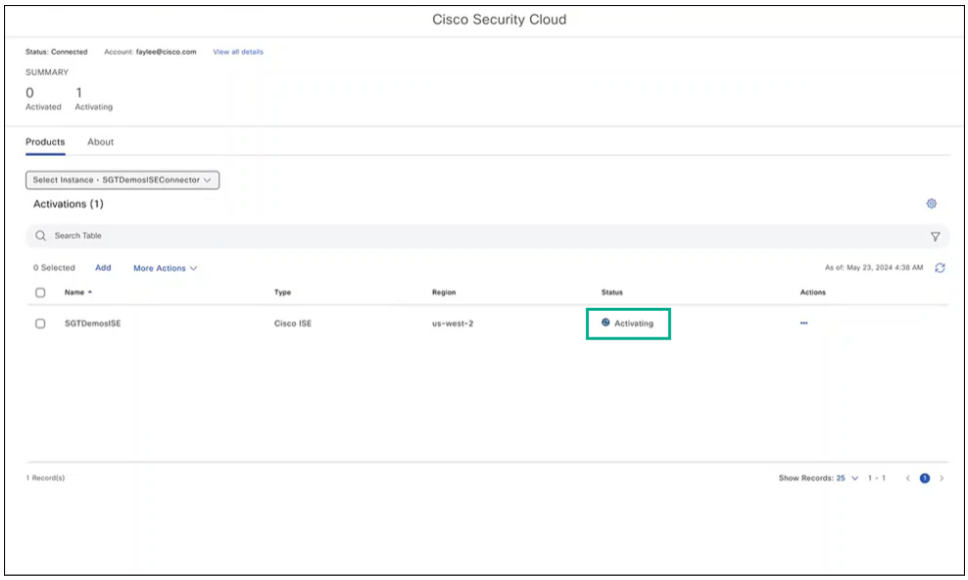


16. Review the application summary. You can click **Edit** to make any changes. Click **Activate** to complete the setup.





17. Monitor the Cisco Security Cloud dashboard to view the status.



18. Once the instance is active in Cisco Security Cloud, it should sync to Cisco Secure Access. You can switch between the tabs to view the state of the sync.

What to do next

We strongly recommend modifying or creating a private access rule to further incorporate this successful integration. You can now include private IP address from the security group tag (SGT) originating from the ISE application as either the source or the destination.

Verify and Monitor Context Sharing

Describes how to verify and monitor context sharing between Cisco ISE and Secure Access for Security Group Tags (SGTs).

This section describes how to verify context sharing between Cisco ISE and Secure Access works for Security Group Tags (SGTs).

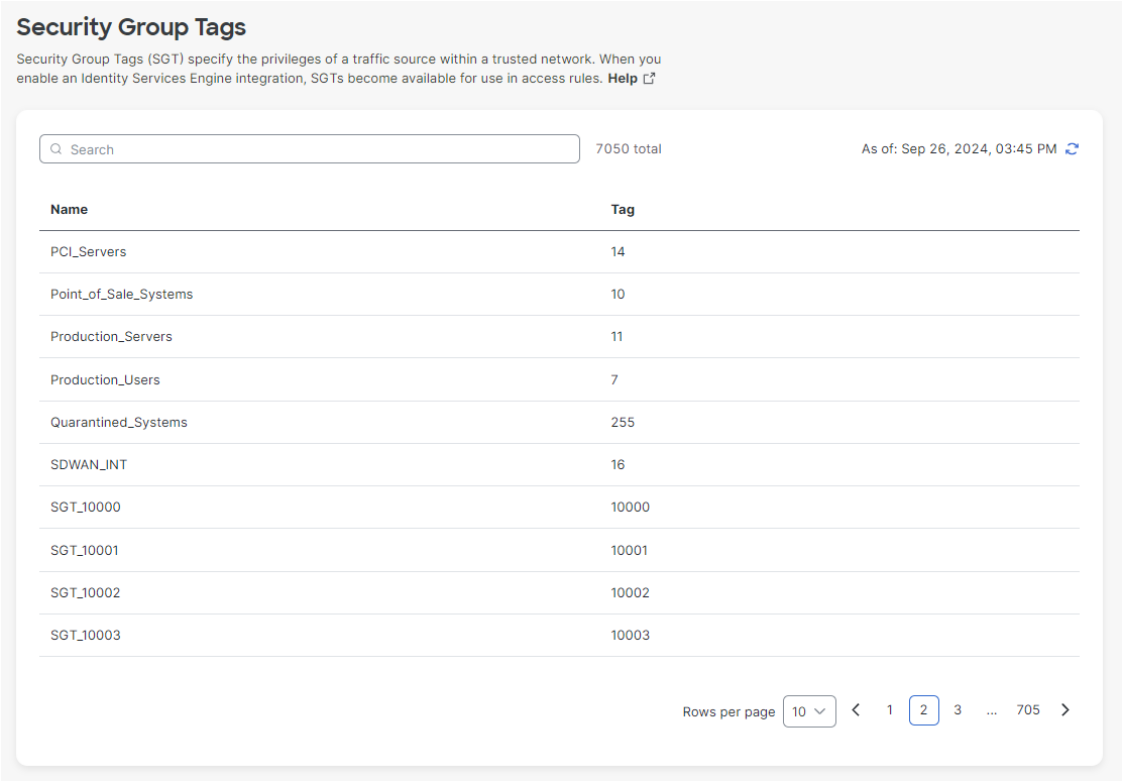
Verify Context Sharing in Secure Access

Provides instructions for verifying Context Sharing in Secure Access. Security Group Tags (SGTs) are added to Secure Access as source resources when Cisco ISE is integrated with Secure Access.

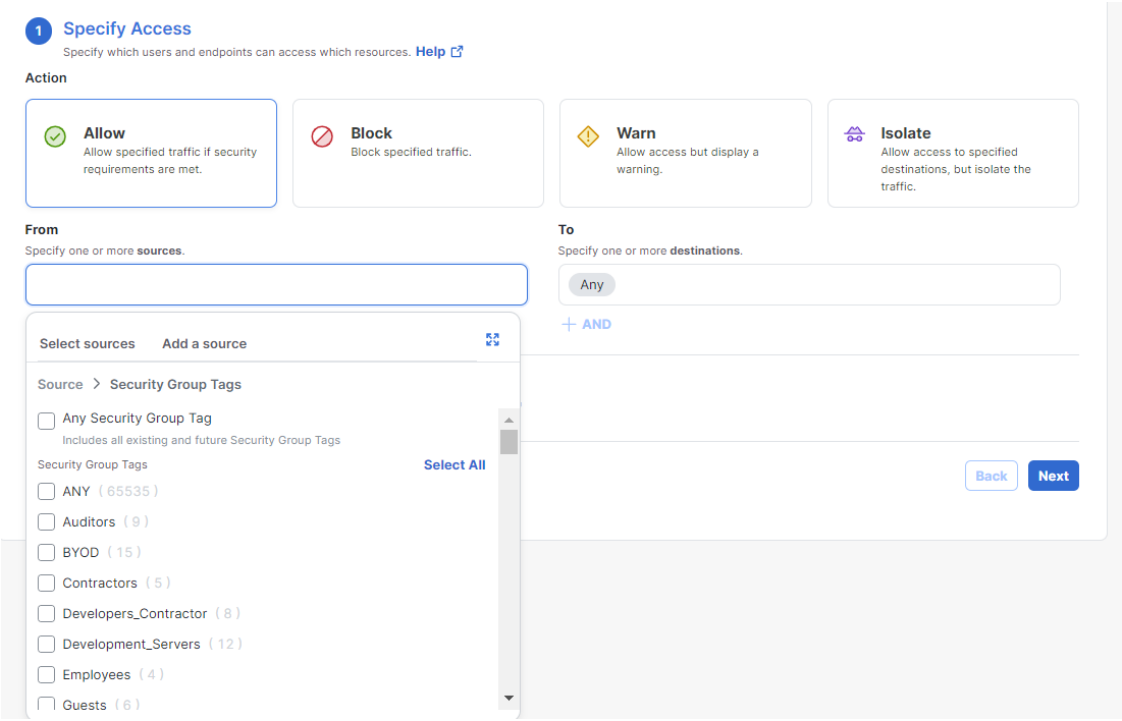
Security Group Tags (SGTs) are added to Secure Access as source resources when Cisco ISE is integrated with Secure Access. Once added, these SGTs can be used when configuring access rules. See Security Group Tags on page 2656 for more information.

Procedure

1. Navigate to **Resources** > **Sources and Destinations** > **Security Group Tags** to verify that the SGTs are shared as resources.



2. Navigate to **Secure** > **Policy** > **Access Policy**.
3. Click the **Add Rule** drop down and choose **Internet Access** to verify that the SGTs are shared as source objects for internet access rules.



4. From the **Select sources** drop down, choose **Security Group Tags** as a rule source.

   From there, you can select **Any Security Group Tag**, which will include all existing and future SGTs in the rule. Alternately, you can select any (or all) existing SGTs for more granular internet access rules.

Activity Search in Secure Access

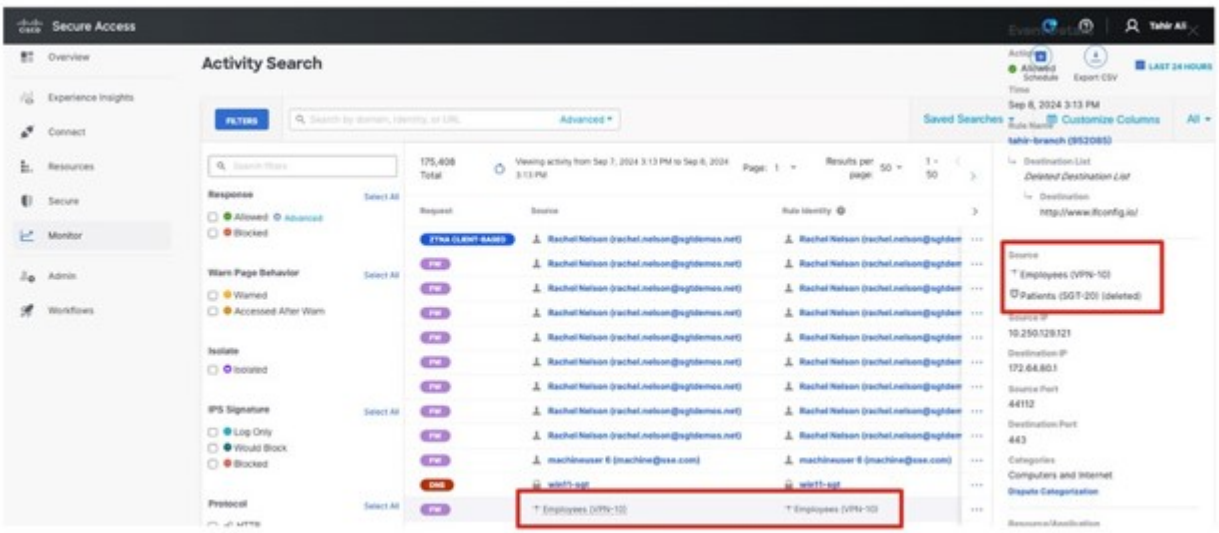
Provides instructions for using the Activity Search report to search for activity from the sources in your environment over a selected time period.

To search for activity from the sources in your environment over a selected time period, use the Activity Search report. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time period.

Procedure

---

1. Navigate to **Monitor** > **Reports** > **Activity Search**. This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time.



2. Hover over individual column values to apply it as a search filter or to exclude it from the search.

Integrate Catalyst SD-WAN with Secure Access

Integration Catalyst SD-WAN with Secure Access to share network context and apply consistent security enforcement for users, devices, and workloads.

Cisco Catalyst SD-WAN integrates with Cisco Secure Access to share network context between the platforms for the purpose of applying consistent security enforcement for users, devices and workloads across the enterprise. Context-aware security policies become key for implementing and achieving a true zero-trust framework for the enterprise.

With this integration feature, administrators can automatically build tunnels with reliability to Secure Access from a Catalyst SD-WAN branch and share VPN ID/name and Security Group Tag (SGT) context learned from the enterprise. Cisco Catalyst SD-WAN can be deployed and connected using either virtual or physical secure routers at branch offices, data center networks, and regional hubs. This integration allows IT teams to:

- Connect any user to any application, with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility on a Secure Access Service Edge (SASE)-enabled architecture.
- Ensure a predictable user experience for applications.
- Optimize Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) connections.
- Offer integrated security, either on-premises or in the cloud.

This section describes how to enable inline context propagation, represented by VPN IDs and Security Group Tags (SGTs).

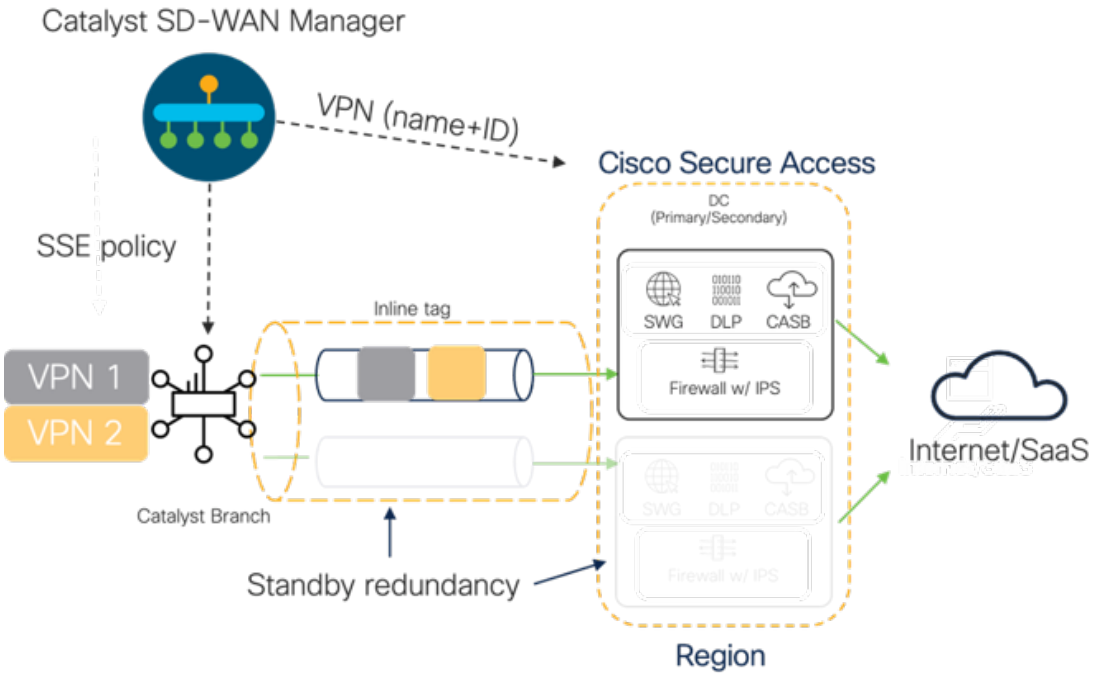
Solution Overview

Provides an overview of the Catalyst SD-WAN integration.

Applying consistent security enforcement for users, devices, and workloads across the enterprise is top-of-mind for any CISO. Whether the security enforcement is within the campus, branch, cloud, or data centers; consistent context-aware security policies are needed to implement and achieve a true zero-trust framework for an enterprise.

Use cases for context-aware security enforcement can revolve around employees, guests, or IoT networks behind a Catalyst SD-WAN branch that need to securely access internet/SaaS applications, with Cisco Secure Access providing cloud-based security enforcement.

With this integration, Cisco Secure Access administrators can use the rich enterprise context shared from Catalyst SD-WAN to configure simpler but granular policy control towards internet/SaaS for branch users.



Note

For information about context sharing with Cisco ISE, see Integrate Identity Services Engine (ISE) with Secure Access.

Components and Prerequisites

Describes the components and prerequisites required for integrating Catalyst SD-WAN with Secure Access.

This topic describes the components and prerequisites required for integrating Catalyst SD-WAN with Secure Access.

Components Used

The information in this integration section is based on the following components:

- Cisco Catalyst SD-WAN release 20.15/17.15
- Cisco Secure Access
- Cisco ISE 3.1 patch or higher

Prerequisites

- A working knowledge of Cisco Catalyst SD-WAN configuration and features.
- A working knowledge of Cisco Secure Access.

Important

The information in this section is based on devices configured in a specific lab environment. All of the devices used started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any procedure or command.

Solution Workflow

Describes how context sharing between Catalyst SD-WAN and Secure Access works for VPN ID.

The following is the workflow for context sharing between Catalyst SD-WAN and Secure Access for VPN ID:

1. Catalyst SD-WAN Manager integrates with Cisco Secure Access using SSE cloud credentials.
2. Cisco Secure Access learns VPN identities using APIs (out-of-band).
3. In Catalyst SD-WAN Manager, the Secure Service Edge policy group is configured to share VPN context in IPsec tunnels.
4. Once the tunnels are up, VPN ID context is shared in the IPsec metadata header inline.
5. VPN identities are leveraged in Secure Access internet access rules.
6. Packets with VPN ID context are then subject to Secure Access policy match as source objects.

Important

VPN ID context sharing is optional. Be aware that if the same VPN ID (*VPN 88* for example) is assigned across different branches, then traffic coming into Secure Access from these branches is subject to the same policy. A Secure Access policy rule cannot differentiate traffic between branches using the same VPN ID.

Related Information

Describes Related Information in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

Cisco Catalyst SD-WAN Getting Started Guide Cisco Catalyst SD-WAN Getting Started Guide

Cisco Catalyst SD-WAN Security Configuration Guide Cisco Catalyst SD-WAN Security Configuration Guide

Cisco Catalyst SD-WAN Segmentation Configuration Guide Cisco Catalyst SD-WAN Segmentation Configuration Guide

Configure Context Sharing Between Catalyst SD-WAN and Secure Access

Describes how to set up context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

This topic describes how to set up context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

Prerequisites

- Make sure the DNS and IP domain-lookup command is configured on vpn0 for devices and Cisco SD-WAN Manager with both having internet access.
- Enable NAT on the WAN of the SD-WAN edge internet interface.
- Re-direct branch internet/SaaS-bound traffic from the branch LAN towards Cisco Secure Access, using the SSE default route in config-group or policy-group (data policy for specific application based redirect). See documentation for more details.
- Use config-group/policy-group infra only on Catalyst SD-WAN Manager.

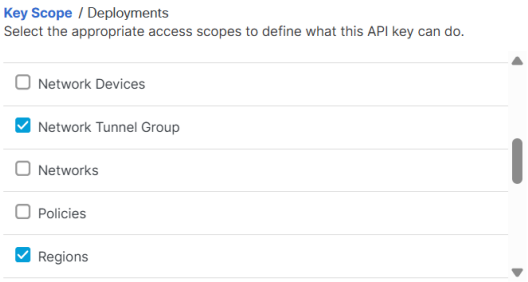
Generate API Key Pair for Context Sharing

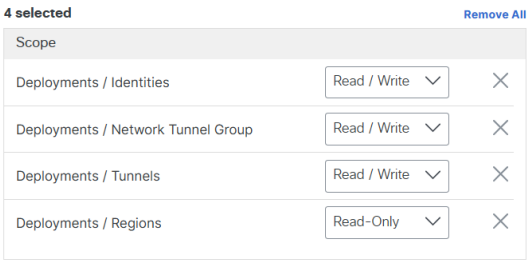
Provides instructions for completing the Generate API Key Pair for Context Sharing workflow in Cisco Secure Access. To configure the API keys needed for Catalyst SD-WAN Manager and Cisco Secure Access to share information, you need to generate key pair from Cisco Secure Access.

To configure the API keys needed for Catalyst SD-WAN Manager and Cisco Secure Access to share information, you need to generate key pair from Cisco Secure Access.

Procedure

1. Log into Cisco Secure Access and navigate to **Admin** > **Management** > **API Keys**.
2. In the upper right, click the **Add** button.
3. Expand the **Key Scope** section and select the options **Identities**, **Network Tunnel Group**, and **Tunnels**.
4. Assign **Read/Write** permissions to the selected scopes.
5. Set **Regions** to **Read Only**.





6. When all scopes are defined, click **CREATE KEY**. Copy and save the resulting key and secret.

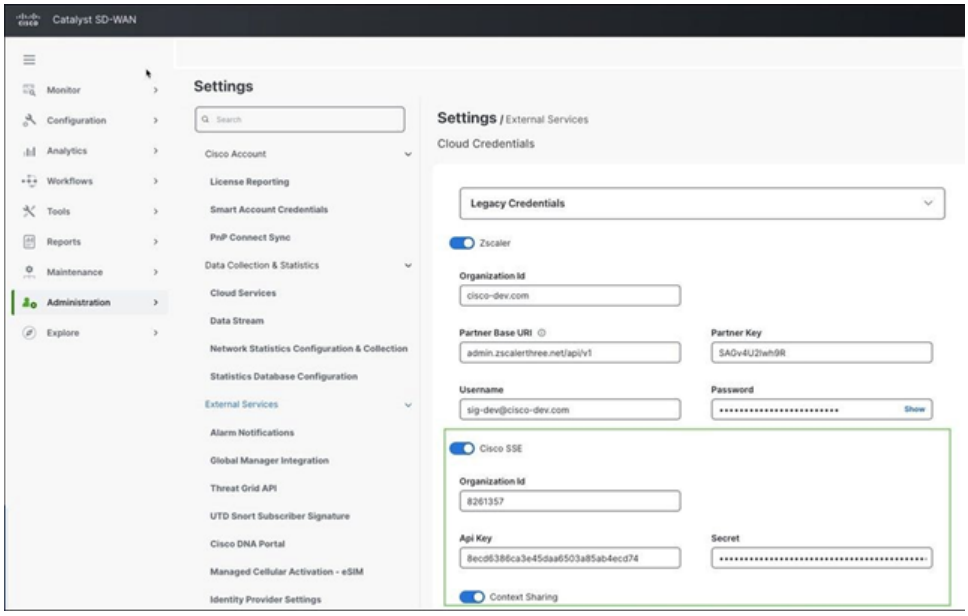
Create Cisco Secure Access Credentials

Provides instructions for completing the Create Cisco Secure Access Credentials workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. In another browser tab, log into Catalyst SD-WAN Manager, and navigate to **Administration** > **Settings** > **Cloud Credentials**
2. Enable **Cisco SSE**.
3. Paste your Secure Access **Organization Id**, **Api key**, and **Secret**.
4. Enable **Context Sharing**.

5. Click **Add**.



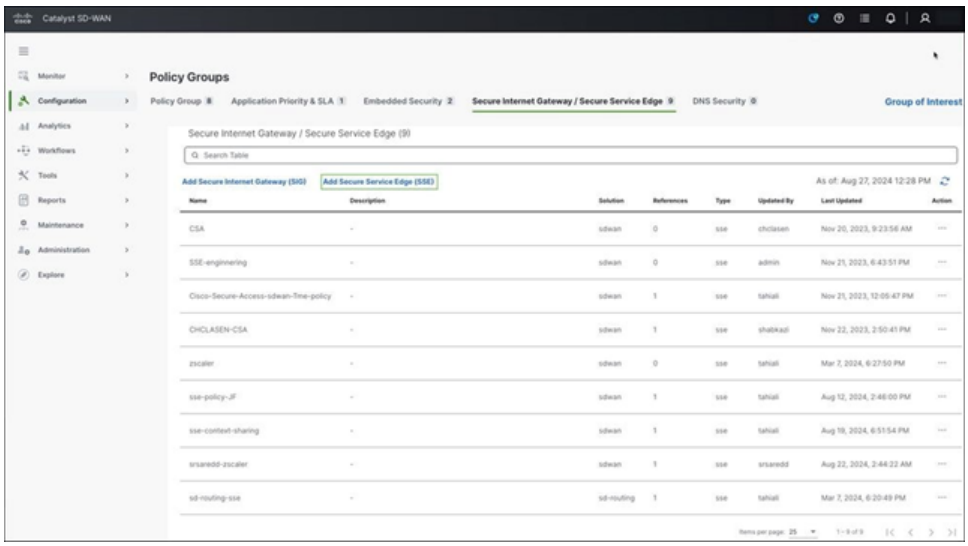
Add a Secure Service Edge (SSE) Policy Group

Provides instructions for adding a Secure Service Edge (SSE) Policy Group in Cisco Secure Access.

Procedure

---

1. Navigate to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**.
2. Click **Add Secure Service Edge (SSE)** to configure the SSE connectivity policy.

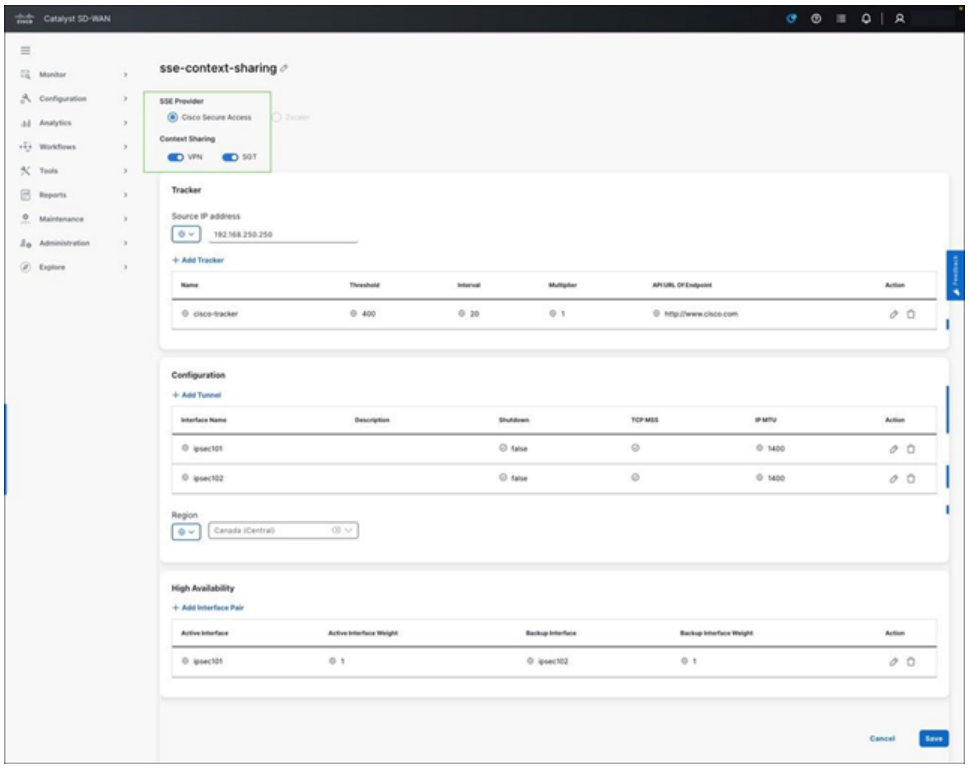


Enable Context Sharing

Provides instructions for completing the Enable Context Sharing workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Under SSE Provider, select **Cisco Secure Access**.
2. Under **Context Sharing**, enable **VPN** and/or **SGT** for context sharing for your SSE policy.
3. Click **Save**.



Verify and Monitor Context Sharing

Describes Verify and Monitor Context Sharing in Cisco Secure Access. This topic describes how verify context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

This topic describes how verify context sharing between Catalyst SD-WAN and Secure Access for VPN IDs.

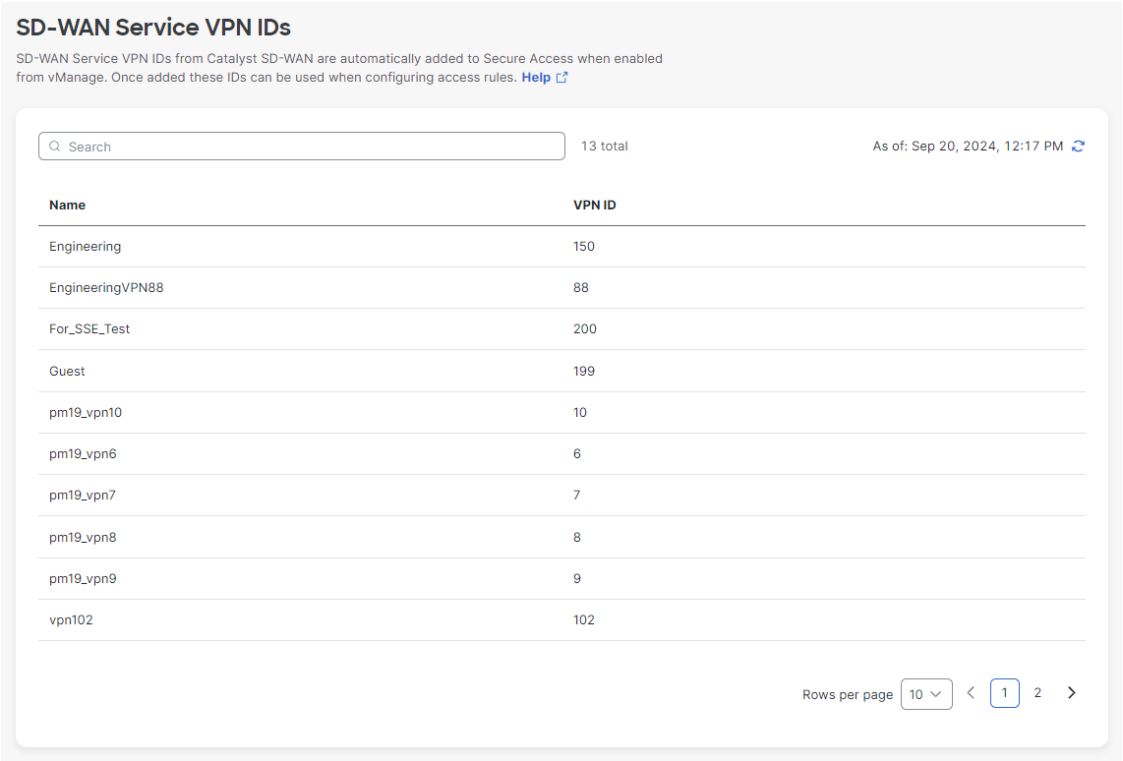
Verify Context Sharing in Secure Access

Provides instructions for completing the Verify Context Sharing in Secure Access workflow in Cisco Secure Access. Service VPN IDs from Catalyst SD-WAN are automatically added to Secure Access as source resources when enabled from the SD-WAN Manager.

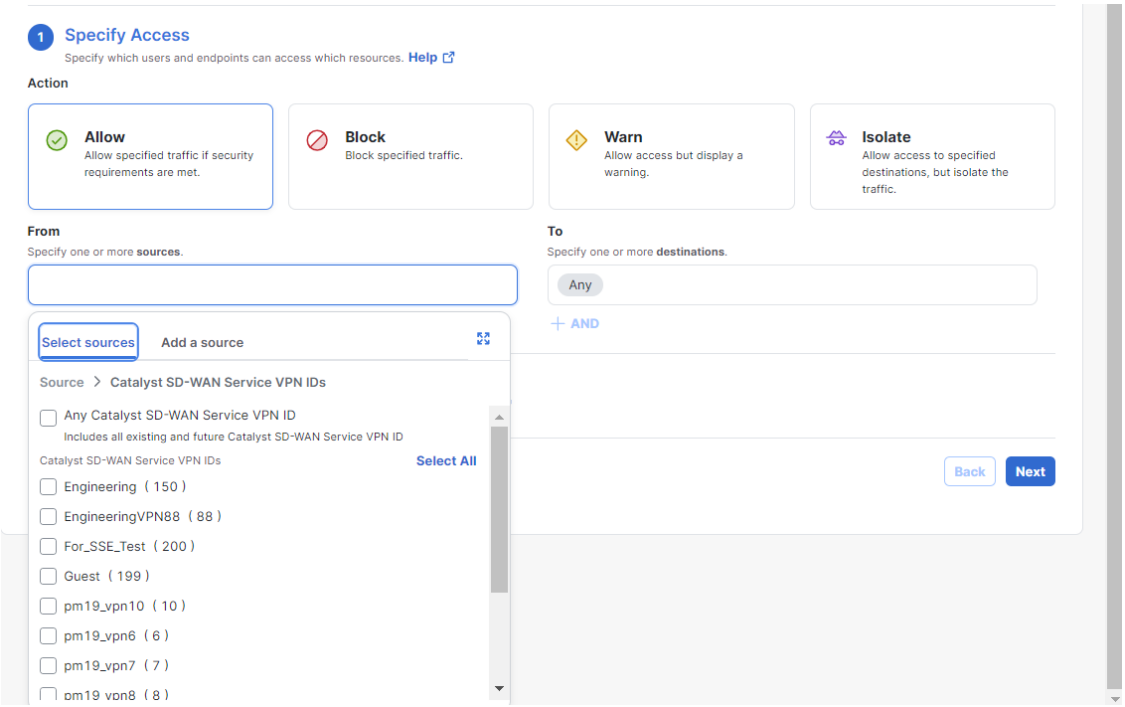
Service VPN IDs from Catalyst SD-WAN are automatically added to Secure Access as source resources when enabled from the SD-WAN Manager. Once added, these VPN IDs can be used when configuring access rules.

Procedure

1. Navigate to **Resources** > **Sources and Destinations** > **SD-WAN Service VPN IDs** to verify that the VPN IDs are shared as resources.



2. Navigate to **Secure** > **Policy** > **Access Policy**.
3. Click the **Add Rule** drop down and choose **Internet Access** to verify that the VPN IDs are shared as source objects for internet access rules.



4. From the **Select sources** drop down, choose **Catalyst SD-WAN Service VPN IDs** as a rule source.

   From there, you can select **Any Catalyst SD-WAN Service VPN ID**, which will include all existing and future VPN IDs in the rule. Alternately, you can select any (or all) existing VPN IDs for more granular internet access rules.

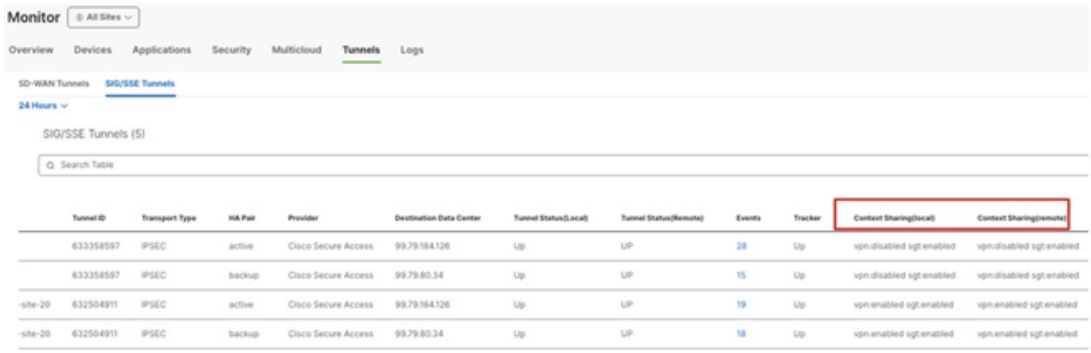
Monitor Context Sharing in SD-WAN Manager

Provides instructions for completing the Monitor Context Sharing in SD-WAN Manager workflow in Cisco Secure Access. You can view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device.

You can view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device.

Procedure

Under SD-WAN Manager Tunnel monitoring Dashboard.



Monitor Secure Access Tunnels using the CLI

Describes Monitor Secure Access Tunnels using the CLI. To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the show sse all command.

To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the `show sse all` command.

```
Device# show sse all

**************************************
   SSE  Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN

Tunnel name : Tunnel15000002
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Backup
Local state: Up
```

```
Tracker state: Up
Destination Data Center: 44.241.136.173
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

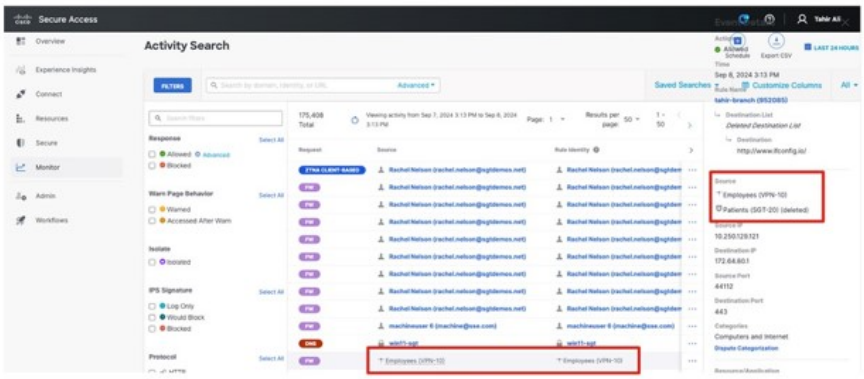
Activity Search in Secure Access

Provides instructions for using the Activity Search report to search for activity from the sources in your environment over a selected time period.

To search for activity from the sources in your environment over a selected time period, use the Activity Search report. The report lists all security (and non-security) activity for the sources reporting to Secure Access for the selected time period.

Procedure

1. Navigate to **Monitor** > **Reports** > **Activity Search**. This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests or traffic events for your organization, tracked over time.



2. Hover over individual column values to apply it as a search filter or to exclude it from the search.

Integrate Cisco Identity Intelligence with Secure Access

Integrate Cisco Identity Intelligence into Secure Access to address issues with user identity fragmentation that can complidate user trust assessment, consistent policy enforcement, and breach detection.

Cisco Identity Intelligence is an AI-powered solution that addresses user identity fragmentation. Fragmentation occurs when an organization relies on multiple identity sources, including:

- Traditional Identity Providers (IdPs), such as Entra ID (formerly Azure AD), Duo, and Okta.
- Non-traditional sources, such as Github, Google, and Salesforce.
- HR systems, such as Workday.

Fragmented identities complicate user trust assessment, consistent policy enforcement, and breach detection. Identity Intelligence continuously monitors user identities, behaviors, and access patterns to detect anomalies and enforce adaptive security policies, mitigating unauthorized access risks.

Identity Intelligence is available as a shared Cisco service through Cisco Security Cloud Control. Security Cloud Control is a platform for managing your Cisco security products. By connecting your IdPs to Security Cloud Control, a unified identity context becomes available to Cisco products such as Secure Access, Cisco XDR, and Cisco Duo. This approach streamlines identity management and ensures consistent identity context across multiple services.

The Cisco Identity Intelligence integration, accessible via Security Cloud Control, is included at no additional charge with any Secure Access subscription. This does not include access to the standalone Cisco Identity Intelligence dashboard. For more information, see Cisco Identity Intelligence.

Configure a New Duo and Cisco Identity Intelligence Tenant with Secure Access

This document describes how to claim and activate your Secure Access subscription with a new Duo and Cisco Identity Intelligence tenant.

Your Secure Access subscription includes a limited license to Duo and Cisco Identity Intelligence at no additional charge. This limited access to Cisco Identity Intelligence provides the essential identity visibility and security features required for your deployment, though it may not include the full suite of advanced features available in standalone Duo or Cisco Identity Intelligence premium subscriptions. See, Duo Limited Usage Details for more information.

This document describes how to claim and activate your Secure Access subscription with a new Duo and Cisco Identity Intelligence tenant.

Before you begin

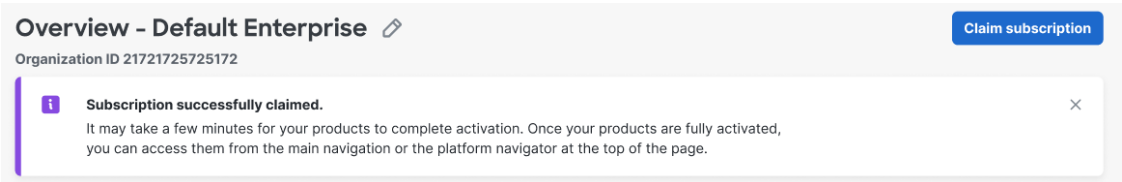
Confirm the following before using this procedure.

- You are not already a Duo customer. If you are an existing Duo customer, follow this procedure instead: Configure an Existing Duo and Cisco Identity Intelligence Tenant with Secure Access.
- **Claim code:** You have the welcome email with the subscription claim code automatically sent to the Provisioning Contact specified when your organization purchased Secure Access. If you do not have the email or claim code, contact Cisco Technical Assistance. For more information, see Overview of Subscription Process in Cisco Security Cloud Control documentation.
- **Security Cloud Control Administrator Group**: Within Security Cloud Control, the administrator must be a member of the **All Products Administrator** group. To add an administrator to Security Cloud Control and assign them to a group, navigate to **Platform Management** > **Access Management** > **Administrator Access** in the Security Cloud Control dashboard.

At the end of this process, you will have four integrated accounts: Security Cloud Control (SCC), Duo, Secure Access, and Cisco Identity Intelligence (CII).

Procedure

1. In Security Cloud Control, enter your Secure Access Subscription Code. For a detailed procedure, see Claim a Subscription in Security Cloud Control documentation.

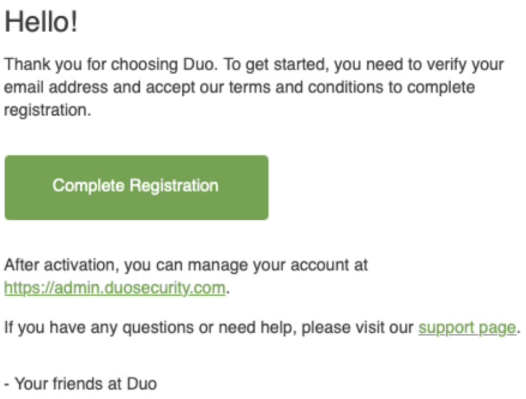


   Secure Access will begin the activation process within Security Cloud Control. Secure Access will be listed under Products in the left navigation menu.

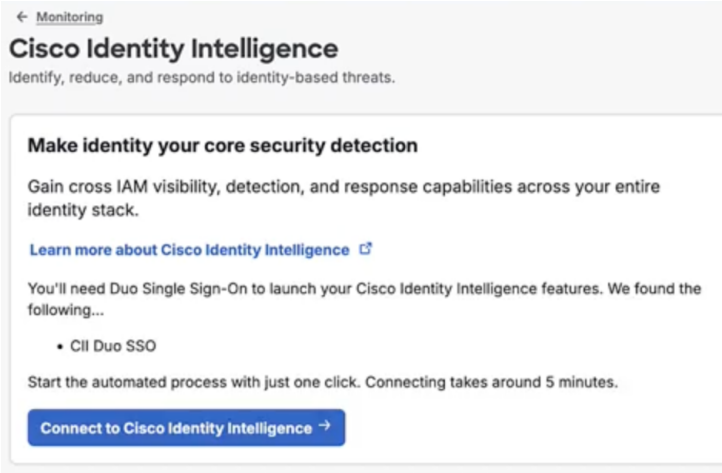
2. Next, activate Duo and Cisco Identity Intelligence. Click **Action required** > select **Create new account** > click **Activate**. This may take a minute to activate.



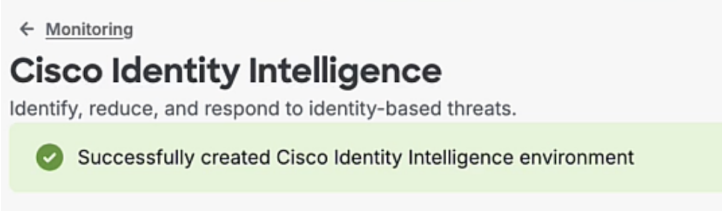
3. The SCC admin who initiated the activation process (received the initial claim code), gets an email from Duo to complete registration.



4. Click **Complete Registration** and follow the steps to setup your first Duo Admin account.
5. Integrate Duo with Cisco Identity Intelligence. For a detailed procedure, see Duo Identity Security with Cisco Identity Intelligence.
6. In Duo's dashboard, click **Monitoring** > **Cisco Identity Intelligence** > **Connect to Cisco Identity Intelligence**.



A success notification appears when Cisco Identity Intelligence is connected.



What to do next

Add the same Identity Providers (IdPs) to both Cisco Identity Intelligence (via Security Cloud Control) and Secure Access. For more information, see After Integrating Cisco Identity Intelligence.

For more information on the Systems Logs feature, see Systems Logs.

Configure an Existing Duo and Cisco Identity Intelligence Tenant with Secure Access

This document describes how to claim and activate your Secure Access subscription with an existing Duo account and Cisco Identity Intelligence tenant.

This procedure is specific to existing Duo accounts and does not use the restricted Duo license provided with new Secure Access subscriptions. If you are performing a first-time setup for a new Duo account and CII tenant follow these instructions here: Configure a New Duo and Cisco Identity Intelligence Tenant with Secure Access.

Before you begin

Confirm the following before using this procedure.

- You are an existing Duo Advantage or Premier customer with an existing Cisco Identity Intelligence tenant in Cisco Security Cloud Control. For more information, see Duo Identity Security with Cisco Identity Intelligence.

  If you are a Duo Essentials customer, you are entitled to a Cisco Identity Intelligence tenant with a Duo limited license. For more information see, Duo Limited Usage Details.

- **Claim code**: You have the welcome email with the subscription claim code automatically sent to the Provisioning Contact specified when your organization purchased Secure Access. If you do not have the email or claim code, contact Cisco Technical Assistance. For more information, see Overview of Subscription Process in Cisco Security Cloud Control documentation.

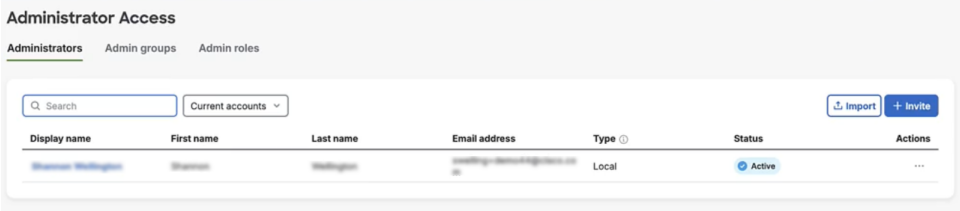
- **Duo Administrator with Owner Role**: Ensure this Duo Owner account holder is also an administrator in Security Cloud Control. Log in to the Duo dashboard, then navigate to **Users** > **Manage** > **Administrators**.

- **Verify Security Cloud Control Administrator Group**: Within Security Cloud Control, the Duo Owner account holder must be a member of the **All Products Administrator** group. To add an administrator to Security Cloud Control and assign them to a group, navigate to **Platform Management** > **Access Management** > **Administrator Access** in the Security Cloud Control dashboard.

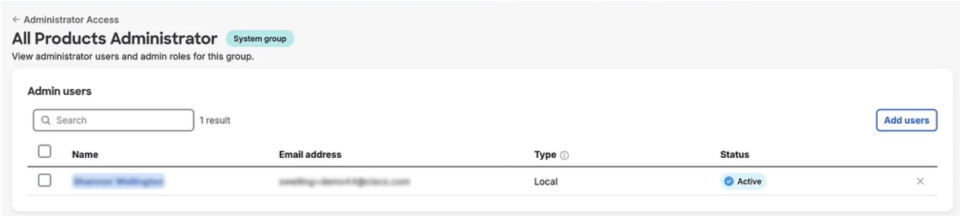
  The Duo owner's email must match the Security Cloud Control's Administrator email and in the All Products Administrator group.

Procedure

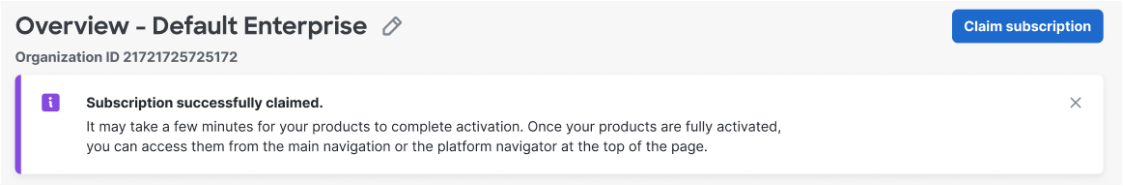
1. In Security Cloud Control, navigate to **Platform management > Administrator Access**. If the Duo owner is not in this list, click **+ Invite** to create an account for the Duo owner.



2. Click **Admin Groups > All Products Administrator**. If the Duo owner is not listed here, click **Add users** to add the Duo owner to the list.



3. In Security Cloud Control, enter your Secure Access subscription claim code. For a detailed procedure, see Claim a Subscription in Security Cloud Control documentation.

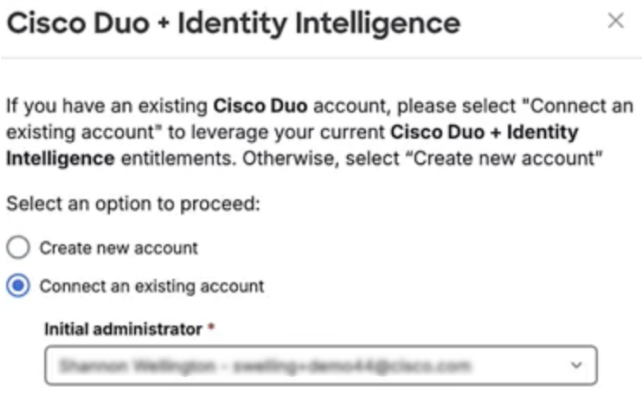


Secure Access will begin the activation process within Security Cloud Control.

4. The Security Cloud Control **Overview dashboard** will update the **Product and service activation status** menu when your Duo and Cisco Identity Intelligence entitlements are available. Click **Action required** to link to your existing Cisco Duo and Identity Intelligence accounts.



5. Select **Connect an existing account**.

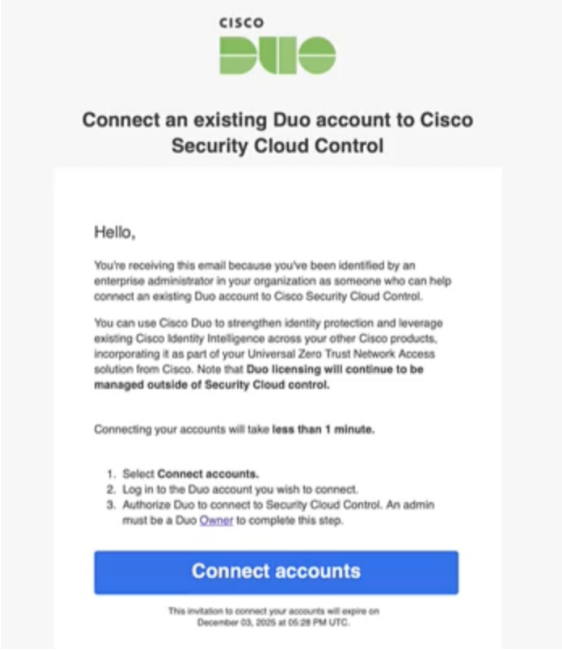


6. From the **Initial administrator** drop-down, choose the Security Cloud Control administrator with the same email address as the Duo Owner.
7. Click **Activate**.

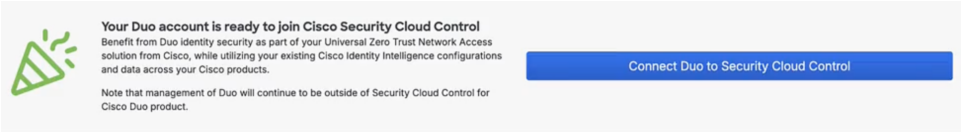
The Security Cloud Control **Overview dashboard** will update to show that Cisco Identity Intelligence is being activated. Security Cloud Control will send an authorization email to the initial administrator.

8. Instruct the Duo Owner to follow these steps to connect their Security Cloud Control and Duo accounts:

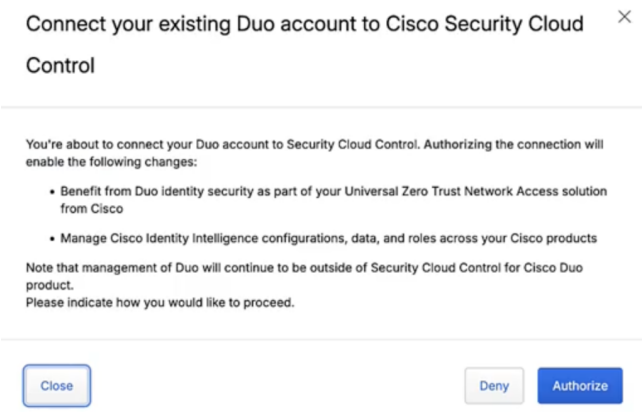
   a) Click the **Connect accounts** link in the email. They will be directed to log in to Duo.



   b) At the top of the Duo dashboard, a banner will appear. Click **Connect Duo to Security Cloud Control**.

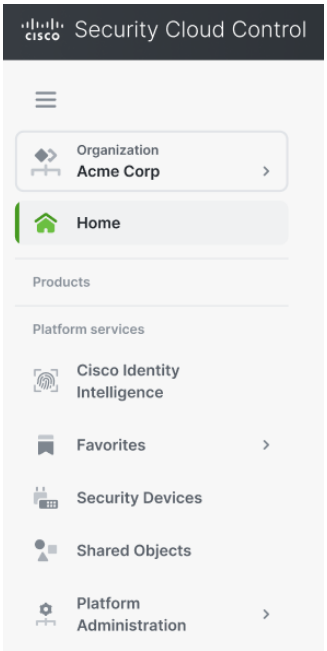


   c) In the pop-up window, click **Authorize**.



The Duo owner will receive an email that Duo, Cisco Identity Intelligence, and Security Cloud Control accounts are connected.

Once your Cisco Identity Intelligence instance is successfully activated, a Cisco Identity Intelligence menu item will become available under **Platform services** in the Security Cloud Control's left navigation menu.



To integrate Duo with Cisco Identity Intelligence, follow steps 5 and 6 in Configure a New Duo and Cisco Identity Intelligence Tenant with Secure Access.

What to do next

Add the same Identity Providers (IdPs) to both Cisco Identity Intelligence (via Security Cloud Control) and Secure Access. For more information, see After Integrating Cisco Identity Intelligence.

For more information on Systems Logs, see Systems Logs.

Integrate your Duo directory with Secure Access. Follow these steps, Duo Directory Integration with Secure Access.

After Integrating Cisco Identity Intelligence

After integrating Secure Access with Cisco Identity Intelligence in Security Cloud Control.

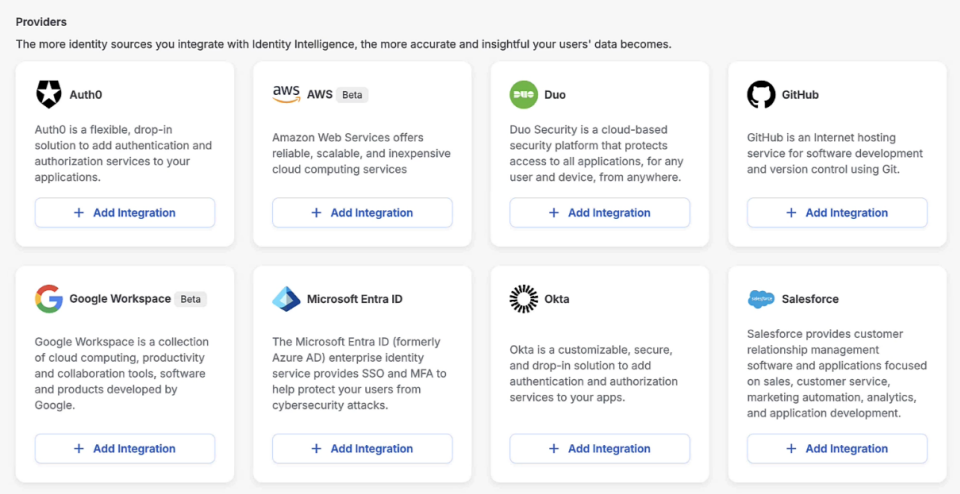
To maximize the effectiveness of Cisco Identity Intelligence (CII), we recommend integrating all available third-party products and IdPs– especially recommend integrating Duo Directory. For more information, see Duo Directory Integration with Secure Access.

By aggregating these disparate identity and data points alongside your primary identity provider, Cisco Identity Intelligence generates a more accurate and comprehensive trust score for every user.

Procedure

---

1. To add IdPs in the Secure Access dashboard:
   a) In Secure Access, navigate to **Connect** > **Essentials** > **Users, Groups, and Endpoint Devices**.
   b) Select **Configuration management**.
   c) Choose **Integrate directories** and follow the detailed instructions in Add a Cloud Identity Provider.
2. To add IdPs to Cisco Identity Intelligence in the Security Cloud Control dashboard:
   a) In Security Cloud Control, navigate to **Platform Services** > **Identity Intelligence** > **Integrations**
   b) Select your provider and click **Add Integration**.



c) Follow the instructions for specific integrations in Configuring Integrations in the Cisco Identity Intelligence knowledge base (formerly Oort).

After successful integration and once the same IdPs are added to both products, user trust levels will become visible in Secure Access.

> **Note**
>
> It can take up to 24 hours for user trust levels to update in Secure Access after the initial integration.

What to do next

After successfully integrating Secure Access with Identity Intelligence via Security Cloud Control, you can verify the integration and explore user trust levels:

- View Users Provisioned in Secure Access: View the potential risk of each user provisioned by an identity sources connected to both Secure Access and Identity Intelligence.
- View User Details: View an explanation and time stamp of a user's most recent Trust Level.

For comprehensive information on user trust levels and their calculation, refer to the User Trust Level documentation in the Cisco Identity Intelligence knowledge base (formerly Oort).

Duo Directory Integration with Secure Access

After integrating Secure Access with Duo and Cisco Identity Intelligence, we recommend configuring your Duo directory as an identity provider for Secure Access.

We highly recommend integrating your Duo directory as an identity provider with Secure Access. This integration ensures users can securely access both private and internet applications while strengthening the accuracy of your user's trust level. If you are interested in integrating other IdPs, see Configure Identity Providers.

Before you begin

Procedure

1. In the Security Cloud Control dashboard > click **Secure Access** in the left navigation bar. For a detailed procedure to add Duo IdP directory, see Add the Duo IdP directory to Secure Access.

   Once Duo Directory Integration is complete, you will see the user's information added to the Users, Groups, and Endpoint Devices page.

2. Next, you need to integrate a SAML 2.0 or OIDC SSO provider.
   a) See Configure Integrations with SAML Identity Providers for steps on how to configure Duo for SAML.
   b) See Configure Integrations with OIDC Identity Providers for steps on how to configure Duo for OpenID Connect.

   May take up to 24 hours for these trust levels to be calculated and updated.

Integrate Cisco SASE with Meraki SD-WAN

Provides instructions for completing the Integrate Cisco SASE with Meraki SD-WAN workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Cisco SASE (Secure Access Service Edge) securely connects users, devices, and applications from anywhere with minimal effort. It combines networking, security, and visibility in a single, easy-to-manage solution. This enables a flexible hybrid work experience that boosts productivity and protects the network.

Cisco SASE supports 1:1 integration between each Secure Access organization and Meraki organization. Secure Access Multi-organization is supported but each Secure Access child organization can connect with one and only one Meraki organization. For more information about this supported integration, see the Cisco Secure Access integration - Design Best Practices and Meraki IPSec to autoVPN Secure Access Manual Migration Guide.

Cisco SASE does not support integration between Meraki SD-WAN and Secure Access DNS.

Important

The Cisco SASE integration established between Meraki SD-WAN and Secure Access is available with no special licensing requirements. This allows the following to ensure smooth onboarding:

- Secure Access organizations created prior to July 2, 2025 may need a flag enabled in order to access this functionality. If your Secure Access org was created after July 2, 2025, you will have this flag. If you encounter an error when onboarding via Meraki, contact Cisco Secure Access Support.
- Secure Access organizations **must** be managed with Security Cloud Control (SCC). If your Secure Access org was created after March 31, 2025, you have this funcoitnality. If you do not have your Secure Access org tied to an SCC enterprise, onboarding via Meraki causes an error. See About Cisco Security Cloud Control or contact Cisco Secure Access Support, your Account team, or CX contact for assistance integrating Secure Access with SCC.
- For more information, see Cisco SASE: Getting Started Guide in Meraki documentation.

Before you begin

Before you begin, review the following prerequisites.

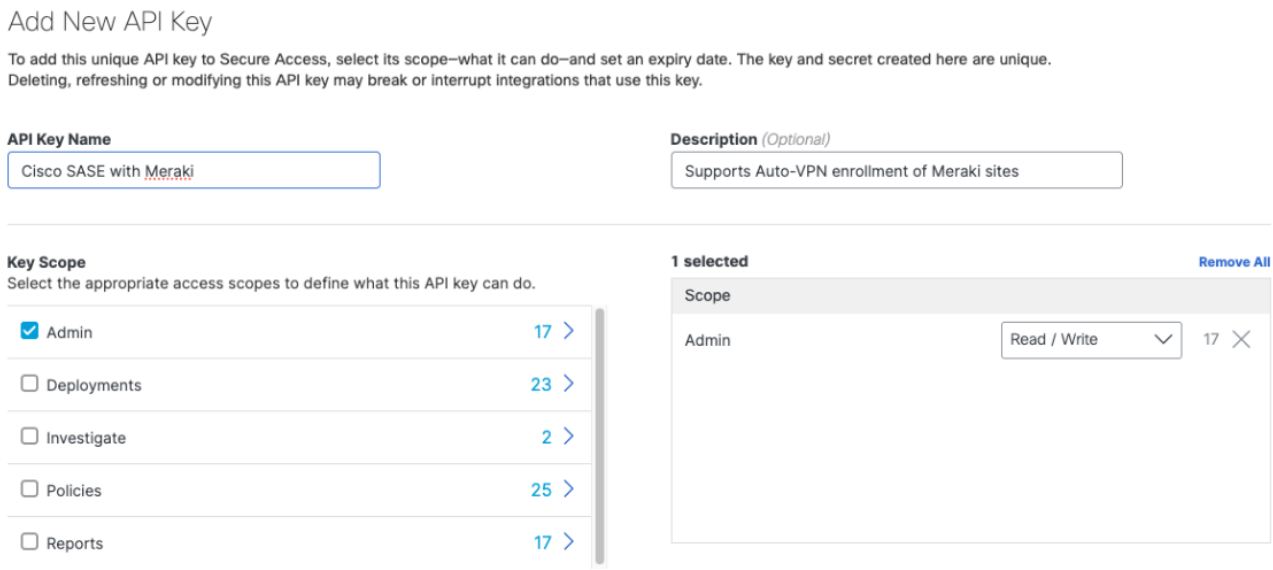
- A Cisco Meraki MX/Z4 device (running Security and SD-WAN (MX,Z) version 19.1+ firmware). For more information, see Meraki Security and SD-WAN (MX,Z) Features Directory.

- A valid Meraki SD-WAN license or subscription.
- A valid Cisco Secure Access subscription.
- An integration established between Secure Access and Security Cloud Control. For more information, see About Cisco Security Cloud Control.
- A Cisco SASE integration established between Cloud Managed Meraki SD-WAN and Secure Access. For more information, see SASE in Meraki Integrations documentation.

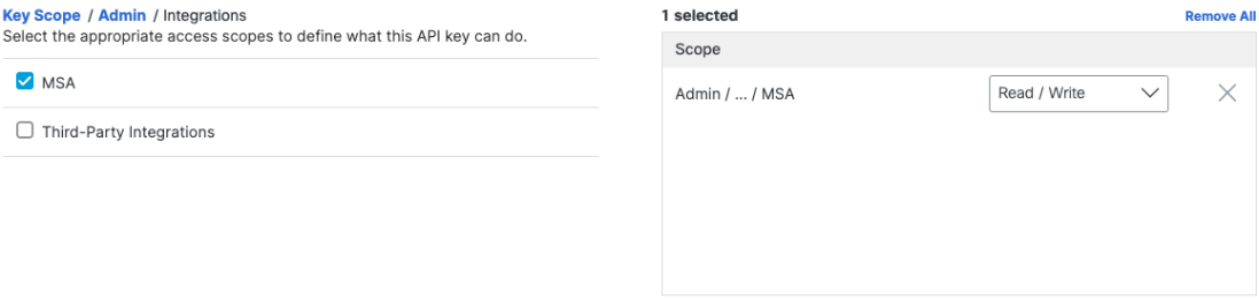
Procedure

Onboarding

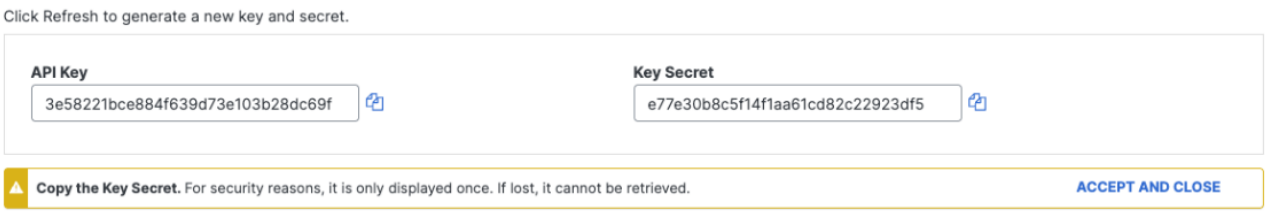
1. In Secure Access, navigate to **Admin** > **API Keys**.
2. Click **Add** at the top right.
3. Configure the **Add New API Key** menu:



a) Enter an **API Key Name**
b) Enter a **Description** (optional).
c) Under **Key Scope**, expand the **Admin** scope, then expand **Integrations**.
d) Check the box for **MSA**. Ensure the **Scope** is set to the default, **Read/Write**.



e) Click **Create Key**.
f) Copy the **API Key** and **Key Secret**.

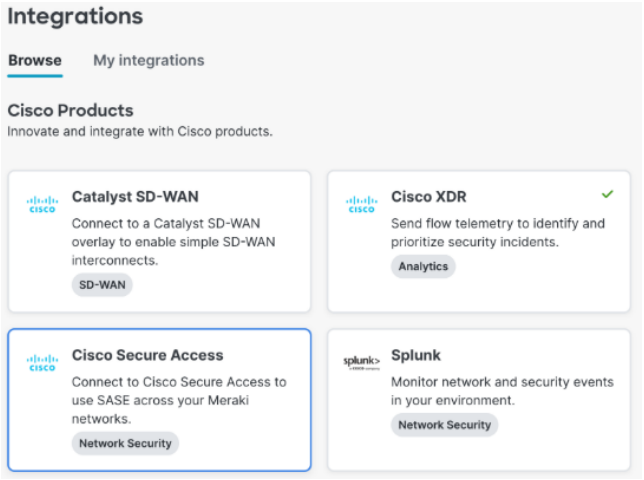


> **Note**
>
> For security reasons, the Key Secret is only displayed once. If lost, it cannot be retrieved.

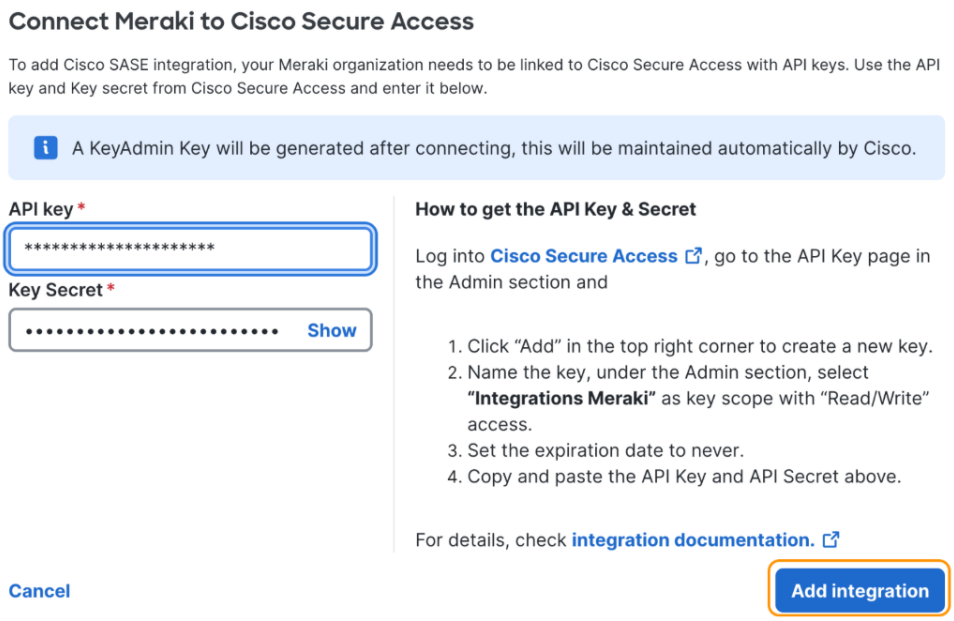
a) Click **ACCEPT AND CLOSE**.

> **Note**
>
> If your SD-WAN environment requires spoke-to-spoke communication over the hub, contact Meraki Support for assistance with the remaining integration steps.

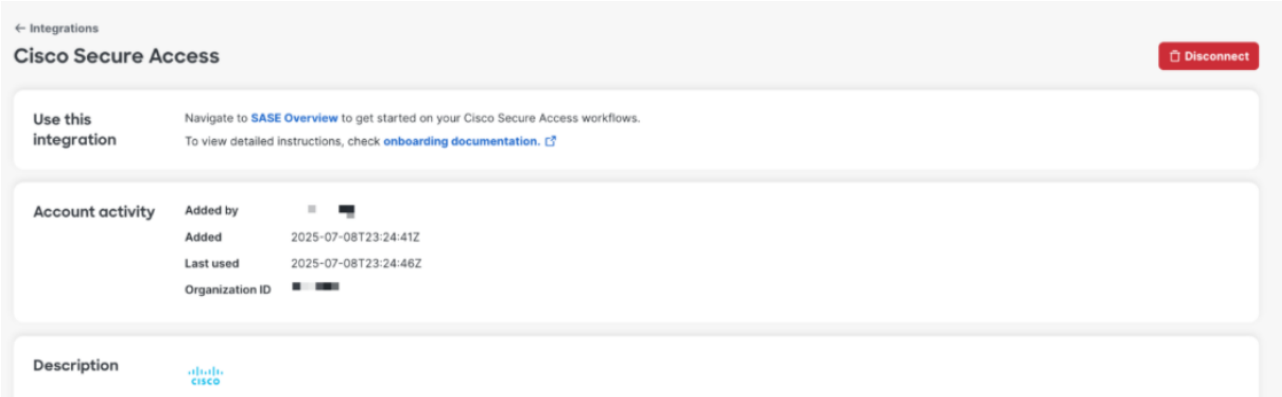
4. In the Meraki dashboard, navigate to **Organization** > **Integrations** (In the **Configure** section).
5. Select **Cisco Secure Access**.



6. Click **+ Connect** at the top right.
7. Enter the Secure Access API key and Key Secret pair that you created in Secure Access, then click **Add integration**.

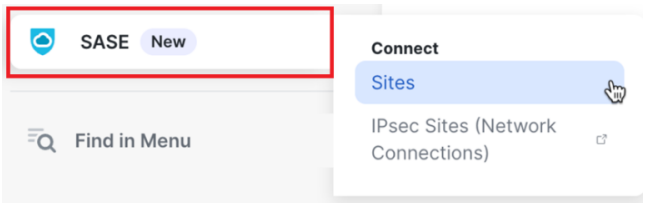


After completion, the page displays the user who added the integration, the integration date, and the organization ID from the Secure Access dashboard.



For more information, see Cisco SASE: Onboarding/Offboarding Cisco SASE with Meraki SD-WAN.

Your Meraki dashboard will now include a **SASE** tab in the left navigation menu.



Your Secure Access dashboard will now include a **Return to Meraki** tab in the left navigation menu.



What to do next

Enroll your Sites

From your Meraki dashboard, connect Meraki sites to Secure Access regions. The SASE Auto-VPN feature will automatically establish primary and secondary IPsec tunnels between your Meraki sites and Secure Access data centers.

For more information, see Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels in Secure Access documentation and Cisco SASE: Sites Connectivity in Meraki documentation.

Configure Access Policy

Once the Auto-VPN tunnels are connected, Meraki sites appear as network tunnel groups in Secure Access. Protect one or more Meraki sites by configuring Secure Access private and internet access rules.

For more information, see Manage the Access Policy in Secure Access documentation and Cisco SASE: Policy in Meraki documentation.

86 Cisco Security for Chromebook Client

Topics:

- About Cisco Security for Chromebooks
- Integrate the Google Workspace Identity Service
- Deploy the Cisco Security for Chromebooks Client
- View Protection Status of Chromebook Devices
- Add Policies to a Chromebook Device
- Cisco Security for Chromebooks Client FAQ
- Google Workspace Identity Service FAQ

Provides an overview of Cisco Security for Chromebook Client in Cisco Secure Access, including About Cisco Security for Chromebooks, Integrate the Google Workspace Identity Service, and Deploy the Cisco Security for Chromebooks Client. It outlines the concepts, configuration tasks, and operational guidance presented in this chapter.

About Cisco Security for Chromebooks

Describes Cisco Security for Chromebooks in Cisco Secure Access. As an IT admin, you need to know which employees are sending certain DNS and web requests so you can create and enforce security policies about their identities and their use of cloud resources.

As an IT admin, you need to know which employees are sending certain DNS and web requests so you can create and enforce security policies about their identities and their use of cloud resources.

The Cisco Security for Chromebook client is a Chrome-browser extension that leverages DNS-over-HTTPS (DoH) to provide enhanced protection and performance for Chromebook devices. The software client enforces DNS and SWG protection for end users on Secure Access with:

- DNS-layer security for the entire Chromebook OS
- Secure web gateway (SIG) protection for the Chrome browser

Key benefits

Describes Key benefits in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

- **Enhanced security:** Added support for custom block pages and safe search.
- **OS protection**: Extends DNS protection beyond the Chrome browser to all Chromebook apps and components.
- **Unified client experience**: Unifies protection for DNS layer and SWG layer in one client.
- **Selective SWG enablement**: SIG customers who want to enable only DNS protection (DoH) for Chromebooks can disable SWG for their organizations.
- **Faster page load**: By leveraging DoH, the client offers a faster and more effective browsing experience.

Prerequisites for Cisco Security for Chromebooks Client

Describes Prerequisites for Cisco Security for Chromebooks Client in Cisco Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic.

To enable DoH and SWG protection on the Cisco Secure Chromebook client, these prerequisites are required:

- You must have Cisco Security for Chromebooks Client.
- You must have Secure Access login credentials.
- A Google Workspace Admin account to push the Cisco Security for Chromebook client to all the Chromebook devices.
- **Recommended**: Sync Google Workspace Identities with Secure Access to apply Google Workspace user and organizational unit based policies. For information, see Integrate Google Workspace Identities.
- Chrome OS 110 or later (to enable DoH-based DNS layer protection on Chromebooks).
- Chromebooks must not be in kiosk mode.
- For DNS-layer protection, port 53 UDP and 443 TCP must be allowed.
- For SWG-layer protection, port 8888 (TCP) must be accessible to 146.112.0.0/16 and 155.190.0.0/16.
- You must have access to:
  - https://registration.polaris.qq.opendns.com
  - https://sync.hydra.opendns.com

    - https://doh.sse.cisco.com

- Chromebooks must be connected and logged in.
- Install Cisco Secure Access root certificate on your Chromebooks to avoid certificate errors when accessing a Secure Access block page. For more information, see Install the Secure Access Root Certificate.
- For more information about how to push the root certificate from Google admin console to all your Chromebook devices, see Set up TLS (or SSL) inspection on Chrome devices.
- In the Google Workspace Admin console, the incognito window must be disallowed. From the Incognito mode menu, choose Disallow incognito mode. For more information, search for Incognito Mode in Chrome Enterprise and Education Help.
- For SWG, you can configure the DNS servers on your network to forward DNS traffic to Secure Access. This configuration provides the most accurate selection of SWG Data Center locations. For more information, see Point your DNS to Cisco Secure Access.
- Third-party web filtering or web proxy solutions may interfere with SWG proxy setup of the Cisco Security for Chromebook client. We recommend that you remove these solutions before deploying Cisco Security for Chromebook client.
- The following devices and operating systems are not supported:
    - Chrome browser on OS X, Windows, and Linux
    - Devices running variations or third-party distributions of ChromeOS, such as Neverware CloudReady

Network requirements

Protection	Port and Protocol	Source/Destination	Notes
DNS and SWG Layer	53 (UDP)		Configured DNS resolvers should be reachable.
DNS and SWG Layer	443 (TCP) Registration.	Registration. polaris.qq.opendns.com	Used for registration of the client.
DNS and SWG Layer	443 (TCP)	sync.hydra.opendns.com	HTTPS. Used to sync device details and to fetch configuration.
DNS and SWG Layer	443 (TCP)	doh.sse.cisco.com	HTTPS. Used to resolve DNS requests.
SWG Layer	8888 (TCP)	146.112.0/0/16 155.190.0.0/16	155.190.0.0/16 SWG Proxy IP address ranges

Limitations for Cisco Security for Chromebooks

Describes Limitations for Cisco Security for Chromebooks in Cisco Secure Access. ChromeOS has introduced the DNS over HTTPS included and excluded domains feature starting from version 131.

Limitation	Description
Internal domains	ChromeOS does not allow configuration of customers' internal domains, which affects configurations involving split domains or split brain DNS configurations. However, if DNS-over-HTTPS (DoH) cannot resolve internal domains, ChromeOS does a local resolution as a backup. To address this situation, use the "DNS-over-HTTPS with insecure fallback" configuration in Google Workspace. For detailed steps, see Enabling DNS-over-HTTPS with Insecure Fallback guide. **Note** ChromeOS has introduced the **DNS over HTTPS included and excluded domains** feature starting from version 131. This feature allows administrators to exclude specific domains from being resolved by Umbrella DoH resolvers, ensuring that internal DNS infrastructure handles these queries. For more information, see Bypass Internal Domains from DNS-over-HTTPS (DoH).
Virtual appliance	Virtual appliance detection and backoff is not supported by the DNS-over-HTTPS based solution because of ChromeOS limitations. However, you should not encounter issues with DNS resolutions in Chromebooks because of the limitation.
APP authentication	While using SWG for Cisco Security for Chromebook client, you might encounter issues uploading and downloading files in Android apps, including Gmail and Google Drive. The problem is that the SWG proxy lacks the required authentication headers for specific app requests, which causes errors in authorizing file transfers: https://chromeenterprise.google/policies/#SystemProxySettings
Reporting and Logging	Because the Cisco Secure Client AnyConnect VPN module on ChromeOS is based on the Android client, there is currently no way to differentiate between Chromebook and Android devices when viewing reports and logs.

Integrate the Google Workspace Identity Service

Describes how to integrate the Google Workspace Identity Service in Cisco Secure Access. If you use the Google Workspace Identity service to manage organizational units (OUs) and user accounts, you can integrate the service with Secure Access to synchronize that information with Secure Access policies.

If you use the Google Workspace Identity service to manage organizational units (OUs) and user accounts, you can integrate the service with Secure Access to synchronize that information with Secure Access policies.

> **Note**
>
> When managing users and Chromebooks in the Google Admin console, it's common practice to create logical groups of users to which you apply specific internet-access and content-filtering policies. For example, you might create a "staff and students" group with two subgroups for that group: "high-school students" and "middle-school students."

> **Note**
>
> These users and groups are currently intended exclusively for Chromebook (DNS/SWG) identification. The users cannot be utilized for other purposes, such as SAML authentication.

This section explains how to install the Cisco User Management for Secure Access app on your organization's Google Workspace. The application authorizes Secure Access to retrieve OUs and users from your Google Workspace account.

Limitations

Describes limitations for the Google Workspace Identity Service in Secure Access. It summarizes the behavior, configuration context, and operational considerations presented throughout the topic for administrators working with the service.

- You can import only Google Workspace users and organizational units. You cannot import Google Workspace groups.
- Google Workspace user and organizational unit updates can take up to 1 hour to appear on Secure Access.
- If you have more than 250K users and organizational units to import from Google Workspace, you must create a support case. Contact Cisco support at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Integrate the Google Workspace Identity Service

Provides instructions for completing the Integrate the Google Workspace Identity Service workflow in Cisco Secure Access. The Google Workspace super administrator must have a Secure Access account with the Full Admin role.

Before you begin

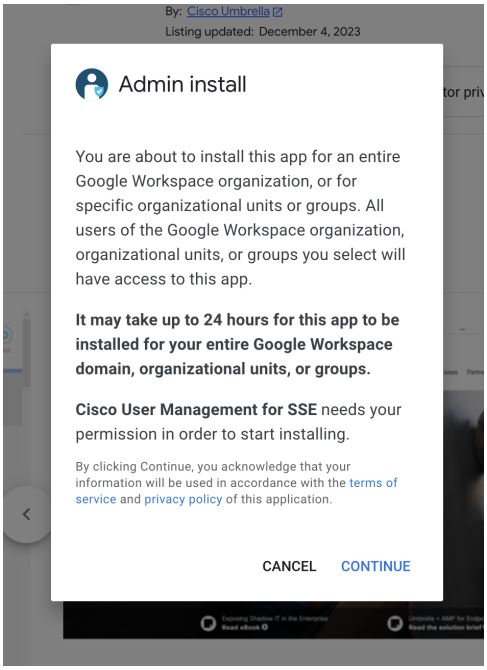
The Google Workspace super administrator must have a Secure Access account with the Full Admin role. For more information about Secure Access user accounts, see Manage Accounts.

Procedure

1. Sign into the Google Workspace administration console with your Google Workspace super administrator ID.
2. From Google Workspace Marketplace, navigate to the **Cisco User Management for Secure Access** app.
3. Click **Install**.

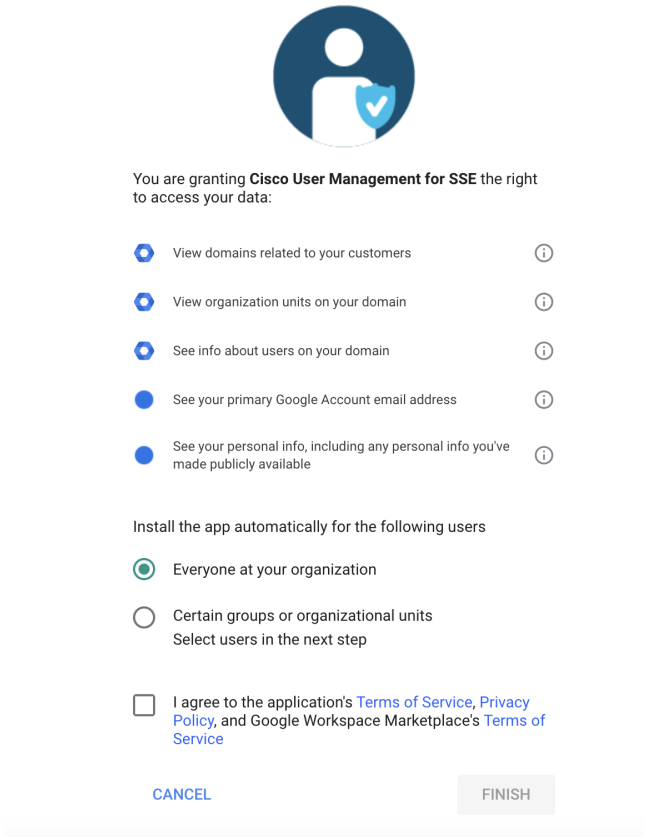


4. In the Admin install pop-up window, click **CONTINUE**.



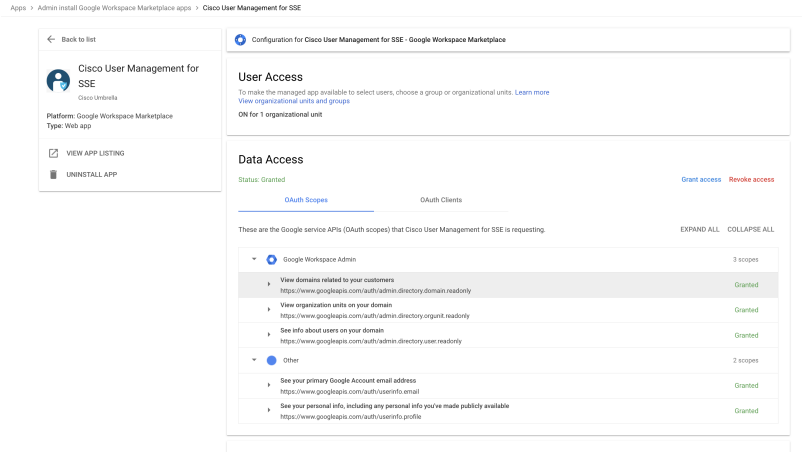
5. Click the checkbox to agree to the Terms of Service statements and Privacy Policy.
6. Click **FINISH**.

Result: The app installs in your organization's instance of Google Workspace.

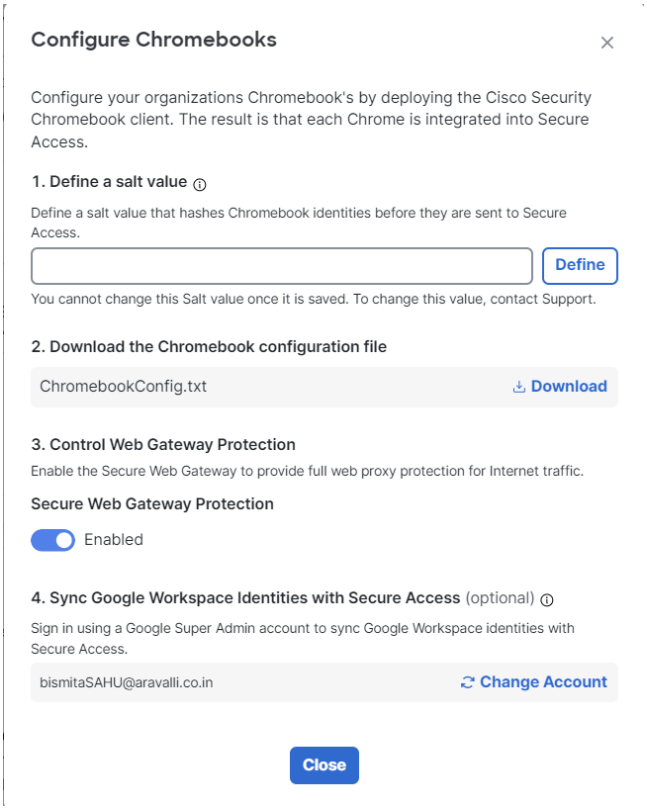


7. To confirm that the app has installed, navigate to **Apps** > **Admin install Google Workspace Marketplace apps** > **Cisco User Management for SSE**.

   Result: The Cisco User Management for Secure Access app displays.



8. In Secure Access, navigate to **Connect** > **End User Connectivity** > **Internet Security** > **ChromeOS** > **Configure**.
9. In the Configure Chromebooks pop-up window, follow the instructions in Step 4 to sync your Google Workspace identities with Secure Access.



Your organization's Google Workspace users and organizational units sync with Secure Access. A sync may take up to 1 hour. After the sync, the Secure Access policy rules display the Google Workspace OUs and users. For more information, see Manage the Access Policy.

Deploy the Cisco Security for Chromebooks Client

Describes how to deploy the Cisco Security for Chromebooks Client in Cisco Secure Access. The Cisco Security for Chromebook client allows you to enable DNS-layer and SWG-layer protection for Chromebook users.

The Cisco Security for Chromebook client allows you to enable DNS-layer and SWG-layer protection for Chromebook users. This section explains the steps for deploying the Cisco Security for Chromebook client that involves the use of Secure Access and the Google Admin console.

About DNS-Layer Protection

Describes About DNS-Layer Protection in Cisco Secure Access. DNS over HTTPS (DoH) is used to send DNS queries to Secure Access resolvers.

DNS over HTTPS (DoH) is used to send DNS queries to Secure Access resolvers. DNS queries are sent using DoH templates, which capture the Chromebook identities. Chromebook identities are hashed using a user-defined salt value, which you can use to:

- copy the DoH templates
- configure the Enterprise policy on the Google Admin console
- propagate the DoH templates to the Chromebooks

About SWG-Layer Protection

Describes SWG-Layer Protection in Cisco Secure Access. For SWG protection, Chromebooks are listed as identities in the internet-access policy.

For SWG protection, Chromebooks are listed as identities in the internet-access policy. Chromebooks are immediately protected by the default rule set and rules of the policy. At any time, add your own rule sets and rules to the internet-access policy to customize your Chromebook protection.

As part of deployment in Secure Access, you copy the Cisco Security for Chromebook client extension ID for access to the Cisco Security for Chromebook client through the Chrome Web Store. During deployment, the file is uploaded to the Google Admin console, which then pushes the Cisco Security for Chromebook client to all your Chromebooks.

> **Note**
>
> After the client is installed on a Chromebook, allow a few hours for Chromebook traffic to appear in Secure Access.

High-Level Steps for Deploying Cisco Security for Chromebook Client

Describes High-Level Steps for Deploying Cisco Security for Chromebook Client in Cisco Secure Access. Deploying Cisco Security for Chromebook client includes procedures in Secure Access and the Google Admin console.

Deploying Cisco Security for Chromebook client includes procedures in Secure Access and the Google Admin console.

Step 1. In Secure Access:

- Configure a salt value
- Get the URLs for two DoH templates
- Download the Chromebook JSON file

Step 2. In the Google Admin console

- Configure the DoH templates

Step 1: Deploying Cisco Security for Chromebook Client

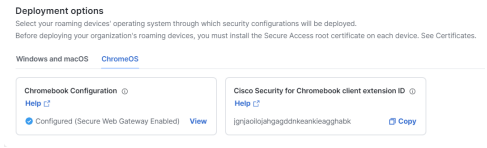
Provides instructions for completing the first step in deploying Cisco Security for Chromebook Client. From Secure Access, navigate to Connect End User Connectivity.

Procedure

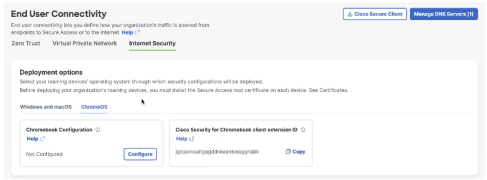
1. From Secure Access, navigate to **Connect** > **End User Connectivity**.
2. On the End User Connectivity page, click the **Internet Security** tab.



3. In the Deployment options section, click the **ChromeOS** tab.



4. In the Chromebook Configuration section, click **Configure**.



5. In the Configure Chromebooks window, follow the onscreen instructions.
   a. Define a salt value.
      - A salt is a piece of random data that is added to a password before the password is hashed and stored. Salting prevents hackers who breach an enterprise environment from reverse-engineering passwords and stealing them from the database.

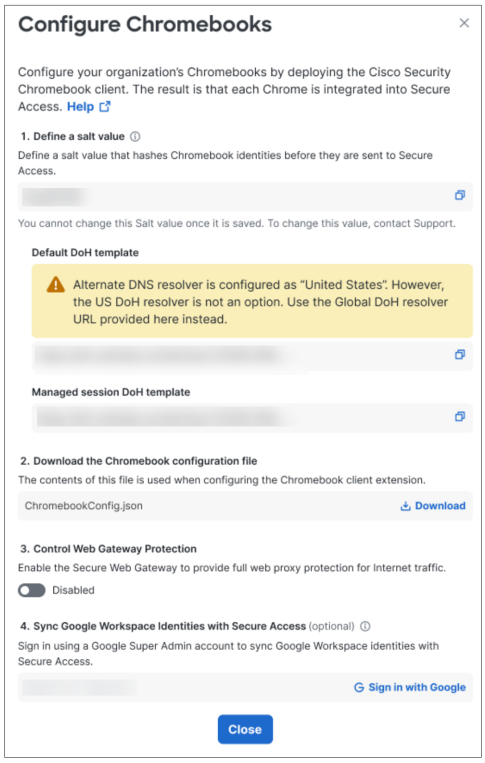
        Important

        Copy and save the salt value. You will need it when you deploy the Cisco Security for Chromebook client in the Google Admin console.

      - **Result**: After you define the salt value, two DoH templates are created:
        - If the Alternate DNS resolver is configured as 'United States', then rather than the US DoH resolver, which is not an option, you will need to use the Global DoH resolver URL provided instead.
        - The managed session DoH template, which is used *only* for managed guest-session devices.
        - **Important**: Copy and save the URLs for the DoH templates. You will need them when you deploy the Cisco Security for Chromebook client in the Google Admin console.

   b. Download the Chromebook configuration file.
   c. Enable SWG protection.

d. Recommended: Sync Google Workspace identities with Secure Access. You need superadmin-level access to Google Workspace.



Step 2: Deploying Cisco Security for Chromebook Client

Provides instructions for completing the Step 2 workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

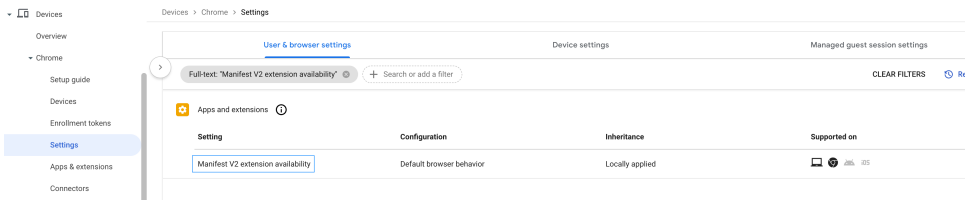
---

1. Sign into the Google Admin console.
2. Navigate to **Devices** > **Chrome** > **Settings** > **Users & browser settings**.

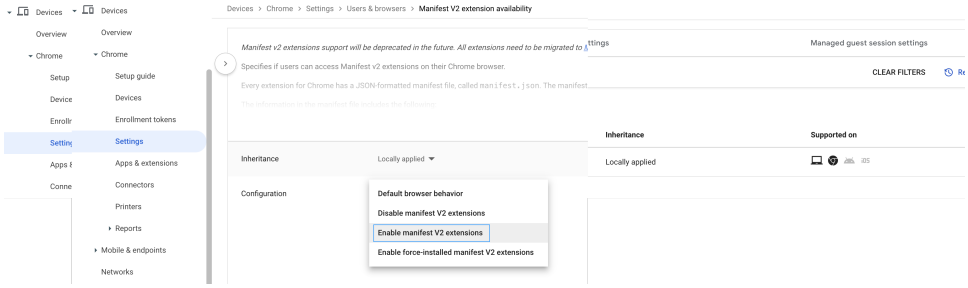
> **Note**
>
> Cisco Security for Chromebook is transitioning from Manifest V2 to Manifest V3 for Chrome extensions. In the meantime, Google recommends that you use the Manifest V2 Extensions Availability policy to ensure the continued functioning of Manifest V2 extensions.

3. To enable the availability of Manifest V2 extensions, filter the settings for **Manifest**.

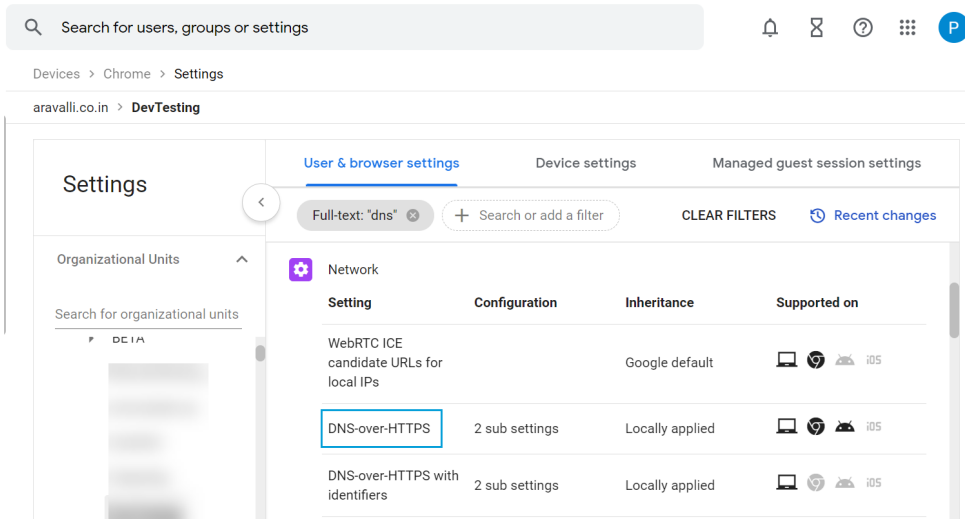
   Result: The Manifest V2 Extension Availability displays.



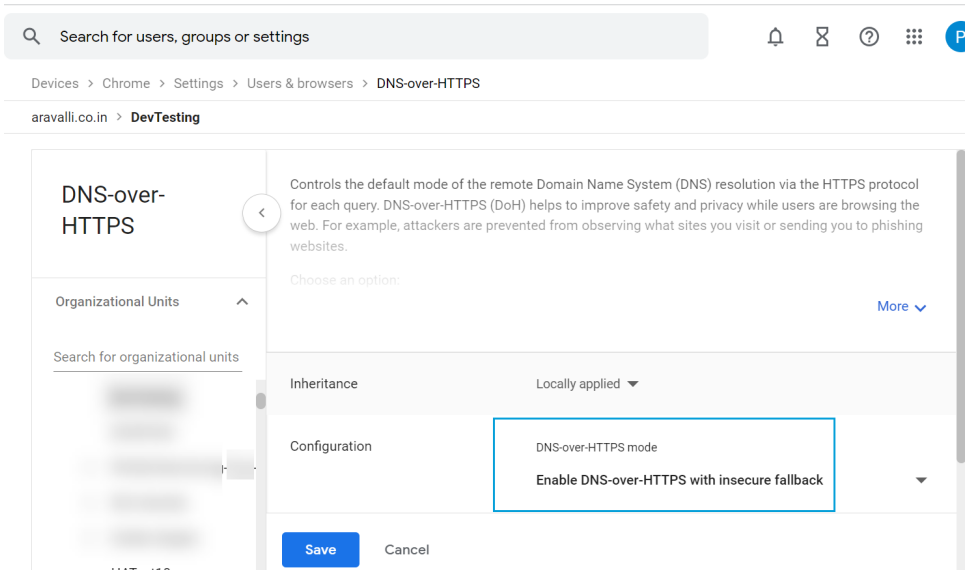
4. Select the parent OU on which you want to enable the Manifest V2 extension availability policy.
5. Click **Manifest V2 extension availability**.
6. In the **Configuration** drop-down list, choose **Enable manifest V2 extensions**.



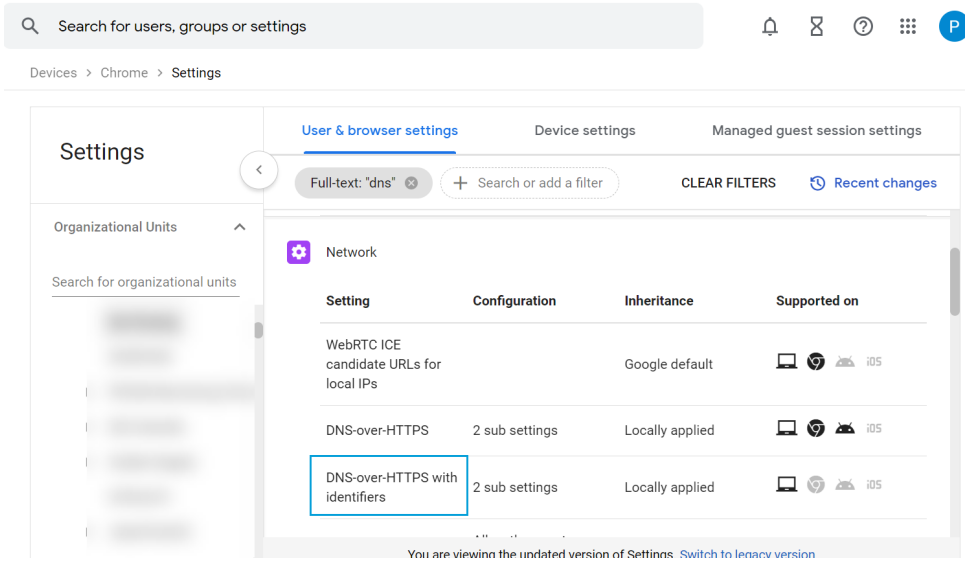
7. Filter for **DNS**.



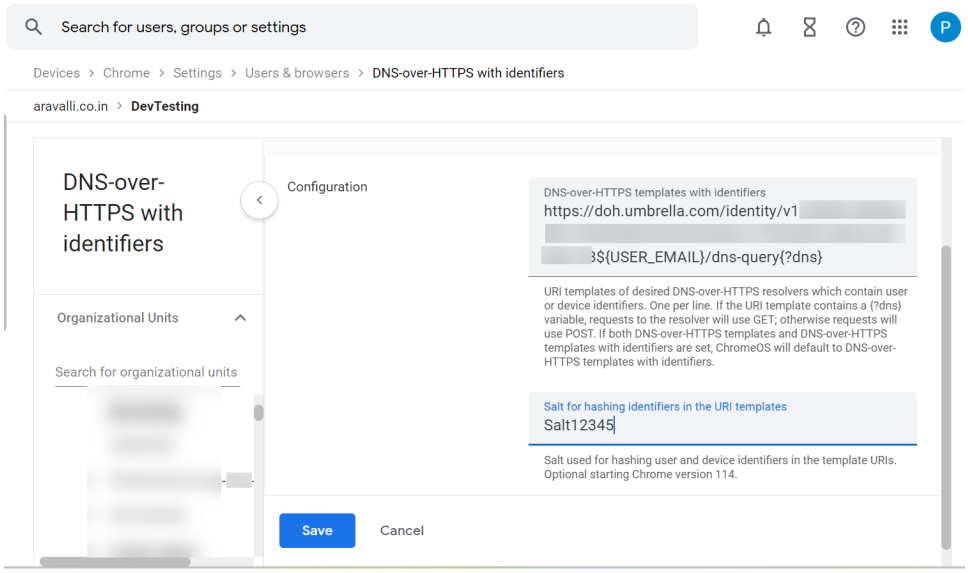
8. Click **DNS-over-HTTPS** and configure it to **Enable DNS-over-HTTPS with insecure fallback**.



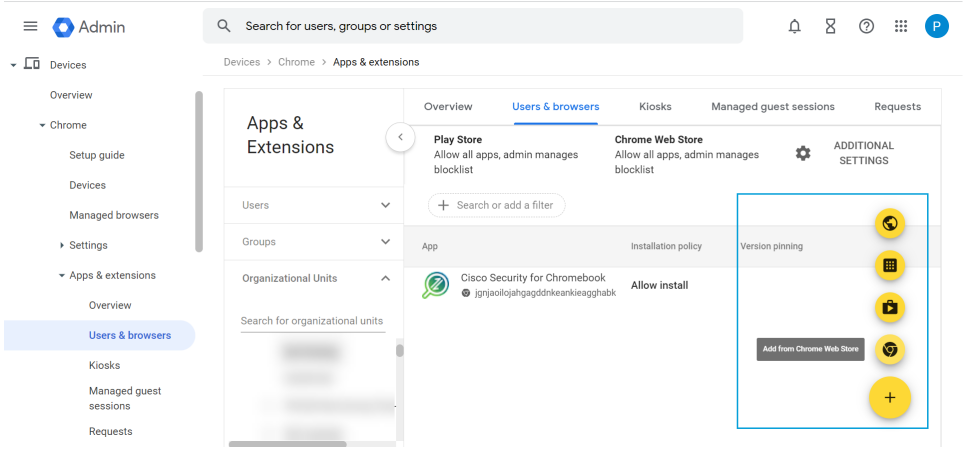
9. Return to the **Users & browser settings** page and click **DNS-over-HTTPS with Identifiers**.



10. Enter the URL of the **Default** DoH template that you copied from Secure Access.
11. Enter the salt value that you copied from Secure Access.
12. Click **Save**.

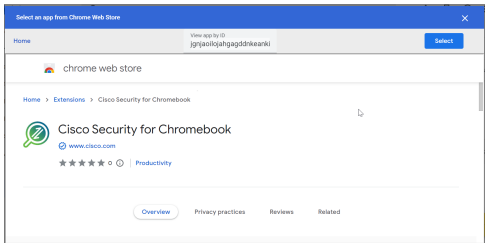


13. From **Apps & Extensions**, navigate to **Users & browsers** > **Organizational Units**.
14. Expand **Organizational Units** and choose the OU to which you want to deploy Cisco Security for Chromebook client.
15. Click **+** and select **Add from Chrome Web Store**.



16. In the Chrome Web Store, navigate to **Extensions**.
17. Search for the Cisco Security for Chromebook client extension using the ID **jgnjaoilojahgagddnkeankieagghabk**.

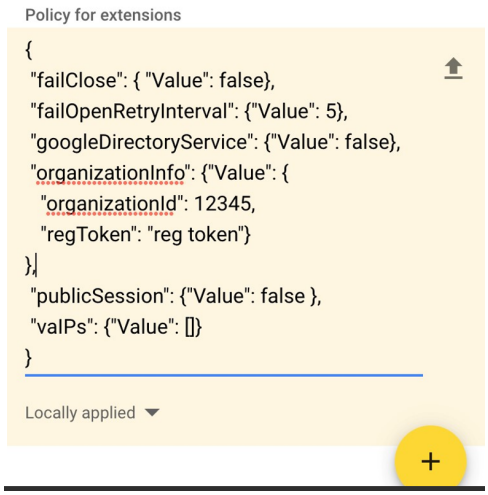
> **Note**
>
> When copying and pasting the extension ID into the search field, ensure there are no spaces before or after it. This will help you locate the Cisco Security for Chromebook client extension.



18. Click **Select**.

    Result: The extension is added to the selected organization unit.

19. For the JSON file you downloaded, click the **Upload** link to upload the file.

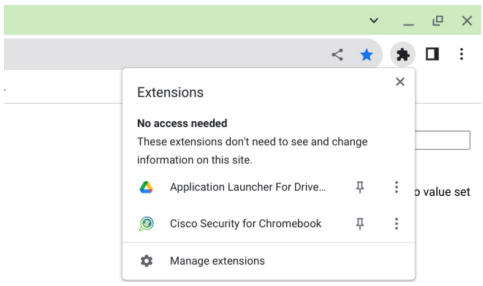


> **Note**
>
> The JSON configuration parameters **googleDirectoryService** and **valPs** apply only to the Umbrella Chromebooks client and **__not __**to the Cisco Security for Chromebooks client.

20. Choose **Force install**.
21. Click **Save**.

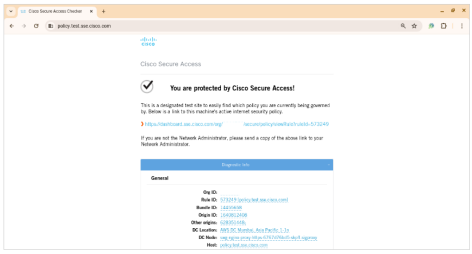
    Result: The Cisco Security for Chromebook client extension is installed. Force install ensures that Chromebook users in the organization unit cannot remove or disable the extension.

22. Confirm that Cisco Security for Chromebook client is installed on the Chromebooks and that the old Umbrella Chromebook Client (app and extension) is blocked.



23. To verify that a device is being protected by Secure Access, go to <https://policy.test.sse.cisco.com>
24. A confirmation message displays.

> **Note**
>
> It may take Google up to 8 hours to push the Chrome extension to all your Chromebooks. After the client is installed in a Chromebook, allow a few hours for Chromebook traffic to appear in Secure Access (the Chromebook must be connected and signed in).



Bypass Internal Domains from DNS-over-HTTPS (DoH)

Describes how to bypass internal domains from DNS-over-HTTPS (DoH) in Cisco Secure Access. Cisco Secure Access provides a secure DNS-over-HTTPS (DoH) service for resolving domain names.

Cisco Secure Access provides a secure DNS-over-HTTPS (DoH) service for resolving domain names. However, some customers may prefer to bypass this service in the following scenarios:

- When internal domains need to be resolved through internal DNS servers instead of Secure Access DoH resolvers, which cannot resolve these domains.
- When split domains require different resolutions when accessed internally and externally.

To bypass internal domain DNS resolution, use the **DNS over HTTPS included and excluded domains** feature in the Google Admin console. This feature allows administrators to exclude specific domains from being resolved by Secure Access DoH resolvers, ensuring that internal DNS infrastructure handles these queries.

This solution offers customers the flexibility to manage DNS resolution for specific internal domains through their internal DNS infrastructure.

Note

The **DNS over HTTPS included and excluded domains** feature is supported starting from ChromeOS version 131. For more details, see the ChromeOS 131 release notes.

Procedure

Provides instructions for bypassing internal domains from DNS-over-HTTPS. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

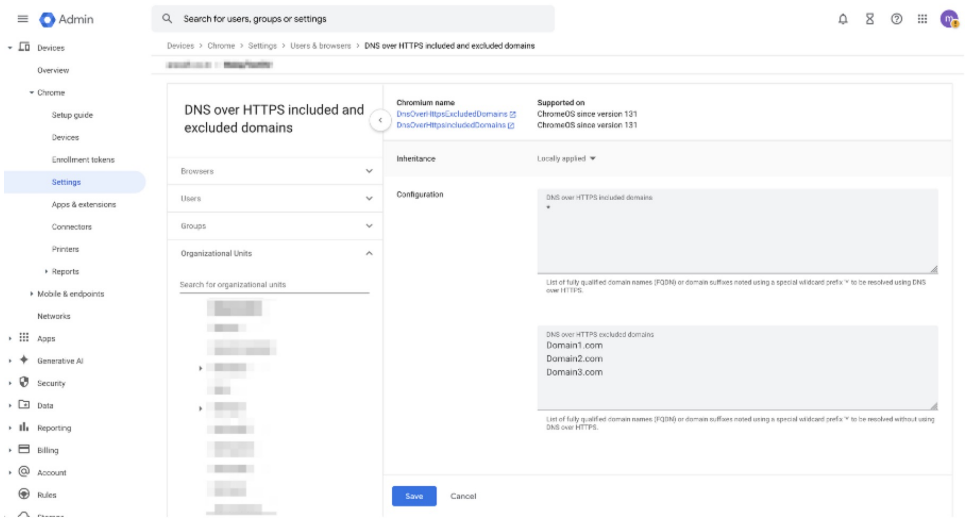
1. Log in to **Google Admin Console**.
2. Navigate to **Devices** > **Chrome** > **Settings**. The **User & browser settings** page appears.
3. Expand **Organizational Units**, and choose the OU where the DoH settings are applied.
4. Configure the **DNS over HTTPS included and excluded domains** option:

What to do next

- **DNS over HTTPS included domains**: Enter the wildcard character asterisk (*) to ensure all DNS traffic is sent to Secure Access DoH resolvers by default.
- **DNS over HTTPS excluded domains**: Enter the domains you want to exclude from Secure Access DoH resolvers, and they will be directed to internal DNS servers.

Note

- In the **DNS over HTTPS excluded domains** list, add all the domains listed under **Internal Domains** (Navigate to **Connect > End User Connectivity > Internet Security > Traffic Steering**, and then click **Add Destination**.) in the Secure Access dashboard.
- When listing multiple domains, enter each domain on a separate line without using commas or semicolons.



Verification

Describes Verification in Cisco Secure Access. After configuration, ensure that internal domains are accessible as expected and are resolved by your internal DNS servers rather than by Secure Access DoH resolvers.

After configuration, ensure that internal domains are accessible as expected and are resolved by your internal DNS servers rather than by Secure Access DoH resolvers. For further assistance, please contact Cisco support.

Enable Reporting for the Private IP Address of a Chromebook Device

Describes how to enable reporting for the Private IP dddress of a Chromebook device in Cisco Secure Access. Chromebook administrators can enable and display the private IP addresses of Chromebooks within the Secure Access Dashboard reports.

Chromebook administrators can enable and display the private IP addresses of Chromebooks within the Secure Access Dashboard reports. This feature supports both Default and Managed Guest Session DoH templates.

To utilize this feature, copy the relevant DoH template from Secure Access, insert the private IP address, and update the modified template in the Google Admin console for the appropriate organizational unit. This will activate the configuration and enable the private IP address to appear in the reports on the Secure Access dashboard.

Important

Applying the new template with the 'DEVICE_IP_ADDRESSES' variable to Chromebooks running an OS version earlier than 126 will result in DoH resolution failure. This failure can lead to a potential loss of internet connectivity and DNS protection. Therefore, ensure that all Chromebooks are updated to ChromeOS 126 or later before implementing this feature to avoid these issues.

Procedure

Provides instructions for enabling reporting for the Private IP Address of a Chromebook Device in Cisco Secure Access. Ensure your Chromebook is updated to Version 126 or later versions.

Before you begin

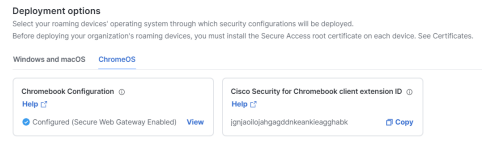
- Ensure your Chromebook is updated to Version 126 or later versions. For more information, look for the 'DEVICE_IP_ADDRESSES' term in the DnsOverHttpsTemplatesWithIdentifiersdocumentation.
- Ensure that your Chromebooks are configured with a Managed Network as the 'DEVICE_IP_ADDRESSES' variable is supported only for Managed Networks. For more information on setting up Managed Networks, see the Set up networks for managed devices guide.

Procedure

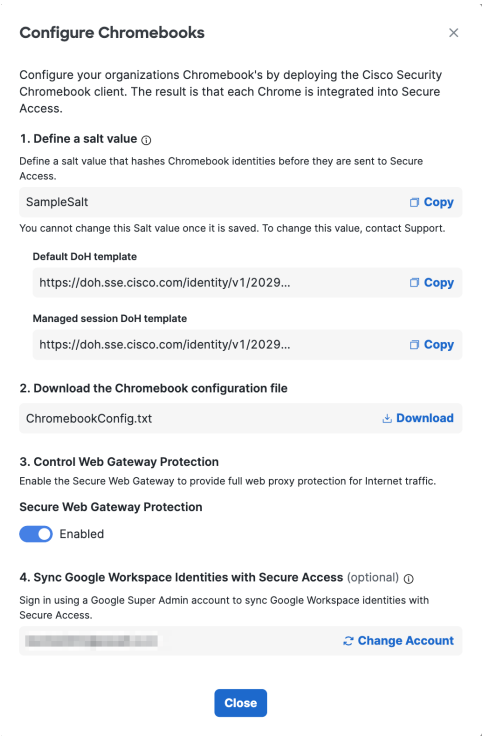
1. From Secure Access, navigate to **Connect** > **End User Connectivity**.
2. On the End User Connectivity page, click the **Internet Security** tab.



3. In the Deployment options section, click the **ChromeOS** tab.



4. In the Chromebook Configuration section, click **View**.



5. In the Configure Chromebooks window, click **Copy** to take a copy of the necessary DoH template URL. Then, add the 'DEVICE_IP_ADDRESSES' placeholder into the DoH template as illustrated in the example URLs below:

Default DoH Template:

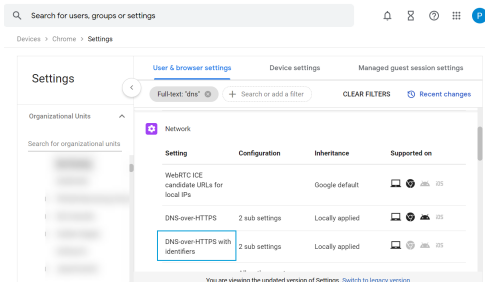
```
https://doh.sse.cisco.com/identity/v1/20292:4f444e530100000999997f7e840002147${USER_EMAIL}40002143${USER_EMAIL}${DEVICE_IP_ADDRESSES}/dns-query
```

Managed Guest/Public Session DoH Template:

```
https://doh.sse.cisco.com/identity/v1/20292:4f444e530100000999997f7e840002143${DEVICE_SERIAL_NUMBER}${DEVICE_IP_ADDRESSES}/dns-query
```

> **Note**
>
> This is a sample URL. Use the actual DoH template from your organization's Secure Access dashboard, ensuring the `DEVICE_IP_ADDRESSES` placeholder is enclosed within ${} without any spaces.

6. In the Google Admin console, navigate to **Devices** > **Chrome** > **Settings** > **Users & browser settings**, choose the organizational unit (OU) on which you want to apply the template configuration, and select **DNS-over-HTTPS with Identifiers**.



7. Enter the updated DoH template to the OU.

> **Note**
>
> We recommend that you test enabling reporting for Private IP Address of Chromebook with a separate test OU before deployment.

After updating the DoH template, your Chromebook device is configured to report their private IP addresses to Secure Access. For assistance, contact Welcome to Cisco Secure Access.

Verify Cisco Security for Chromebooks Client Deployment

Describes Verify Cisco Security for Chromebooks Client Deployment in Cisco Secure Access. Verify the deployment of the Cisco Security for Chromebooks client on a Chromebook device by confirming that the DoH template and the salt values that you configured in the Google Admin console propagated to the device.

Verify the deployment of the Cisco Security for Chromebooks client on a Chromebook device by confirming that the DoH template and the salt values that you configured in the Google Admin console propagated to the device.

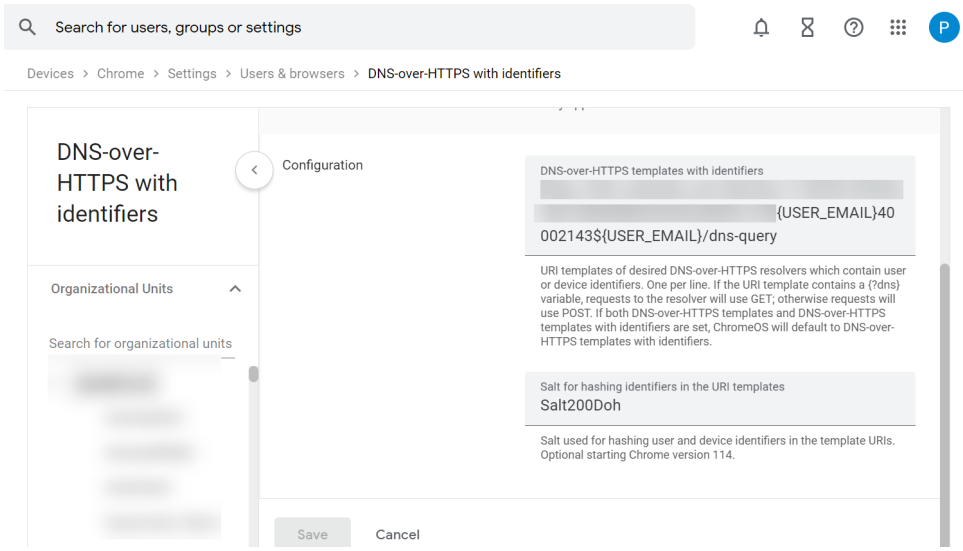
Procedure

Provides instructions for verifying the Cisco Security for Chromebooks Client deployment in Cisco Secure Access. From the Chrome browser on the Chromebook device, go to chrome://policy.

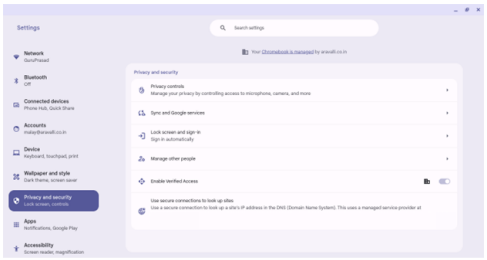
> **Note**
>
> The Chromebook user must belong to the organizational unit (OU) in which the DoH template and salt value were configured.

Procedure

1. From the Chrome browser on the Chromebook device, go to **chrome://policy**.
2. Search for **DNS**.
3. Verify the values of these properties:
   - DnsOverHttpsSalt
   - DnsWithHttpsTemplatesWithIdentifiers

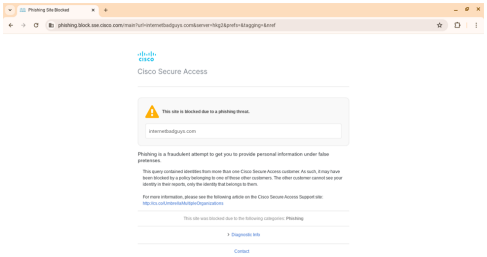


4. Verify that the DoH template resolution with the email ID or serial number is what was configured for the DoH template.
   a) Navigate to **Chromebook Setting** > **Privacy and security** > **Use secure connections to look up sites**.



   b) To verify that a known prohibited site is inaccessible on the Chromebook, go to: https://internetbadguys.com

A confirmation displays that the site was blocked.



Export Device Data to CSV

Describes Export Device Data to CSV in Cisco Secure Access. The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria.

The Export feature allows users to export device information to a CSV file, offering flexibility to export all devices, a specified number of devices, or devices that meet specific search criteria. Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

The exported CSV file contains the following information for each device:

- originId
- label
- serialNumber
- appliedBundle
- dnsProtectionStatus
- swgProtectionStatus
- lastDnsProtectionStatus
- lastSync
- version
- osVersion
- osVersionName
- type

Here the **dnsProtectionStatus** field displays the DNS protection status of respective devices. For information about the various DNS protection statuses, refer to the View DNS Protection Status topic.

For information about the various SWG protection statuses, refer to the View SWG Protection Status topic.

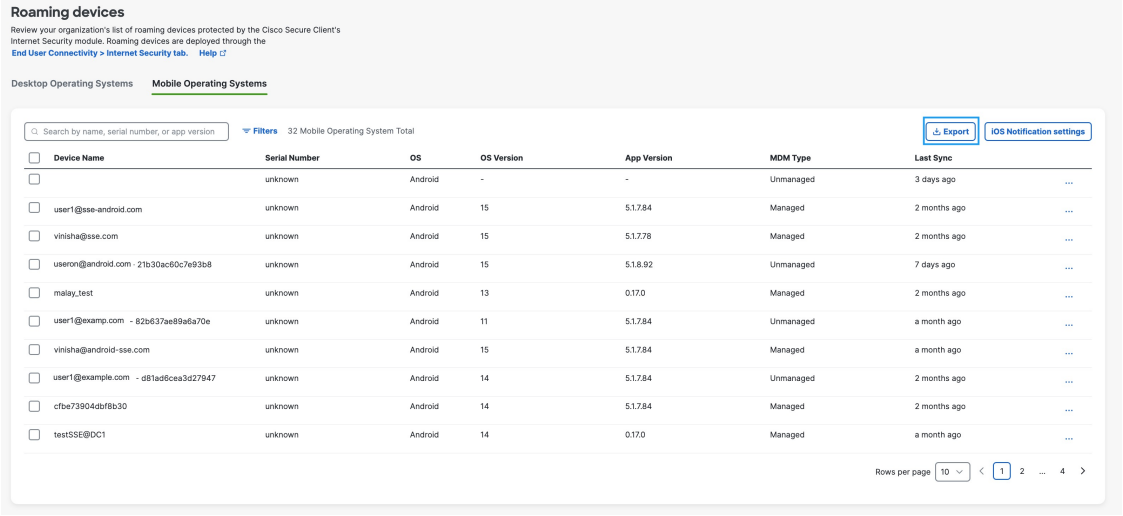
Procedure

Provides instructions for exporting device data to a CSV It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

1. Navigate to **Resources** > **Sources and destinations** > **Roaming Devices**.

2. For roaming devices running mobile operating systems, click **Mobile Operating Systems** or click **Desktop Operating Systems** for roaming devices running desktop operating systems.



3. Choose one of the following export options as per your requirement:
   - Export All Devices
     - Click **Export** at the top of the table to export all devices.
   - Export Selected Devices
     - Check the required number of devices and click **Export Selected** to export a specific number of devices.
   - Export Devices Based on Search Criteria
     - Search by name, serial number, or app version in the search bar. To further refine your search, click **Filter** and specify a search criteria to filter the devices accordingly.
     - Click **Export** to export all the devices meeting the search criteria. Check the required number of devices, and click **Export Selected** to export a specific number of devices that meet the search criteria.

What to do next

Once the export process is complete, the CSV file is downloaded to your **Downloads** folder.

DNS Protection Status in Exported Reports

Describes DNS Protection Status in Exported Reports in Cisco Secure Access. The dnsProtectionStatus column in Resources Roaming Devices exports uses these values.

The **dnsProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No DNS protection status is set or reported.	Not applicable
Open	The device is unprotected because Secure Access DNS resolvers are unreachable.	Unprotected (FailOpen)

Status	Description	Related client state
Transparent	DNS protection is active and reporting, but DNS queries are not encrypted.	Protected
Encrypted	DNS protection is active and DNS queries are encrypted.	Encrypted
VA	DNS protection is provided through a Virtual Appliance.	BehindVA
Network	DNS protection is provided at the network level.	BehindNetwork
Disabled	DNS protection is disabled by configuration or policy.	Disabled
Uninstalled	The Cisco Secure Client Secure Access module is uninstalled.	Not applicable
TrustedCustomerNetwork	DNS protection is disabled on a customer-defined trusted network.	Trusted customer network
CiscoTrustedNetwork	DNS protection is disabled on a Cisco trusted network.	Cisco trusted network
DisabledDueToACVpnFullTunnel	DNS protection is disabled while a full-tunnel VPN connection is active.	DisabledDueToACVpn
Off	The device has not synchronized within the timeout period. Its last status is stale.	Not applicable

Note

`Off` is not applied when the raw status is `Uninstalled` or `-`.

To know more about the DNS protection status of the Cisco Secure Client, see View DNS Protection Status

SWG Protection Status in Exported Reports

Describes SWG Protection Status in Exported Reports in Cisco Secure Access. The swgProtectionStatus column in Resources Roaming Devices exports uses these values.

The **swgProtectionStatus** column in **Resources** > **Roaming Devices** exports uses these values.

Status	Description	Related client state
-	No SWG protection status is set or reported.	Not applicable
Protected	SWG protection is active.	Protected
Unprotected	SWG protection is inactive.	Unprotected
Disabled	SWG protection is disabled by configuration or policy.	Disabled
DisabledDueToVPN	SWG protection is disabled while a VPN full-tunnel connection is active.	Disabled (VPN connection)

Status	Description	Related client state
DisabledDueToTrustedNetwork	SWG protection is disabled while the device is on a trusted network.	Disabled (trusted network)
ConfigError	SWG protection cannot be applied because of a configuration error.	Configuration Error
CloudServiceUnavailable	The SWG cloud service is unreachable from the device.	Cloud Service Unavailable
Offline	The device has not synchronized within the timeout period. Its last SWG status is stale.	Not applicable

To know more about the SWG protection status of the Cisco Secure Client, see View SWG Protection Status

Manage Device Deployment

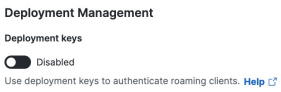
Describes how do manage device deployment in Cisco Secure Access. The Deployment Keys feature provides an effective way to manage device registration within organizations while mitigating unauthorized access.

The **Deployment Keys** feature provides an effective way to manage device registration within organizations while mitigating unauthorized access. This feature introduces the concept of a **deployment key** that can be activated, deactivated, and revoked. By utilizing deployment keys, administrators gain control over the credentials used by devices during registration for Secure Access protection. A deployment key is a field in the Chromebook configuration (ChromebookConfig.txt) file, which is used when registering devices to your organization's network. This feature ensures that only authorized devices are enrolled by requiring an active deployment key for registration.

Deployment keys facilitate seamless device registration and ongoing validation while offering the flexibility to deactivate keys when necessary. If any unauthorized devices try to connect, administrators can swiftly deactivate the current deployment key and delete the suspected devices from the dashboard, ensuring a secure and efficient network environment. The devices will not be able to reregister with the now-deactivated deployment key. Administrators can then activate a new deployment key. This allows IT teams to maintain operational continuity while safeguarding against unauthorized access.

Prerequisites for Device Deployment Management

- For a global deployment, the deployment key feature is optional. If deployment keys are disabled, you must enable them first (**Connect** > **End User Connectivity** > **Internet Security**).

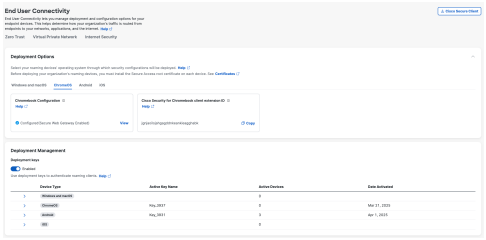


Add and Activate Deployment Key

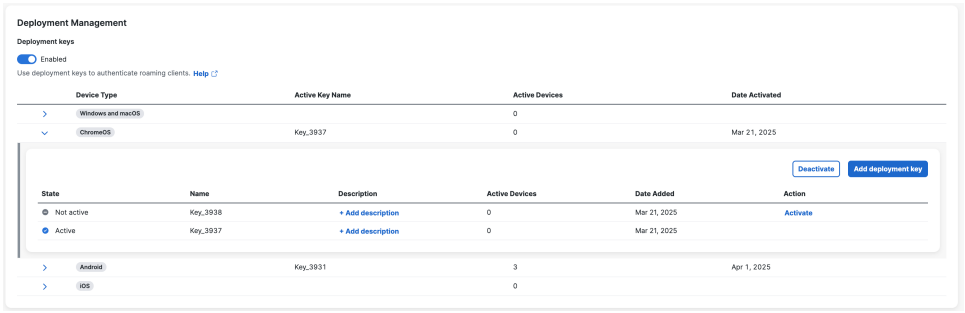
Provides instructions for completing the Add and Activate Deployment Key workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

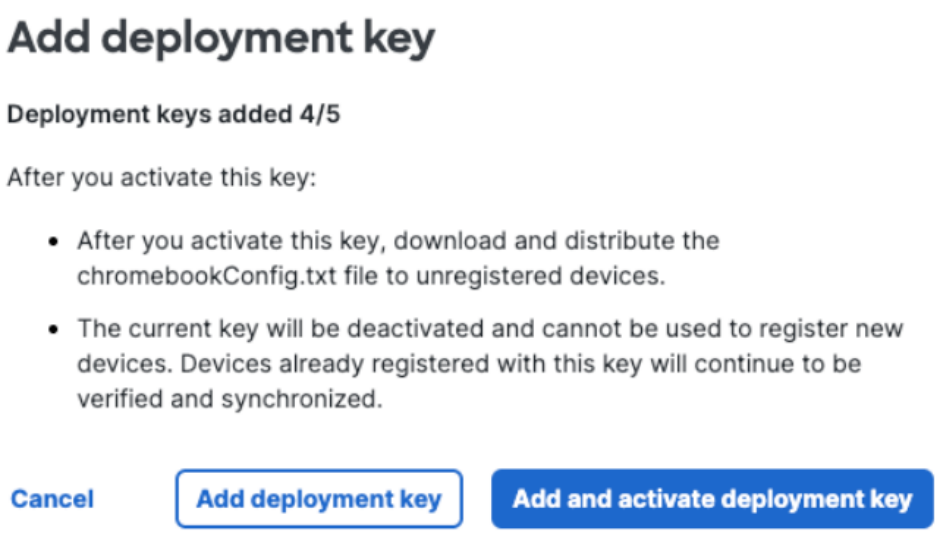
1. Navigate to **Connect** > **End User Connectivity**.
2. Click **Internet Security**.



3. In the **Deployment Management** section, expand the device type (ChromeOS).



4. Click **Add deployment key**.
5. In the **Add deployment key** window, click **Add & activate deployment key** to create and activate a deployment key for inclusion in your organization's Chromebook configuration file.

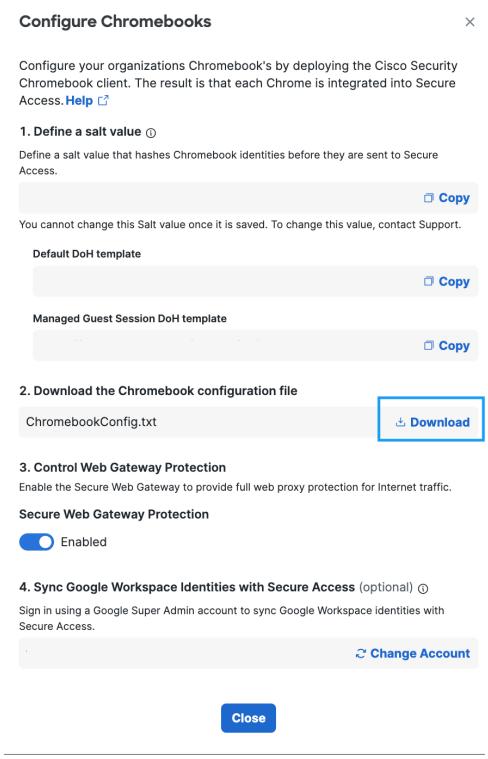


You can choose to add the deployment key immediately, but activate it later. In such a scenario, click **Add deployment key**. The deployment key is added to the table. When you are ready to activate the deployment key, click **Activate** in the **Action** column.

Important

- Only one deployment key can be active at a time for each device type.
- You can add up to five deployment keys per device type. To remove a key, contact Cisco support or your Account Manager.
- The deployment key name includes a random number to ensure its uniqueness.

If your Secure Access deployment requires a deployment key, or if your organization has already enabled them, the Chromebook configuration file can only be downloaded when there is an active deployment key (see image below). Then, push the Chromebook configuration file to Google Admin Console. For more information, see Deploy the Cisco Security for Chromebooks Client.



Manage Deployment Key Compromise

Provides instructions for completing the Manage Deployment Key Compromise workflow in Cisco Secure Access. If you determine that a key has been compromised, take action to protect your network's integrity and security.

If you determine that a key has been compromised, take action to protect your network's integrity and security. Compromised keys can pose significant risks, as they may allow unauthorized access to your network.

This section outlines the necessary actions to be taken to ensure network security and continuity, including deactivating compromised keys, understanding the effects on existing clients, and steps for activating and distributing a new key for secure device registration.

Procedure

1. **Deactivate the Compromised Key**: Prevents any further device registrations using the deactivated key, ensuring that your network remains secure.

   To deactivate a deployment key, perform the following steps:

   a. Navigate to **Connect** > **End User Connectivity**.

   b. Click **Internet Security.**

   c. In the **Deployment Management** section, expand the device type.

   d. Click **Deactivate** in the **Action** column.

Upon deactivating the compromised deployment key, it is important to consider its implications on both existing clients and the registration of new devices:

- **Effect on existing clients**: Deactivating a key will not disrupt the operation of clients already using it. These clients will continue to function normally, minimizing any potential impact on your current network operations.
- **Limitations for new devices**: However, deactivated keys cannot be used for registering new devices. This means that any device attempting to register itself with the deactivated key will be unable to do so.

> **Note**
>
> Devices that are deleted from the dashboard will automatically get reregistered when the Umbrella module is restarted, provided the deployment key in their Chromebook configuration file is active.

2. **Activate the new deployment key**: To facilitate the registration of new devices, you must activate a different deployment key. This new key will replace the compromised one and will be used for future device registrations.
3. **Download a new profile**: After the new key is activated, download a new profile, specifically the Chromebook configuration file. This file contains the updated information, including the new active deployment key.
4. **Distribute the new profile to new devices**: Distribute the updated Chromebook configuration file to any new devices that need to connect to your network. This ensures that they have the correct and secure credentials to register and operate within your network environment.
5. **Update the Chromebook configuration file for registered devices**: Devices that are already registered and require an update to the Chromebook configuration file will automatically receive changes once the configuration is updated in the Google Admin console.

Delete a Deployment Key

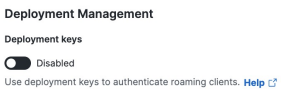
Provides instructions for completing the Delete a Deployment Key workflow in Cisco Secure Access. To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

To delete a deployment key, submit a support ticket to Cisco support or contact your Account Manager.

Revert to the Legacy Deployment Implementation

Provides instructions for how to revert to the Legacy Deployment Implementation. If needed, you can revert to the legacy registration mechanism by disabling the Deployment Keys feature (Connect End User Connectivity Internet Security).

If needed, you can revert to the legacy registration mechanism by disabling the **Deployment Keys** feature (**Connect** > **End User Connectivity** > **Internet Security**).



Procedure

---

1. After disabling the Deployment Keys feature, devices that are currently using the last activated deployment key will continue to be protected by Secure Access. However, new devices will not be able to register with the deactivated deployment key.

2. To revert to the legacy registration mechanism, download the updated Chromebook configuration (ChromebookConfig.txt) file, which will no longer include the deployment key. New devices can now register using the legacy method.

Backward Compatibility

Describes Backward Compatibility in Cisco Secure Access. This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

This feature is designed for backward compatibility, allowing organizations to adopt the new deployment key functionality at their own pace without disrupting existing workflows or functionality.

For example, on Chromebook:

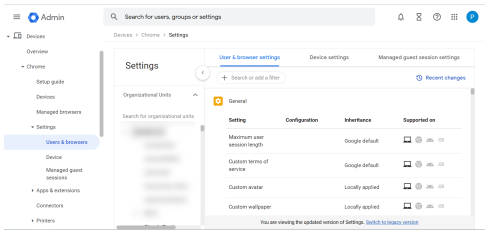
- Cisco Security for Chromebook Client Release 2.2.0 or earlier will continue to use the legacy User ID and fingerprint for registration purposes, regardless of whether a deployment key is present.
- Cisco Security for Chromebook Client Release 2.2.1 or later will use the deployment key for registration, regardless of whether the User ID and fingerprint are present. If the deployment key is unavailable, the legacy User ID and fingerprint will be used for registration instead.

Troubleshoot Cisco Security for Chromebooks Client Deployment

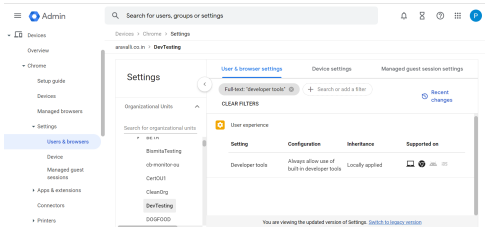
Provides instructions for completing the Troubleshoot Cisco Security for Chromebooks Client Deployment workflow in Cisco Secure Access. From the Google Admin console, navigate to Devices Chrome Settings User and browsers settings .

Procedure

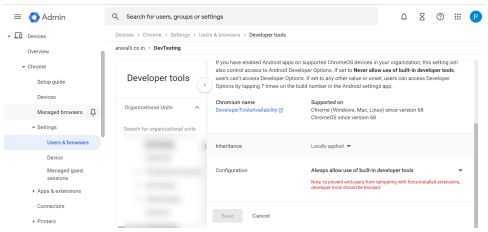
1. From the Google Admin console, navigate to **Devices** > **Chrome** > **Settings** > **User & browsers settings**.



2. Select an organizational unit.
3. Filter for **Developer Tools**.



4. Choose **Always allow use of built-in developer tools**.



View Protection Status of Chromebook Devices

Describes how to view the Protection Status of Chromebook Devices in Cisco Secure Access. After deploying the Cisco Security for Chromebook client to your ChromeOS devices, you can view the state of protection on the devices.

After deploying the Cisco Security for Chromebook client to your ChromeOS devices, you can view the state of protection on the devices.

> **Note**
>
> Fail Open **and** Fail Close states are specific to SWG protection.

Procedure

Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Procedure

Click the Cisco Security for Chromebook icon.

The icon associated with each device reflects the protection status of that device.

Protected – Device is protected by SWG-layer and DNS-layer security.



Fail Open – Device protection is suspended.



Fail Close – Device protection is suspended.



Registration or Sync Failure – Device is not protected.



Disabled – Device is not protected.



Add Policies to a Chromebook Device

Describes how to add policies to a Chromebook Device in Cisco Secure Access. Add a Chromebook-specific access policy in Secure Access to protect all Chromebook devices that are connected to your network.

Add a Chromebook-specific access policy in Secure Access to protect all Chromebook devices that are connected to your network. By creating an internet access rule for the policy, you specify how traffic to internet destinations is handled.

> **Tip**
>
> To maintain end-user privacy when Chromebooks are connected at remote locations, disable content logging and include only security-related events in your reporting.

Procedure

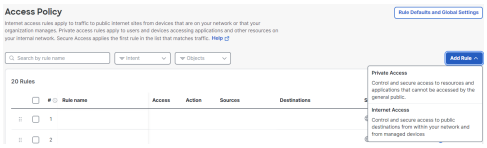
Provides instructions for completing the Procedure workflow in Cisco Secure Access. It explains the sequence of actions and relevant settings presented in the procedure.

Before you begin

- Cisco Security for Chromebook client must be deployed. For more information, see Deploy the Chromebook Client.
- To avoid certificate errors when accessing a Secure Access blocked page, install the Cisco Secure Access root certificate on all Chromebook devices. See Install the Cisco Secure Access Root Certificate.
- Full admin access to Secure Access. See Manage Accounts.

Procedure

1. Navigate to **Secure** > **Access Policies**.
2. On the Access Policy page, click .



3. On the **Add New Internet Access Rule** page, complete the Rule name and Rule order fields and specify the desired access for the rule. For more information, see Add an Internet Access Rule.
4. Click the **From** field and do one of the following:

- To choose a Google Workspace user:
  a. Click **Users**.
  b. Click **Google Workspace Users**.
  c. Check the checkbox for the user.
- To choose a Google Workspace organizational unit:
  a. Click **User Groups and Organizational Units**.
  b. Click Google Workspace Organizational Units.
  c. Click the checkbox for the Google Workspace organizational unit.
- To choose a Chromebook device:
  a. Click **Roaming Devices**.
  b. Click **Chromebooks**.
  c. Click the checkbox for the Chromebook.

5. Choose your destination and configure security requirements. For more information, see Add an Internet Access Rule.

Cisco Security for Chromebooks Client FAQ

Provides frequently asked questions (and answers) about Cisco Security for Chromebooks Client FAQ in Cisco Secure Access.

Q: Does the Cisco Security for Chromebook client work in the Chrome browser for Windows or MacOS?

A: No, the client is designed specifically for ChromeOS and does not function with other operating systems.

Q: Do I need Google Admin console to install the Cisco Security for Chromebook client?

A: Yes, you install the Cisco Security for Chromebook client from the Google Admin console and upload your Secure Access organization-specific JSON file from it. Note that extensions are unlisted on the Chrome store and manual installation on the Chrome browser will break the functionality.

Q: Does the Cisco Security for Chromebook client proxy internet traffic?

A: Yes, the Cisco Security for Chromebook client proxies HTTP and HTTPS traffic.

Q: Is SafeSearch supported?

A: Yes.

Q: Are custom block pages supported?

A: Yes.

Q: Which features are supported by the Cisco Security for Chromebook client and the Secure Access roaming client?

A: See the table below.

Feature	Cisco Security for Chromebook Client	Secure Access Roaming Client
OS support	Chrome OS	Windows and macOS

Feature	Cisco Security for Chromebook Client	Secure Access Roaming Client
DNS-layer security blocks phishing and malicious domains	Yes	Yes
DNS logs augmented with endpoint IP information	Yes	Yes
EDNS message encryption between client and resolver	Yes	Yes
Customizable block page	No	Yes
User email IDs included in logs	Yes	No
User-based policies	Yes	Yes
Organization-wide policies	Yes	Yes
Group-based policies	Yes	Yes
Internal domains	Yes	Yes

Q: How do I know that my Chromebook users are protected?

A: To confirm that a user is protected by the Cisco Security for Chromebook client, go to www.internetbadguys.com from the user's Chrome browser. If a Secure Access block page displays, the client is working.

Q: Can I use welcome.opendns.com to confirm that the Cisco Security for Chromebook client is working?

A: No, welcome.opendns.com is not supported.

Q: How is the Cisco Security for Chromebook client updated?

A: Google is responsible for updating the software in Chromebooks. When Cisco updates the Cisco Security for Chromebook client in the Chrome web store, the upgrade is pushed automatically by Google to all the Chromebooks. The process can take several hours.

Q: Are managed guest sessions and public sessions supported?

A: Yes.

Q: Is kiosk mode supported?

A: No.

Google Workspace Identity Service FAQ

Provides frequently asked questions (and answers) about the Google Workspace Identity Service in Cisco Secure Access, including behavior, configuration context, and operational considerations.

Q: What is the Google Workspace identity service?

A: The service is an enhancement to the Cisco Security Chromebook client. The service enables you to use Secure Access policy enforcement based on your Google Workspace organizational units.

Q: Why is the Google Workspace super administrator's ID needed to enable Google Workspace identity service?

A: To query Google Directory Services using their API, Google requires the super administrator ID. Secure Access uses the ID only to query organizational units and to map users from the Google Directory Server.

Q: How long does it take for Google Workspace identities to appear in Secure Access?

A: Google Admin console organizational units and user information updates take up to 60 minutes to appear in Secure Access.

Q: Can I use the Google Workspace identities service feature without having the Cisco Security Chromebook client?

A: No.

Q: How do I configure the Google Workspace identity service with Secure Access?

A: See Integrate the Google Workspace Identity Service.